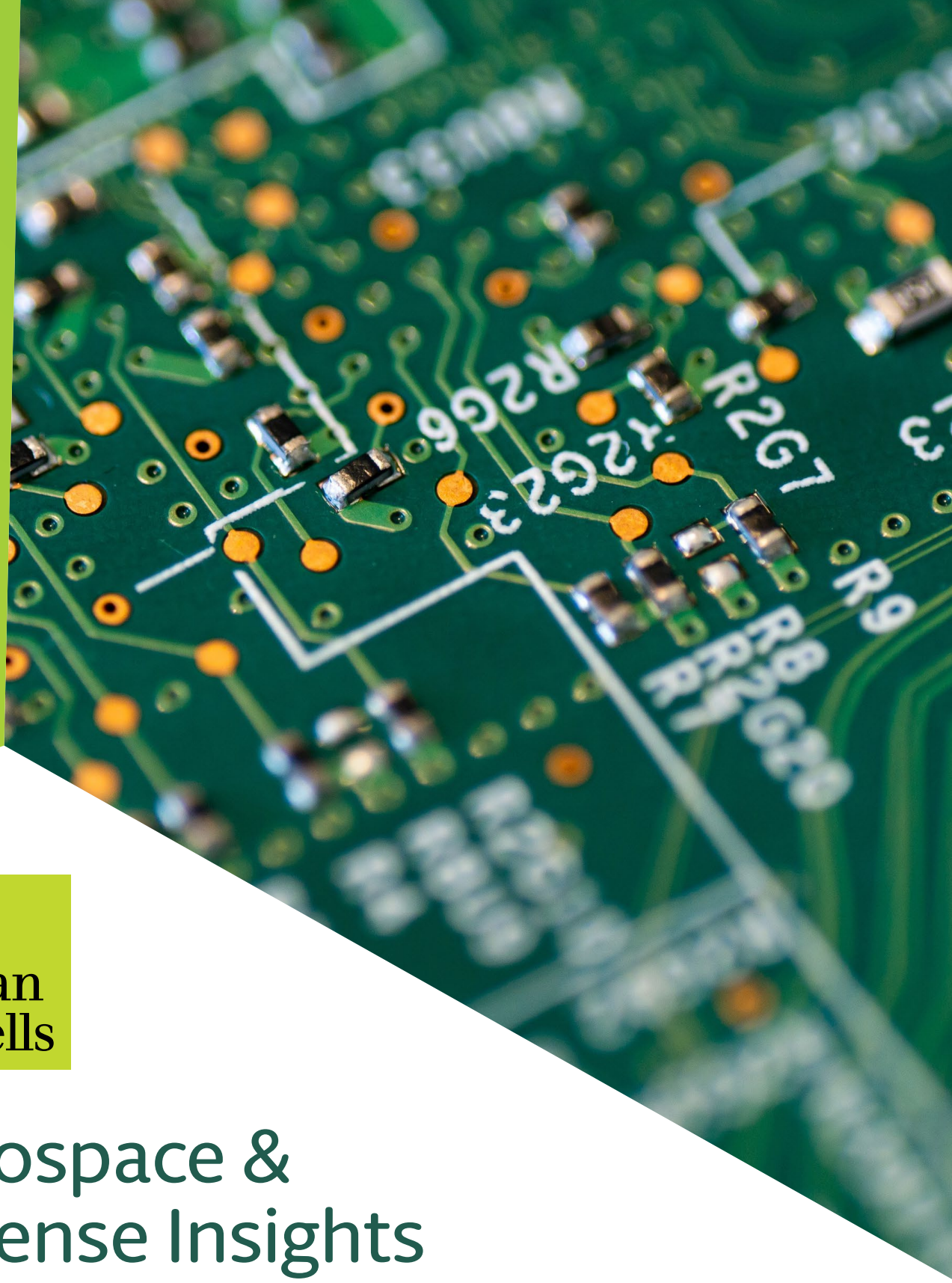


Hogan Lovells

Aerospace & Defense Insights

Top cybersecurity developments for A&D companies

Michael Mason, Michael Scheimer, Stacy Hadeka, and Rebecca Umhofer.

Through Aerospace & Defense Insights, we share with you the top legal and political issues affecting the aerospace and defense (A&D) industry. Our A&D industry team monitors the latest developments to help our clients stay in front of issues before they become problems, and seize opportunities in a timely manner.

On March 21, 2022 President Biden warned that Russia may conduct malicious cyberattacks on U.S. entities in retaliation for U.S. sanctions and support for Ukraine, and called on U.S. companies to "harden your cyber defenses immediately."

This also came on the heels of the Cybersecurity and Infrastructure Security Agency's (CISA's) "Shields Up" advisory, warning of malicious cyber activity against the U.S. homeland and the Intelligence Community's alert warning of Russia targeting cleared defense contractor networks. These heightened cyber threats underscore the importance of the ongoing, substantial efforts to improve the nation's cyber defenses. Many of those efforts were initiated by a May 12, 2021 Executive Order (EO) issued by President Biden. But the U.S. Department of Defense (DoD), Congress and the Department of Justice have also taken action over the past year to fortify protection of the U.S. government's digital assets. Below, we review key cybersecurity developments over the past year that impact companies operating in the aerospace and defense industry.

Biden cybersecurity executive order

On May 12, 2021, President Biden issued an Executive Order (EO) calling for "bold changes" to how the public and private sectors protect the nation's infrastructure from cyberattacks. EO 14,028 *Improving the Nation's Cybersecurity* outlines dozens of actions that federal agencies must take, many of which signal changes for federal contractors and may even trickle down to the private sector. The EO issuance followed the SolarWinds, Microsoft Exchange, and Colonial Pipeline hacks, and has been underscored more recently by U.S. satellite communications provider Viasat's report that its broadband services across central and

eastern Europe were disrupted by a cyberattack that began February 24, 2022 — the day of the Russian invasion of Ukraine.

The EO calls for a diverse set of actions, many of which will take some time to fully implement. We review the current status of those most relevant to aerospace and defense companies below.

Critical software

Section four of the EO describes a key effort to enhance security of software used by the federal government, with a particular focus on the security and integrity of "critical software." While the EO broadly described "critical software" as "software that performs functions critical to trust (such as affording or requiring elevated system privilege or direct access to networking and computing resources)," the EO also directed the National Institute of Standards and Technology (NIST) to publish the formal definition of "critical software." NIST did so on June 24, 2021 defining critical software as "any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:

a) Is designed to run with elevated privilege or manage privileges;

b) Has direct or privileged access to networking or computing resources;

c) Is designed to control access to data or operational technology;

d) Performs a function critical to trust; or

e) Operates outside of normal trust boundaries with privileged access."

This definition applies to all forms of software (*e.g.*, standalone software, software integral to specific devices or hardware components, cloud-based software) purchased for, or deployed in, production systems and used for operational purposes.

The EO further directs NIST to issue guidance on security measures for critical software, and directs the Office of Management and Budget (OMB) to require agencies to comply with that guidance. On July 8, 2021, NIST issued guidance about security measures for critical software, and OMB then published a memorandum on August 10, 2022 instructing how executive departments and federal agencies should implement those security measures. The OMB memo instructs agencies to implement the security measures in phases, focusing first on "standalone, on-premise software that performs security-critical functions or poses similar significant potential for harm if compromised." The OMB memo indicates this would include applications that provide these services:

- identity, credential, and access management (ICAM);
- operating systems, hypervisors, container environments;
- web browsers;
- endpoint security;
- network control;
- network protection;
- network monitoring and configuration;
- operational monitoring and analysis;
- remote scanning;
- remote access and configuration management; and
- backup/recovery and remote storage.

The OMB memo requires that all agencies implement the security measures designated by NIST for the above categories within one year (by August 10, 2023). Subsequent phases of implementation are to be determined by CISA and will include:

- software that controls access to data;
- cloud-based and hybrid software;
- software development tools, such as code repository systems, testing software, integration software, packaging software, and deployment software;
- software components in boot-level firmware; and
- software components in operational technology (OT).

Software supply chain security

The EO also calls on NIST to issue guidance identifying practices that enhance software supply chain security. To this end, on September 30, 2021, NIST issued a draft update to the Secure Software Development Framework (SSDF); NIST issued a final version of February 3, 2022. The SSDF identifies a "set of fundamental, sound practices for secure software development" and "defines only a high-level subset of what organizations may need to do, so organizations should consult the references and other

resources for additional information on implementing the practices." NIST also notes that the SSDF focuses on outcomes of the identified sound practices rather than on specific tools, techniques, and mechanisms to reach these outcomes.

NIST also revised Special Publication (SP) 800-161 Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* in October 2021, and issued a final version on May 5, 2022. The prior draft of this publication was released in April 29, 2021 before the May 12, 2021 EO. The revisions and final version include two new appendices that aim to respond to the EO: one that provides additional guidance to federal executive agencies related to supply chain risk assessment factors, assessment documentation, risk severity levels, and risk response; and a second that responds to the EO's directive that NIST outline existing industry standards, tools, and recommended practices.

Software bill of materials

The EO also directs the Secretary of Commerce to coordinate with the National Telecommunications and Information Administration (NTIA), to develop requirements for a Software Bill of Materials (SBOM). SBOMs are defined by the EO as "formal record[s] containing the details and supply chain relationships of various components used in building software," and software developers will need to provide SBOMs to government purchasers. The Department of Commerce and NTIA jointly published minimum elements for a SBOM on July 12, 2021. The minimum elements fall into three broad areas: (1) Data Fields: Documenting baseline information about each component that should be tracked; (2) Automation Support: Allowing for scaling across the software ecosystem through automatic generation and machine-readability; and (3) Practices and Processes: Defining the operations of SBOM requests, generation and use. More information about SBOMs is available at Nita.gov/SBOM.

Zero trust architecture

The EO requires agencies to develop their own plans for implementing a "zero trust architecture," which is a security model based on an acknowledgement that threats exist both *inside* and *outside* traditional network boundaries. Networks should be designed in a way to require "continuous verification" throughout the system and therefore guard against internal threats, not only external ones, by denying an attacker that breaches a system the ability to roam freely (i.e., lateral movement) within the system.

On January 22, 2022, OMB released a federal strategy to move the U.S. Government toward a "zero trust" approach to cybersecurity. The strategy requires federal agencies to meet certain cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024.

The key goals outlined in the zero trust strategy are organized under five complimentary pillars of effort developed by CISA. The strategy specifies certain actions agencies should take in each of these areas:

- Identity: Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks.
- Devices: The Federal Government has a complete inventory of every device it operates and authorizes for Government use, and can prevent, detect, and respond to incidents on those devices.
- Networks: Agencies encrypt all DNS requests and HTTP traffic within their environment, and begin executing a plan to break down their perimeters into isolated environments.
- Applications and Workloads: Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports.
- Data: Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies are taking advantage of cloud security services to monitor access to their sensitive data, and have implemented enterprise-wide logging and information sharing.

OMB's Federal Zero Trust Strategy notes that "[a] key tenet of a zero trust architecture is that no network is implicitly considered trusted—a principle that may be at odds with some agencies' current approach to securing networks and associated systems." The Strategy says that "[w]hile the concepts behind zero trust architectures are not new, the implications of shifting away from 'trusted networks' are new to most enterprises, including many Federal agencies," and

this "will be a journey for the Federal Government, and there will be learning and adjustments along the way as agencies adapt to new practices and technologies."

DoD, which published its own Zero Trust Reference Architecture in April, 2021, has announced that it awarded a $6.8 million contract to Booz Allen Hamilton to develop a prototype of a new security model based on zero trust principles.

FAR rulemakings

The EO directs the FAR Council to publish for public comment proposed contract language to address, among others: standardizing security incident reporting provisions government-wide; standardized common cybersecurity contractual requirements; and cybersecurity information-sharing with the federal government.

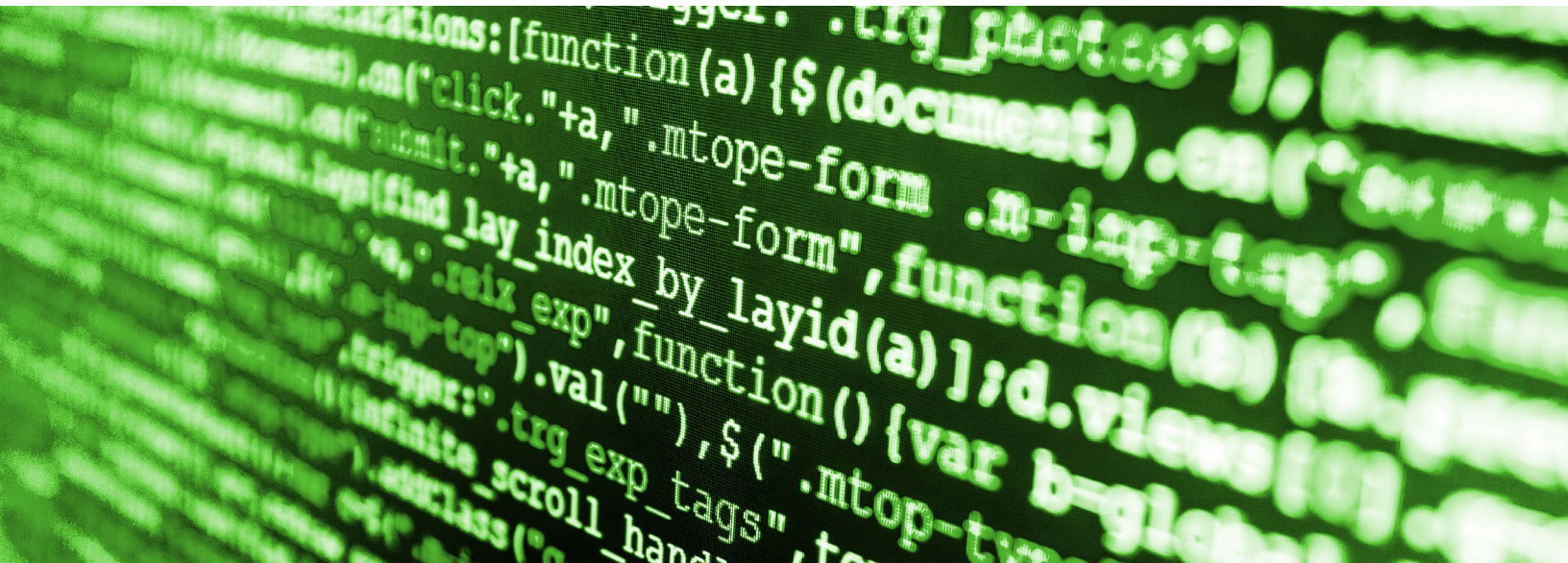
According to the EO, "current cybersecurity requirements for unclassified system contracts are largely implemented through agency-specific policies and regulations, including cloud-service cybersecurity requirements. Standardizing common cybersecurity contractual requirements across agencies will streamline and improve compliance for vendors and the Federal Government."

EO Section 2(i) directs the Department of Homeland Security (DHS) to "review agency-specific cybersecurity requirements that currently exist as a matter of law, policy, or contract and recommend to the FAR Council standardized contract language for appropriate cybersecurity requirements. Such recommendations shall include consideration of the scope of contractors and associated service providers to be covered by the proposed contract language."

The EO also directs OMB to evaluate current contract terms and restrictions of companies offering the federal government information technology (IT) and OT services to remove barriers to sharing "cyber threat and incident information" with agencies responsible "for investigating or remediating cyber incidents such as CISA, the Federal Bureau of Investigation (FBI) and the intelligence community.

These reviews are underway:

- FAR Case 2021-019, *Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems*, will standardize common cybersecurity contractual requirements across agencies for unclassified federal information systems, pursuant to DHS recommendations in accordance with sections 2(i) and 8(b) of the EO. On May 4, 2022, the Defense Acquisition Regulations Council (DARC) agreed to draft the proposed FAR rule.
- FAR Case 2021-017, *Cyber Threat and Incident Reporting and Information Sharing*, will increase cyber threat and incident information sharing between the Government and certain providers, pursuant to OMB recommendations, in accordance with EO Sections 2(b)-(c), and DHS recommendations, in accordance with EO Section 8(b). In addition, the rule will require certain contractors to report cyber incidents to the Federal Government to facilitate effective cyber incident response and remediation, DHS recommendations in accordance with EO Section 2(g)(i). As of May 20, 2022, the Defense Acquisition Regulations and FAR staff are resolving open issues on the draft proposed FAR rule.



DoD Modifies the cybersecurity maturity model certification framework

DoD announced its strategic direction for the Cybersecurity Maturity Model Certification (CMMC) program on November 4, 2021. The "CMMC 2.0" program maintains the program's original goal of safeguarding Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) shared with and handled by DoD contractors and subcontractors on contractor information systems through a unified cybersecurity standard and certification program. DoD first introduced CMMC 1.0, in January 2020 (see our prior discussion of CMMC 1.0 here). The November 2021 announcement marked the completion of an internal review and the implementation of an enhanced CMMC 2.0 program that simplifies the previously articulated CMMC standard and provides additional clarity on cybersecurity regulatory, policy, and contracting requirements. CMMC 2.0 focuses the most advanced cybersecurity standards and third-party assessment requirements on companies supporting the highest priority programs and increase DoD oversight of professional and ethical standards in the assessment ecosystem (see our prior write-up on the CMMC 2.0 changes here).

The announcement of the CMMC 2.0 program paused implementation of a previously published interim rule (see our previous comments on the rule here) that went into effect on November 30, 2020. That rule created a new Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7021, *Cybersecurity Maturity Model Certification Requirements*, while implementing a five-year phase-in piloting strategy with the goal to include CMMC requirements in all DoD contracts by 2026. However, a November 2021 advanced notice of proposed rulemaking suspended the CMMC piloting efforts and explained that no CMMC requirement will be included in DoD solicitations until the CMMC 2.0 program is fully implemented through the rulemaking processes, including through rulemaking to title 32 of the Code of Federal Regulations (CFR) and title 48 of the CFR, which is expected by May of 2023.

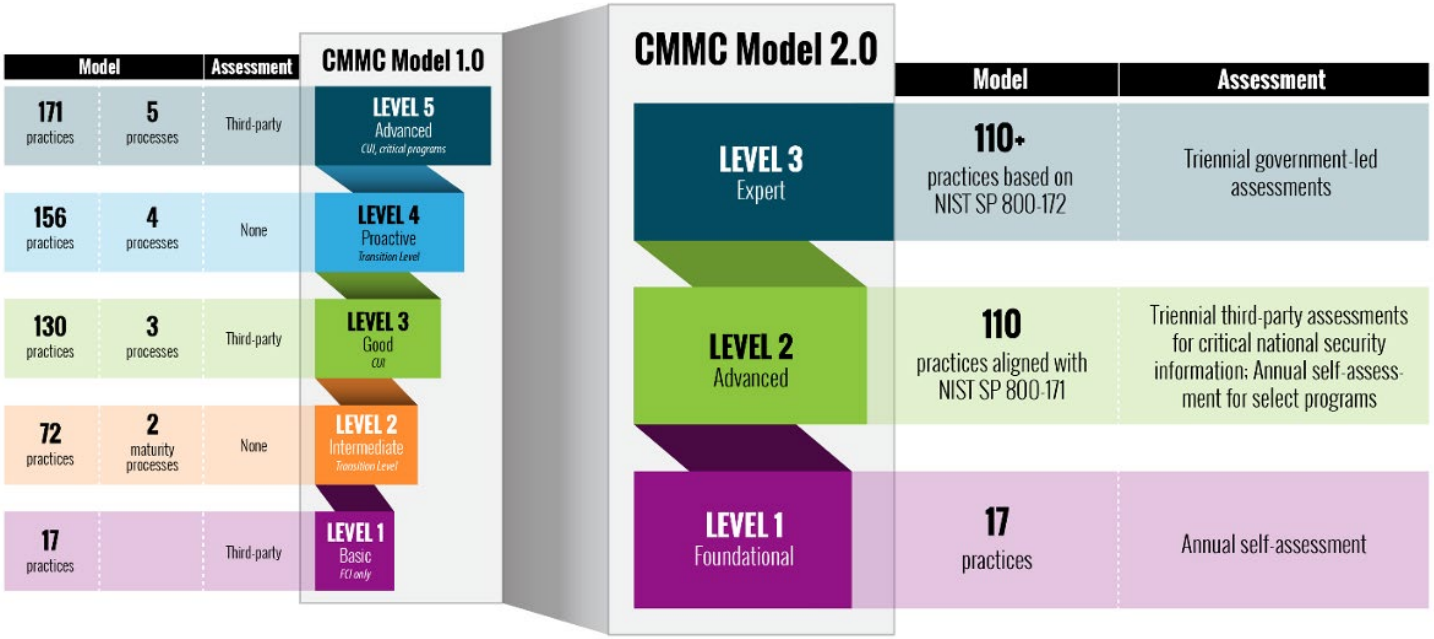
The CMMC 2.0 program eliminates two levels of cybersecurity maturity described in the original

CMMC 1.0 program – CMMC 1.0 levels 2 and 4 – to streamline the existing framework into ***three*** increasingly progressive levels, depending on the type and sensitivity of information the company handles. These levels now align with NIST cybersecurity standards (rather than CMMC-unique security practices) and focus the most stringent requirements on those companies supporting DoD's highest priority programs.

- **Level 1 – Foundational**: Level 1 largely tracks the prior Level 1 under CMMC 1.0 and requires adherence to the standards in FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems. Level 1 no longer requires CMMC Third Party Assessment Organization (C3PAO) assessments – instead, contractors demonstrate Level 1 compliance through annual self-assessments and affirmations by senior company officials.
- **Level 2 – Advanced**: The revamped Level 2 largely aligns with the former Level 3, and maps directly to the 110 security requirements listed in NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. Level 2 is now bifurcated to distinguish between "prioritized acquisitions" and "non-prioritized acquisitions," depending on whether the company handles information deemed critical to national security.
  - — Level 2 companies that handle such critical information ("prioritized acquisitions") must undergo, on a triennial basis, an independent third-party assessment by the C3PAOs.
  - — Level 2 companies that do not handle critical information ("non-prioritized acquisitions") may demonstrate compliance through annual self-assessments and company affirmations.
- **Level 3 – Expert**: Level 3 is based off of the former Level 5. It now largely relies on NIST SP 800-172, which supplements the 110 controls contained in NIST SP 800-171 by providing enhanced cybersecurity controls to protect controlled unclassified information associated with a critical program or a high value asset from advanced persistent threats. Contractors will be subject to government-led assessments occurring on a triennial basis.

CMMC 2.0 will allow contractors, under certain circumstances, to work towards achieving CMMC certification through a Plan of Action and Milestones (POA&Ms). Under CMMC 1.0, contractors were required to obtain certification demonstrating total compliance at their desired CMMC level (without any open / unresolved action items on a POA&M).

CMMC 2.0 will introduce a selective, time-bound waiver process for certain acquisitions. Senior DoD leadership approval is required for such waivers, indicating they will not be available on a wide basis.



Developments in the National Controlled Unclassified Information (CUI) program

On September 14, 2016, the National Archives and Records Administration (NARA) released its CUI Final Rule, codified at 32 C.F.R. Part 2002, *Controlled Unclassified Information*, which formally identifies the approved categories and subcategories of federal CUI, establishes the official CUI Registry, and prescribes the use of NIST SP 800-171 when CUI will reside on non-federal information systems. However, after five years, DoD is still the only agency explicitly mandating in its acquisition regulations that its covered contractors follow NIST SP 800-171 (as required in the NARA rule) for safeguarding CUI on *contractor systems*.

FAR case 2017-016 controlled unclassified information

NARA announced in a November 12, 2021 blog post that "one of the highest priorities of the CUI Executive Agent is getting a CUI FAR clause issued." The long anticipated FAR clause "will create a common mechanism to communicate which information contractors create for and receive from the Federal Government must be protected, how to protect it, and who it can be shared with…will be a standard vehicle for conveying whether CUI is involved in the contract and what the existing requirements are for safeguarding it [and] Contractors and Government officials will know the place in any solicitation or contract to find this information." A draft proposed rule was sent to OMB's Office of Information and Regulatory Affairs on February 24, 2022 and is still under review.

Updates to NIST 800-171 and NIST 800-172

NIST SP 800-171 establishes the 110 baseline security standards for government contractors that process, store, or transmit CUI. Revisions to this standard are tied to those associated with NIST SP 800-53. NIST SP 800-53 Revision 5 was published in September 2020, seven months ***after*** the last update to SP 800-171 (Revision 2). As a result, NIST is in the process of determining what changes need to made to SP 800-171 to align with the updated controls in SP 800-53, and anticipates publishing SP 800-171 Revision 3 sometime in 2022.

Separately, as part of its overhaul of CMMC (discussed above), DoD has said it has plans to propose additional controls from its old CMMC model for inclusion in the next update to NIST SP 800-171. As part of the CMMC 2.0 reorganization, DoD consolidated the number of maturity levels from five to three and removed the 20 controls that go beyond SP 800-171 from the new level two. However, DoD has stated that some of those requirements will be proposed to NIST for inclusion in the next revision of NIST SP 800-171 with the end result that they will become part of the technical standards baseline itself (*i.e.*, listed in NIST SP 800-171) rather than layered on by the CMMC program.

On July 6, 2020, NIST published draft SP 800-172, a companion publication to SP 800-171 that includes additional protections for CUI from advanced persistent threats (APTs). The final version of SP 800-172 was released in February 2021. While SP 800-171 is focused on ***confidentiality***, the enhanced controls in SP 800-172 address protecting the ***confidentiality***, ***integrity***, and ***availability*** of CUI on contractor information systems from APT. Agencies are expected to identify and selectively apply enhanced security SP 800-172 protections in addition to the basic and derived requirements in SP 800-171. A decision to select a particular set of enhanced security requirements from SP 800-172 should be based on the specific mission and business protection needs of the agency, and informed by ongoing risk assessments. Moreover, as noted above, DoD will leverage a subset of these safeguards when implementing CMMC 2.0 Level 3.

In April 2021, NIST published draft SP 800-172A, *Assessing Enhanced Security Requirements for Controlled Unclassified Information*, which will provide federal agencies and nonfederal organizations with assessment procedures that can be used to carry out assessments of the enhanced requirements in SP 800-172. NIST published the final version of SP 800-172A on March 15, 2022.

Congress has some unsettled cyber business

The National Defense Authorization Act (NDAA) for FY 2021 (H.R. 6395) reauthorized the U.S. Cyberspace Solarium Commission through December 2021. Although the Commission officially sunset on December 21, 2021, the involved lawmakers have publicly affirmed their intention to continue pursuing some of the commission's initiatives as part of a new "Solarium 2.0" nonprofit organization.

The Commission was charged with monitoring federal implementation of prior cybersecurity policy recommendations, as well as revising, amending, or making additional recommendations to advance the nation's strategic approach to cybersecurity.

The Commission's August 12, 2021 Annual Report on Implementation highlights numerous achievements but notes that several key initiatives remain in limbo pending much-needed appropriations and ongoing congressional negotiations. These include efforts to (1) establish dedicated congressional committees on cybersecurity; (2) enact a national data security and privacy protection law; (3) develop public-private partnerships to share threat intelligence, and establishing a federal cyber statistics bureau to create much-needed incident response data for use in policy decision-making.

Cyber-related enforcement is a high priority

On October 6, 2021, DOJ announced a Civil Cyber-Fraud Initiative through which DOJ will use the False Claims Act (FCA) to target cybersecurity-related fraud by government contractors and grant recipients. Although it does not impose new regulatory or legal requirements, it signals a new focus and prioritization of resources by DOJ to improve cybersecurity across the government, the public sector, and at key "industry partners."

Although government contractors have long been prime targets for FCA whistleblowers, this new DOJ initiative further elevates this risk. It's important to note that the FCA imposes liability not only on a prime contractor or direct grant recipient, but it applies to any entity, including subcontractors, whose conduct causes a false claim to be presented to the United States for payment or approval. Although prime contractors or grant recipients typically submit claims for payment directly to the government on behalf of their subcontractors, a subcontractor that causes a prime contractor or recipient to present a false claim for payment can be held liable for FCA damages and penalties.[1]

On March 8, 2022, DOJ announced its first resolution of an FCA case involving alleged cyber fraud since Civil Cyber-Fraud Initiative began. In that case, a health services provider that provided medical services at State Department and Air Force facilities in Iraq and Afghanistan agreed to pay $930,000 to resolve allegations that, among other things, it failed to disclose that it had not complied with contractual requirements to store all patients' medical records on a secure electronic medical record system.

Another long-running case, which was recently settled, underscores the risk that failure to disclose noncompliance with contract clauses related to cybersecurity may give rise to FCA liability. In *United States v. Aerojet Rocketdyne Holdings*, the United States District Court for the Eastern District of California denied the defendant's motion for summary judgment as to promissory fraud FCA claim that asserts the defendant secured government contracts while failing to disclose noncompliance with cybersecurity-related contract clauses.[2] Among other things, the court found issues of fact as to whether noncompliance with government's cybersecurity requirements found in DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, and NASA FARS 1852.204-76, *Security Requirement for Unclassified Information Technology Resources*, are material to the government's decisions to approve contracts.[3] Before this case was able to make it to trial, it was settled on April 26, 2022.

In addition to tracking cases associated with DOJ's Civil Cyber-Fraud Initiative, aerospace and defense companies should see our prior article on FCA cybersecurity-related risk here.

What's next

Over the past year, there have been several developments related to cybersecurity impacting the aerospace and defense industry. As noted above, we have begun to see more concrete efforts by the federal government as a result of the Biden Cybersecurity EO, while we expect additional updates to the FAR, DFARS, and NIST SPs within the coming year. We also expect to see an uptick in whistleblower cases and enforcement actions. Here are five key cybersecurity takeaways for government contractors in the aerospace and defense industry sector:

1. Monitor and implement the actions coming out of the Biden Cybersecurity EO, if applicable. Currently, companies should be familiarizing themselves with the critical software, software supply chain, SBOM, and zero trust architecture updates. Companies should also be tracking new FAR rules implementing the EO.
2. Get prepared in advance for CMMC 2.0. Although CMMC 2.0 will not be a contractual requirement until DoD completes rulemaking to implement the program, companies are encouraged to self-assess their compliance or seek early certification if available.
3. Understand requirements for safeguarding CUI, adopt and implement a CUI program if applicable, and monitor agency-specific and government-wide requirements for CUI protection.
4. Follow Congressional actions and outstanding key initiatives of the Cyberspace Solarium 2.0.
5. Track FCA litigation developments regarding DOJ's Civil Cyber-Fraud Initiative.

Michael Mason
Partner | Washington, D.C.
T: +1 202 637 5499
E: mike.mason@hoganlovells.com

Michael Scheimer
Partner | Washington, D.C.
T: +1 202 637 6584
E: michael.scheimer@hoganlovells.com

Stacy Hadeka
Counsel | Washington, D.C.
T: +1 202 637 3678
E: stacy.hadeka@hoganlovells.com

Rebecca Umhofer
Senior Knowledge Lawyer | Washington, D.C.
T: +1 202 637 6939
E: rebecca.umhofer@hoganlovells.com

References

1. *See* 31 U.S.C. § 3729(a)(1); *United States v. Bornstein*, 423 U.S. 303, 309 (1976) ("It is settled that the Act . . . gives the United States a cause of action against a subcontractor who causes a prime contractor to submit a false claim to the Government.").
2. *See* No. 2:15-CV-02245 WBS AC, 2022 WL 297093 (E.D. Cal. Feb. 1, 2022), reconsideration denied, No. 2:15-CV-02245 WBS AC, 2022 WL 815823 (E.D. Cal. Mar. 17, 2022).
3. *Id.* at *7.

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dublin
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.

*Our associated offices
Legal Services Center: Berlin

www.hoganlovells.com