

CYBERSECURITY & SUPPLY CHAIN PRIMER FOR GOVERNMENT CONTRACTORS

Greenberg Traurig's Government Contractor Cybersecurity group comprises experienced lawyers intimately familiar with the unique cybersecurity challenges facing the government contracting industry. The government relies on a massive network of contractors to augment its federal civilian employee workforce to perform critical operations and execute on a wide range of duties. A shared understanding of and adherence to baseline cybersecurity standards is critical to this effort.

Working closely with our Greenberg Traurig International Trade, Export Controls & Economic Sanctions, and Data Privacy & Cybersecurity colleagues, we help clients navigate their ever-evolving and nuanced cybersecurity needs.

In response to high-profile cyber attacks and investigative findings of repeat contractor non-compliance, the government is increasing its focus on ensuring that contractors implement adequate cybersecurity and supply chain practices. With ongoing settlements under the Civil Cyber-Fraud Initiative, the ever-increasing regulations, and the evolving threat landscape, contractors must take a proactive approach to compliance and dedicate adequate resources to these areas.

CYBERSECURITY ESSENTIALS

The government is interested in the protection of its information, either in its own possession or in the possession of contractors. Contractors that hold federal information in their systems are required to comply with specific controls and regulations.

BASIC CYBER REQUIREMENTS

The government has issued regulations to impose minimum standards for cybersecurity practices.

Civilian Contractors

- ✔ Must implement the 15 controls identified in FAR 52.204-21.

Defense Contractors

- ✔ Contractors handling Controlled Unclassified Information (CUI) must comply with the 110 controls in NIST SP 800-171, as required by DFARS 252.204-7012 since 2017.
- ✔ DFARS 252.204-7019 further requires defense contractors and subcontractors to post a compliance score reflecting their implementation of the 110 controls.

CMMC REQUIREMENTS

Based on findings in a 2019 Department of Defense (DoD) Inspector General Report, DoD learned that most of its contractors were not consistently implementing the mandatory security requirements despite assessing as such. The then-existing regulations also did not afford DoD with a mechanism to verify contractor compliance. DoD introduced the CMMC Program, which was finalized and implemented under 32 C.F.R. Part 170 and 48 C.F.R. Parts 204, 212, 217, and 252. As of Nov. 10, 2025, contractors and subcontractors should see CMMC requirements rolled out in solicitations over four phases.



[READ OUR GT ALERT SERIES EXPLORING DOD'S CMMC PROGRAM](#)

CIVIL CYBER FRAUD SETTLEMENTS

Since the launch of the Civil Cyber-Fraud Initiative in 2021, the Department of Justice (DOJ) has actively utilized the False Claims Act to pursue cybersecurity related fraud by government contractors. In 2025 alone, the DOJ settled at least eight cyber fraud actions, which involved claims not just against the prime contractors, but against subcontractors and investors, for allegedly failing to comply with cybersecurity requirements in the performance of federal contracts or being otherwise deficient in their safeguarding postures.

SUPPLY CHAIN ESSENTIALS

The government is also focused on increasing the resiliency of supply chains in cyberspace as well as for critical industries. This focus has largely materialized in obligations on contractors to know their data flows; an increased onus to document vendor and supplier relationships; and greater responsibility to affirm their respective organizations' compliance postures to the federal government.

SECTION 889

A provision in the 2019 NDAA, Section 889, prohibits the government from using telecommunications and video surveillance products or services provided by five specific Chinese companies. Also, prime contractors cannot utilize such equipment internally, even for purposes distinct from contract performance.

INFORMATION & COMMUNICATIONS TECHNOLOGY & SERVICES

The Commerce Department is empowered to prohibit transactions involving goods or services designed, developed, manufactured, or supplied from a foreign adversary or by a company that was formed in a foreign adversary. In 2021, President Biden expanded this authority under EO 13873 to cover "connected software applications" in addition to information and communications technologies and services – this rule was finalized and went into effect on July 17, 2023.

DATA SECURITY PROGRAM RULE

The DOJ's new Data Security Program (DSP) Rule also builds upon EO 13873 and imposes significant restrictions on U.S. government contractors and global companies that handle cross-border data flows and transactions. Any U.S. person or company handling Americans' bulk sensitive personal data or U.S. government-related data is now required to implement a written data compliance program that lays out specified due diligence, audit, reporting, and recordkeeping processes.



[READ MORE ON THE DATA SECURITY PROGRAM RULE](#)

SOFTWARE BILL OF MATERIALS (SBOMS)

SBOMs provide those who produce, choose, and operate software with information that enhances their understanding of the software supply chain. In June 2025, the Cybersecurity and Infrastructure Security Agency issued draft updated guidance on the Minimum Elements for a Software Bill of Materials, which the National Telecommunications and Information Administration (NTIA) first published in 2021 in response to EO 14028, "Improving the Nation's Cybersecurity." Broadly, NTIA's SBOM framework provides a standardized mechanism for recording software inventory and has become a critical part of securing the software supply chain at the component level. CISA's updated guidance builds upon this framework and recognizes the rapid growth and distinct developments in the ecosystem, including SaaS in cloud environments and AI systems.



[READ MORE ON SOFTWARE BILL OF MATERIALS](#)

UPCOMING DEVELOPMENTS

NIST REV. 3 CONTROLS

In May 2024, NIST released rev. 3 of the 800-171 controls. DoD has issued a class deviation to DFARS 252.204-7012 to maintain rev. 2 as the CMMC assessment standard, but DoD has started the rulemaking process to adopt rev. 3 and is also developing crosswalk guidance for assessors. On Sept. 29, 2025, NIST also issued the Final Public Draft of rev. 3 to the 800-172 controls for public comment. Contractors that will need to achieve CMMC Level 3 status or otherwise need to comply with higher level controls should monitor developments to this latest revision.

FAR CUI RULE

On Jan. 15, 2025, the FAR Council published a proposed FAR CUI Rule to codify a standardized approach to designating, handling, and safeguarding CUI across all federal executive agencies. The proposed rule also introduced new procedures, including reporting and compliance obligations, and defined roles and responsibilities for both the government and contractors who use and handle CUI. The FAR Council will issue a final rule after resolving all the public comments.



CYBERSECURITY & SUPPLY CHAIN PRIMER

FOR GOVERNMENT CONTRACTORS

This primer provides a general overview of some key cybersecurity regulations and supply chain practices for contractors. The rules are complicated and frequently developing. If you need to implement cybersecurity or supply chain requirements, please reach out to an experienced government contracts lawyer to help you navigate the rules and requirements that apply to your circumstances.



Jeffery M. Chiow
+1 202.331.3149
Jeff.Chiow@gtlaw.com



Jennifer S. Zucker
+1 202.331.3114
ZuckerJS@gtlaw.com



Eleanor M. Ross
+1 202.530.8565
Eleanor.Ross@gtlaw.com



Cassidy Kim
+1 415.590.5133
Cassidy.Kim@gtlaw.com



Olivia Bellini
+1 215.988.7860
Olivia.Bellini@gtlaw.com