

Alert | Government Contracts



December 2025

Federal Contracting Updates for Golden Dome for America Contractors

Go-To Guide:

- The Golden Dome for America (GDA) is a major initiative to develop multi-layered, integrated homeland air and missile defense systems, requiring rapid contractor participation.
- Contractors and vendors throughout the GDA supply chain would be expected to meet stringent cybersecurity requirements, including Controlled Unclassified Information (CUI) controls and Cybersecurity Maturity Model Certification (CMMC) certification.
- GDA contractors would also be expected to comply with the Department of Defense (DoD)'s expanded scope of foreign ownership, control, and influence review.
- Early and ongoing diligence and compliance will be crucial for contractors seeking GDA awards.

Under [Executive Order 14186](#), the current administration issued a directive for DoD to develop a homeland air and missile defense system. This initiative, later named GDA, calls for a complex “system of systems” that would seamlessly integrate space-based interceptors and sensors with existing air and missile defense systems. The administration further seeks to complete GDA over a three-year timeline, and estimated costs range from \$542 billion to \$831 billion over 20 years.

Given the scope of GDA, the call to action has garnered quick interest from both legacy federal contractors and nascent Small Business Innovation Research (SBIR) awardees alike, and has compounded funding

activities from private investors, both domestic and abroad. Further, GDA's goals are reflected in DoD's overall shifts in its [acquisition strategy](#), which prioritizes accelerating commercial preferences and rapid contracting practices. The foregoing incentives are key to reaching GDA milestones but may also create new risks and threat vectors, including cybersecurity vulnerabilities throughout an extended supply chain.

This GT Alert covers key federal contracting updates and compliance requirements that prospective GDA contractors may wish to plan for.

GDA DIB Cybersecurity Requirements

Following the GDA executive order, in July 2025, the DoD CIO issued a comprehensive memorandum outlining cybersecurity implementation and verification requirements for GDA (GDA Memo). The GDA Memo highlights that the GDA "system of systems" design will rely on numerous technology components that are to be integrated into a holistic system. Given this, it will be imperative that contractors throughout the entire GDA defense industrial base (DIB) ecosystem, including vendors, will need to comply with robust cybersecurity requirements, including:

- **CUI controls** in accordance with Defense Acquisition Regulation Supplement (DFARS) 252.2024-7012, -7018, -7019, -7020, and -7021;
- **CMMC certification** based on applicable National Institute of Standards and Technology (NIST) SP 800-171 and Special Publication (SP) 800-172 requirements;
- **Threat intelligence sharing** for all vendors in the supply chain, vulnerability monitoring, and scanning;
- **Secure software development environment**; attestation to Executive Order 14028, "Improving the Nation's Cybersecurity";
- **Insider threat program** that complies with 32 CFR Part 117 and the National Industrial Security Program Operating Manual (NISPOM);
- **Complete bill of materials**, including hardware, software, firmware, microelectronics, chemical, and raw materials;
- **Mature supply chain risk management (SCRM) and controls** for information and communications technology (ICT) supply chain;
- **Tamper protection program** for covered systems and system components; and
- **Artifacts and recordkeeping**, such as for hardware/software inventory, certifications and approvals, test results, incident response plan, SCRM policy, and implemented security technical implementation guides (STIGs).

CMMC Requirements and Compliance Costs

On Sept. 10, 2025, DoD issued a [final rule](#) amending the DFARS to implement the CMMC program for government contractors. The go-live date for the start of phase 1 of CMMC began on Nov. 1, 2025. Since then, multiple DoD components have issued solicitations specifying self-assessment requirements under CMMC Level 1 and 2 and, in some instances, have begun to exercise discretionary authority to require Level 2 third-party assessments.

Many DIB companies that expect to work on GDA efforts will need to be certified timely under the CMMC program. As we covered in [prior GT Alerts](#), proper CMMC certification is a matter of contract eligibility

and must generally be achieved prior to the award of a contract or subcontract. Given the exponential growth in the commercial space sector in recent years, some prospective GDA contractors may need to now implement, for the first time, the underlying controls to safeguard CUI pursuant to NIST SP 800-171, rev. 2. These contractors may incur not only certification costs but also the costs of implementing the underlying controls, which have been a part of DFARS 252.204-7012 since 2018. Moreover, all DIB contractors handling CUI will need to account for forthcoming updates to CMMC Level 2 that will align the requirements to the rev. 3 version of SP 800-171. For now, DoD and the DIB are operating under a **class deviation** that keeps the prior version as the standard; however, contractors should expect that DoD will soon require adherence to rev. 3 through formal rulemaking.

Certain contractors working on breakthrough technologies and critical programs within GDA may also need to comply with enhanced security requirements, including a subset of the NIST SP 800-172 requirements, and achieve Level 3 certification through Defense Contract Management Agency Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) assessments. The foregoing certification expenses are supplemental to the costs to achieve Level 2 final status. Level 3 requirements may start appearing in solicitations beginning in November 2026, and prospective GDA contractors should consider acting now to prepare for a DIBCAC assessment if their capabilities align with the more critical and sensitive efforts expected under GDA.

Enhanced Security Requirements for Safeguarding CUI

On Sept. 29, 2025, NIST issued **draft revisions** to SP 800-172 and SP 800-172A, which prescribe enhanced security requirements for protecting CUI in nonfederal systems. SP 800-172 specifies enhanced controls that are designed to strengthen the protection of CUI associated with critical programs or high value assets, which are susceptible to advanced persistent threats. The enhanced controls, which span 17 security requirement families, include more robust supply chain risk management requirements, including:

- **Notification agreements and procedures** with entities throughout the supply chain for early notification of compromises;
- **Inspection of systems or components** at regular cadence to control for and detect tampering, such as in response to changes in packaging, specifications, factory location, or when individuals return from high-risk locations;
- **Component authenticity** to control for counterfeit risks and to establish incident reporting procedures; and
- **Supply chain integrity**, including provenance and pedigree validation procedures designed to assess supplier claims, increase assurance, and expose any discrepancies in the internal composition of system components and chronology of origin of critical assets.

Under the CMMC program, contractors working on the most sensitive programs and assets will be required to certify at the highest level (Level 3), which derives its requirements from the SP 800-172 controls. The GDA Memo also makes clear that certain contractors will need to comply with these selected SP 800-172 requirements, indicating that at least some GDA awards will require Level 3 certification.

While the GDA Memo does not specify which version of SP 800-172 will apply, the latest **CMMC Assessment Guide** refers to the earlier published version (March 2022). Given the foregoing NIST revisions to SP 800-172 and expected lead time before Level 3 requirements start appearing in

solicitations (at the earliest, in November 2026), GDA contractors may rely on the current class deviation for CMMC Level 2 for a similar pathway for version controlling SP 800-172 for Level 3 assessments.

DoD FOCI Review Expansion

Section 847 of the National Defense Authorization Act (NDAA) for FY 2020 mandated expanding DoD's examination of contractors' foreign ownership, control, or influence (FOCI), requiring pre-award FOCI reviews for unclassified DoD contracts or subcontracts valued above \$5 million. While contracts for commercial products or services are generally excluded under this expansion, a senior DoD official may still require vetting if there is a determination of "risk or potential risk to national security or potential compromise because of sensitive data, systems, or processes." This potential scrutiny may be particularly germane to GDA contractors as private and foreign investment interests grow in commercial space companies, which may trigger robust disclosure requirements about beneficial ownership and other foreign relationships.

Contractors should expect formal implementation of the FOCI expansion through a new DFARS rule, which is still under development. Despite the delay, not to mention the current administration's Federal Acquisition Regulation overhaul efforts and overall shifts in commercial acquisition strategy, prospective GDA contractors should be aware that the FOCI review expansion is grounded in statute (Pub. L. No. 116-92 (Dec. 20, 2019), § 847) – accordingly, the DFARS rule will likely be implemented absent a change in law, bringing thousands of new DoD matters under pre-award vetting.

Takeaways

As companies prepare to bid on and participate in the GDA DIB, they should consider the essential requirements for which DoD will expect compliance readiness. Companies should therefore consider any unique challenges and mitigation strategies for teaming opportunities involving relatively new federal contractors that have special capabilities but might need assistance with ramping up their regulatory compliance postures from both a technical and policy perspective. This may be particularly important in the early phases of GDA, where Space Force acquisition leaders have recently stated workforce reduction challenges and potential difficulties with conducting adequate market research of available commercial solutions – contractors that are positioned to readily present information and validate compliance may be more viable awardees. Additionally, companies and investors should work together on upfront and ongoing diligence efforts to ensure the relationship does not compromise a contractor's qualifications to work on key GDA efforts.

Authors

This GT Alert was prepared by:

- **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

Abu Dhabi*. Albany. Amsterdam. Aspen. Atlanta. Austin. Berlin*. Boston. Charlotte. Chicago. Dallas. Delaware. Denver. Dubai*. Fort Lauderdale. Houston. Las Vegas. London*. Long Island. Los Angeles. Mexico City*. Miami. Milan*. Minneapolis. Munich*. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix.

Portland. Riyadh*. Sacramento. Salt Lake City. San Diego. San Francisco. São Paulo». Seoul». Shanghai. Silicon Valley. Singapore». Tallahassee. Tampa. Tel Aviv^ . Tokyo». Warsaw~. Washington, D.C. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. †Greenberg Traurig's Abu Dhabi office is a branch of Greenberg Traurig, P.A., which is registered with the Abu Dhabi Global Market Registration Authority (Registration No. 29906) and licensed to carry out legal services and regulated as a DNFBP by the ADGM Financial Services Regulatory Authority. ‡Greenberg Traurig's Berlin and Munich offices are operated by Greenberg Traurig Germany, LLP, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ‹Greenberg Traurig's Dubai office is operated by Greenberg Traurig Limited, a company registered in the Dubai International Financial Centre (Registration No. CL7238), regulated as a DNFBP by the Dubai Financial Services Authority and licensed by The Government of Dubai Legal Affairs Department. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Studio Legali Associato, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ‹‹Greenberg Traurig operates in the Kingdom of Saudi Arabia through Greenberg Traurig Khalid Al-Thebity Law Firm, a professional limited liability company, licensed to practice law by the Ministry of Justice. ›Greenberg Traurig's São Paulo office is operated by Greenberg Traurig Brazil Consultores em Direito Estrangeiro – Direito Estadunidense, incorporated in Brazil as a foreign legal consulting firm. Attorneys in the São Paulo office do not practice Brazilian law. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ¯Greenberg Traurig's Singapore office is operated by Greenberg Traurig Singapore LLP which is licensed as a foreign law practice in Singapore. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. †Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimbengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by GREENBERG TRAUIG Nowakowska-Zimoch Wysokiński sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in GREENBERG TRAUIG Nowakowska-Zimoch Wysokiński sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2025 Greenberg Traurig, LLP. All rights reserved.*