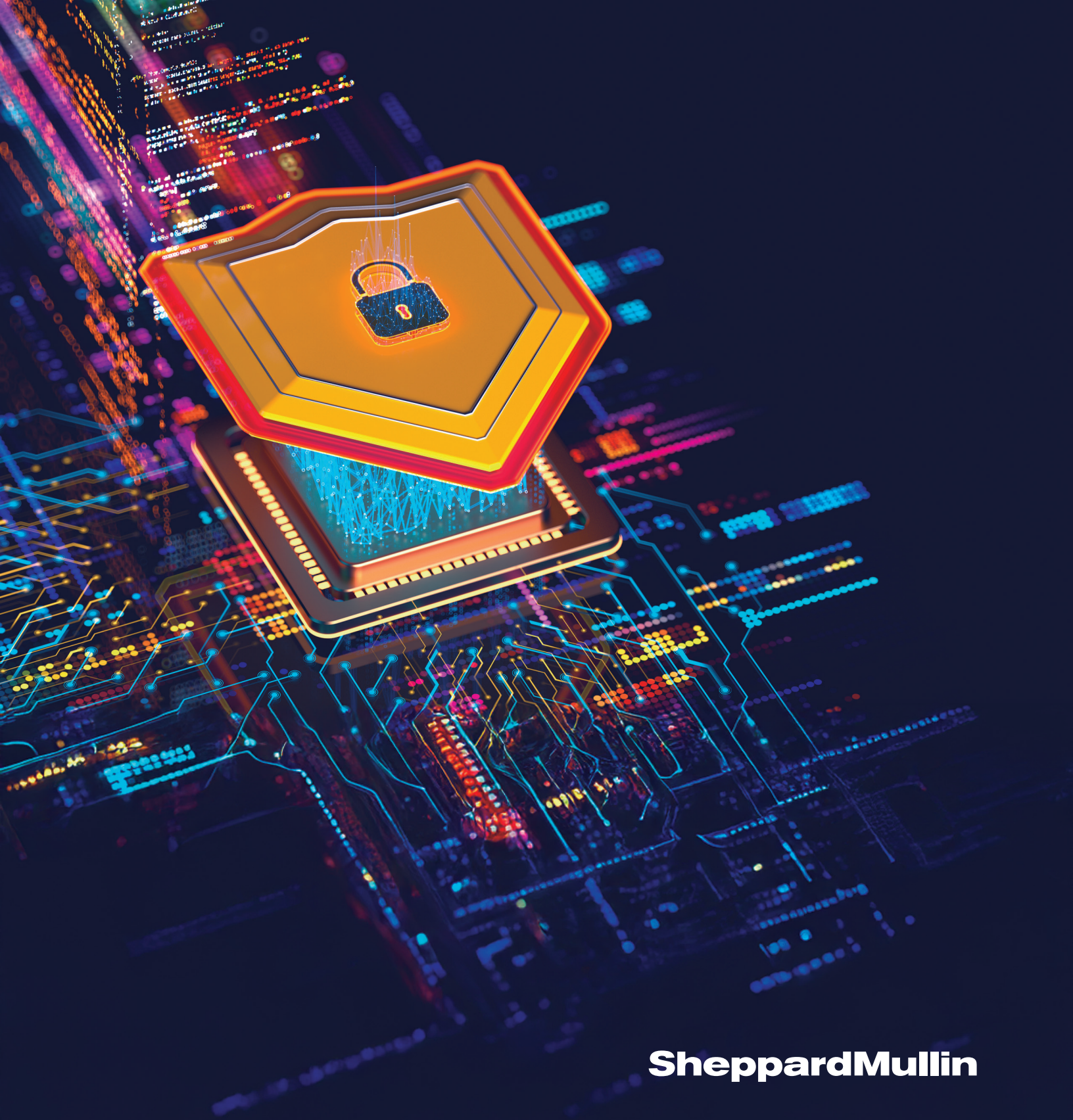


SheppardMullin

Governmental Practice
Cybersecurity and Data Protection

2024 Recap & 2025 Forecast Alert

Governmental Practice Cybersecurity and Data Protection

2024 Recap & 2025 Forecast Alert

To kick off the New Year (and as is now tradition, since we put out a similar Recap & Forecast last year), Sheppard Mullin's Governmental Practice Cybersecurity & Data Protection Team has prepared a cybersecurity-focused 2024 Recap (highlighting major updates and including links to the resources we put out over the past year) and a 2025 Forecast (previewing what we expect to see in 2025). This Recap & Forecast covers the following six high-interest topic areas relating to cybersecurity and data protection:

(01) DoD and CMMC

(02) FAR Updates & Software Security

(03) FedRAMP & Security in the Cloud

(04) Artificial Intelligence

(05) Critical Infrastructure Reporting & National Security

(06) Cybersecurity Fraud & Enforcement

AUTHORS

Townsend Bourne
Team Leader, Partner
202.747.2184
tbourne@sheppardmullin.com
Bio

Nikki Snyder
Team Deputy, Associate
202.747.3218
nsnyder@sheppardmullin.com
Bio

Daniel Alvarado
Associate
202.747.2325
dalvarado@sheppardmullin.com
Bio

Lillia Damalouji
Associate
202.747.2307
ldamalouji@sheppardmullin.com
Bio

Jordan Mallory
Associate
202.747.1866
jmallory@sheppardmullin.com
Bio

Patrick Amano Dolan
Associate
202.747.1891
pdolan@sheppardmullin.com

Sidney Howe
Cybersecurity Fellow
202.747.1886
showe@sheppardmullin.com

CONTENTS

01

DoD and CMMC

DFARS and CMMC

Throughout 2024, we closely followed updates relating to the DoD's Cybersecurity Maturity Model Certification (CMMC) program as well as the development of three Defense Federal Acquisition Regulation Supplement (DFARS) cybersecurity updates (currently styled as "DFARS Cases" while in development). These relate to safeguarding and reporting requirements, data security assessments, and implementation of the CMMC program.

DFARS Cases Relating to Cybersecurity

- **Updates to the Safeguarding Covered Defense Information and Cyber Incident Reporting Clause (DFARS Case 2023-D024)** – This will amend the existing clause at DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, to incorporate references to NIST SP 800-172 requirements (for the small percentage of defense contractors with the most strict security requirements), harmonize certain terminology in line with the CMMC program, address international agreements, and streamline the vendor identification process. The update will come in the form of a proposed rule, with a current deadline of January 8, 2025 (though these deadlines often get pushed back).

- **NIST SP 800-171 DoD Assessment Requirements (DFARS Case 2022-D017) –** This rule was split from the DFARS Case below to implement the NIST SP 800-171 DoD Assessment Methodology, which requires certain DoD contractors to conduct self-assessments and enables the DoD to assess contractor implementation of the cybersecurity requirements in NIST SP 800-171. The requirements of this rule are currently effective per DFARS 252.204-7019 and -7020. We discussed the related Interim Rule (which was published in 2020) here. The most recent status update indicates that the draft final rule report is due to the DARC Director on January 22, 2025.

- **Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041) –** This amends an interim rule to implement the CMMC framework 2.0 in the DFARS. The CMMC framework assesses compliance with applicable information security requirements and this rule aims to provide the DoD with assurances that a DIB contractor can adequately protect unclassified information at a level commensurate with the risk, accounting for information flow down to its subcontractors and service providers in a multi-tier supply chain. As of November 13, 2024, the DARC Director tasked the Acquisition Technology & Information Committee to review the public comments and draft a final rule. This report was originally due on December 4, 2024 but was extended until January 8, 2025.

The CMMC Program

The CMMC program has been in the works for some time. By way of brief recap, here are major milestones in the development of the program:

January 30, 2020

The CMMC program is first introduced, we wrote about this here.

September 29, 2020

An Interim Rule implementing the CMMC Program in the DFARS in published, which we discussed here.

March 2021

DoD initiates an internal review of CMMC.

November 2021

"CMMC 2.0" is announced, based on review of over 850 public comments received in response to the September 2020 Draft CMMC rule. We wrote about the key differences between CMMC 1.0 and 2.0 here.

December 26, 2023

Proposed CMMC Program Rule (under Title 32) is published, we wrote about this here.

August 15, 2024

Proposed Rule implementing CMMC Program in the DFARS (under Title 48) is published, as we discussed here.

October 15, 2024

Final CMMC Program Rule is published in Title 32, we wrote about this here.

December 16, 2024

The CMMC program (under 32 CFR Part 170) officially went into effect. The Cyber AB also published two long-awaited sister resources, the CMMC Assessment Process (CAP) guide and the CMMC Code of Professional Conduct (CoPC).

IMPORTANT REMINDER

Remember, the CMMC 48 CFR Part 204 Proposed Rule (which will implement CMMC requirements in the DFARS, thus making it binding on DoD contractors) remains in the rulemaking process. The CMMC program will not be effective for DoD contractors until this DFARS rule is published and effective.

As noted above, the past year saw key developments in two CMMC Rulemakings. First, on August 15, 2024, the DoD published the proposed rule to implement the CMMC Program in the DFARS ("DFARS Title 48 Rule"). This DFARS Title 48 Rule went through a public comment period and we are currently waiting for publication of an associated final rule, which will trigger requirements for DoD contractors. Separately, the DoD published the final version of its CMMC Program Rule in Title 32 of the Code of Federal Regulations effective December 16, 2024, which updates the DoD's national security regulations). Implementation of the first phase of CMMC will occur on the effective date of the complementary DFARS Title 48 Rule, which is still pending.

Final CMMC Program Rule in Title 32

Following the publication of the proposed CMMC Program Rule in December 2023, the DoD reviewed hundreds of public comments and made several key updates. The Final CMMC Program Rule, effective December 16, 2024, includes several notable changes. It revises the timeline for the four-phase roll-out (extending Phase 1 from six months to one year), updates assessment requirements for Security Protection Assets and Data, and provides welcome clarification regarding treatment of External Service Providers. See our in-depth analysis here.

In addition, as a result of the Final CMMC Program Rule effective date, the Cyber AB (an independent, non-profit organization responsible for supporting the CMMC Program, including serving as the sole accreditation body for CMMC) released new materials relating to third-party assessments:

- The CMMC Assessment Process (CAP) is the official procedural guide for CMMC Third Party Assessment Organizations (C3PAOs) conducting a CMMC Level 2 certification assessment for an Organization Seeking Certification (OSC). The CAP is published and maintained by the Cyber AB and reviewed and approved by the CMMC Program Management Office. It is a resource for the entire CMMC Ecosystem, including DIB companies and organizations. The purpose of the CAP is to ensure the consistency and integrity of CMMC Level 2 certification assessments.
- The CMMC Code of Professional Conduct (CoPC) establishes the ethical and professional standards required for participants operating within the CMMC Ecosystem, as well as the procedures for investigating and adjudicating violations of the CoPC. It also provides guidance for CMMC Ecosystem participants on navigating prospective conflicts-of-interest and other impartiality issues.

Timeline for Phased CMMC Roll-Out

Phase	Phase 1	Phase 2	Phase 3	Phase 4 (Full Implementation)
Start Date	CMMC DFARS Rule effective date (estimated in Mid-2025).	One calendar year after Phase 1 begins.	One calendar year after Phase 2 begins.	One calendar year after phase 3 begins.
Impact	Inclusion of Level 1 (Self) or Level 2 (Self) requirement in applicable solicitations/contracts (as a condition of award).	Level 2 (C3PAO) (third party certification assessment) requirement in applicable solicitations/contracts (as a condition of award).	Level 2 (C3PAO) as a condition for exercising option periods; and Level 3 (DIBCAC) requirement for all applicable solicitations/contracts (as a condition of award).	Full implementation of the CMMC requirements in all applicable solicitations and contracts, including option periods.

Proposed Rule Implementing the CMMC Program in the DFARS.

While the Proposed Rule contained no major surprises, it includes a longer proposed DFARS 252.204-7021 clause, spelling out the obligations for contractors and subcontractors under the CMMC Program. The Proposed Rule sets forth certain requirements for contractors:

1. Have a current CMMC certificate or self-assessment at the requisite CMMC level, or higher;
2. Maintain the required CMMC level for the duration of the contract for all applicable information systems;
3. Only store, process, or transmit data in appropriate information systems;
4. Notify the Contracting Officer within 72 hours of any lapses in information security or changes in the status of CMMC certificate or self-assessment levels;
5. Complete and maintain on an annual basis, or when changes occur, an affirmation of continuous compliance with the security requirements;
6. Ensure all subcontractors and suppliers complete and maintain on an annual basis, or when changes occur, an affirmation of continuous compliance with the security requirements;
7. Report (a) the unique identifiers issued by DoD for each information system included in SPRS; (b) the results of contractor self-assessments in SPRS; and (c) any changes to the list of unique identifiers.

We discuss notable updates, including the new notification requirement, here. Note it is possible these requirements could change in the final version of the DFARS CMMC rule as a result of public comments. As a reminder, Phase 1 of the CMMC Program will begin on the effective date of this final rule (estimated to be early to mid-2025).

What to Expect in 2025

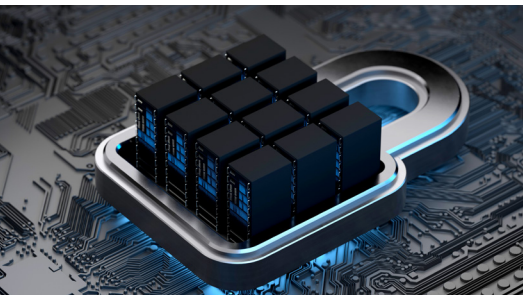
With the final version of the DFARS CMMC Rule expected in early to mid-2025, DoD contractors should focus seriously on CMMC compliance now (if they have not already) as preparing for and completing the assessment can take time. There is significant preparation that is necessary before completing the actual assessment, including identifying, negotiating with, and hiring a C3PAO, completing an in-depth scoping analysis of all entities to be assessed, and identifying any conflicts of interest. The CMMC program is new and complex, making it especially beneficial to consult experts. This is important because once the roll-out begins, contractors will be ineligible for award, and eventually for option periods or extension of performance, if they do not have the required CMMC level compliance in place. We also are interested to see how the change in administration will affect CMMC, if at all. Recently, there has been some pushback from Congress (including some lawmakers pushing a formal "disapproval" to overturn the CMMC rule), but we do not expect these CMMC critics to derail the program or materially change the implementation discussed above.

02

FAR Updates & Software Security

FAR Cybersecurity Updates

Throughout 2024, we closely followed the development of several FAR rules related to cyber and supply chain security. Below, we provide a short description and status of these forthcoming rules (styled as "FAR Cases" while in development) and an update on the recently published FAR Part 40 final rule, which establishes a new section of the FAR to consolidate regulations related to information security and supply chain security.



The forthcoming FAR rules, listed in chronological order from when the FAR Case was issued, include:

- ***Controlled Unclassified Information*** **(FAR Case 2017-016)** – This FAR Case has been on the books for years and will implement the National Archives and Records Administration (NARA) CUI program, which provides implementing regulations for safeguarding and handling of CUI and guidance for responding to breaches involving Personally Identifiable Information (PII). This rule seeks to establish uniform CUI program requirements for all federal contracts. After several years of radio silence, the proposed rule cleared regulatory review in October 2024 and we expect the rule to be published in the coming weeks. There will then be a public comment period before a final rule is issued.
- ***Implementation of Federal Acquisition Supply Chain Security Act (FASCSA) Orders*** **(FAR Case 2020-011)** – This rule implements Section 1323 of the SECURE Technology Act (Pub. L. 115-390) (FY19), which created the Federal Acquisition Security Council (FASC) and authorized issuance of exclusion and removal orders. These orders are issued to protect national security by excluding certain covered products, services, or sources from the Federal supply chain upon the recommendation of the FASC. This rule currently is in the "Final Rule Stage." The FASCSA interim rule was released in October 2023 (which we covered here and here) and the final rule is expected to be released in August 2025. The FAR Acquisition Technology Team is currently reviewing public comments and drafting the final FAR rule.
- ***Cyber Threat Incident Reporting and Information Sharing*** **(FAR Case 2021-017)** – This rule includes requirements to increase sharing of information about cyber threats and new incident reporting and response obligations. It is meant to apply to contractors that provide products or services to the Government that include information and communications technology and currently is in the "Final Rule Stage." The proposed rule was released in October 2023 alongside FAR Case 2021-019 (discussed below) and contains several new definitions, requirements, and representations relating to federal contractor cybersecurity, which we cover in depth here and here. The final rule was originally expected to be published in December 2024, though we anticipate it will likely be published in early 2025, with requirements to become effective soon after publication.

- ***Standardizing Cybersecurity Requirements for Federal Information Systems* (FAR Case 2021-019)** – This rule ensures Federal Information Systems maintained by contractors are better positioned to protect from cybersecurity threats by standardizing common cybersecurity contractual requirements. This rule is applicable to contractors that develop or operate a "Federal Information System" and currently is in the "Final Rule Stage." The proposed rule was released alongside the above FAR Case 2021-017 in October 2023 and the final rule is expected to be published in early 2025. This rule contains updated definitions, requirements, and representations relating to standardizing cybersecurity requirements for Federal Information Systems (covered more in depth here and here). The draft final FAR rule is currently being processed, which typically is the final step before publication. The requirements contained in this rule will become effective soon after the final rule is published.

- ***Supply Chain Software Security* (Case No. 2023-002)** – This rule implements Section 4(n) of Executive Order 14028 (on Improving the Nation's Cybersecurity), which requires software suppliers to comply with and attest to compliance with applicable secure software development requirements. This rule will apply to suppliers of software for purchase by agencies and currently is in the "Proposed Rule Stage," although a draft has not yet been publicly released (see more on this below).

- ***Prohibition on Unmanned Aircraft Systems from Covered Foreign Entities* (Case No. 2024-002)** – This rule implements the American Security Drone Act of 2023, which prohibits executive agencies from procuring or operating covered unmanned aircraft systems manufactured or assembled by certain covered foreign entities and is applicable to all solicitations and contracts. This interim FAR rule was published in November 2024 in the new FAR Part 40 (*see* FAR 40.202) and became effective upon publication as a national security measure to protect sensitive Government information and operations. The public comment period ends on January 13, 2025.

Final Rule – FAR Part 40, Information Security and Supply Chain Security

In April 2024, the FAR Council published the final rule that established the framework for the new FAR Part 40. This section will serve as a centralized location to cover the broad security requirements, policies, and procedures for managing information and supply chain security, which were previously dispersed across multiple parts of the FAR. We highlighted the key features of the final rule here.

In November 2024, FAR Part 40.202 was introduced as part of Case No. 2024-002 and became effective upon publication. As discussed above, this section generally prohibits executive agencies from procuring and operating certain unmanned aircraft systems from American Security Drone Act-covered foreign entities, with limited exceptions. Unless an exemption, exception, or waiver applies, this provision applies to ***all*** acquisitions, including contracts at or below the micro-purchase threshold and to contractor for commercial products or services. The applicable FAR clause at FAR 52.240-1 is a mandatory flow-down and must be inserted in all subcontracts.

What to Expect in 2025

While FAR 40.202 is the only new provision of substance contained in the FAR Part 40 framework thus far, we expect the FAR Council will begin to compile existing information security and supply chain security provisions from throughout the FAR into this framework throughout 2025 and may introduce other new provisions in this FAR Part as well.

Software Security

In 2024, the Biden Administration continued efforts to enhance the security of the software supply chain in furtherance of Executive Order 14028 (the "Cyber EO") (which we previously discussed here).

This year's major focus was on the Cyber EO's attestation requirement, which mandates that agencies only use software from suppliers that comply – and attest to compliance – with secure software development requirements.

Attestation Requirement

As a refresher, the Cyber EO mandated that the government take action to protect software – with a focus on "critical software" – against cyber-attacks. Among other things, the Cyber EO required the Government to provide a definition of "critical software"; to publish the minimum elements for a software bill of materials (SBOM); to publish guidelines for minimum standards for vendors' testing of software source code; and to recommend language to the FAR Council requiring suppliers of software to agencies to comply – and to attest to compliance – with such requirements via the Secure Software Development Attestation form (also known as the "Common Form"), which we've previously covered here, here, and here.

On March 11, 2024, the Cybersecurity and Infrastructure Security Agency (CISA) and the Office of Management and Budget (OMB) released the Common Form (which we covered here), currently being used by federal agencies to obtain attestations from software developers regarding the security of their products, in accordance with the Cyber EO and OMB Memoranda M-22-18 and M-23-16.

The most recent guidance from OMB (Memorandum M-23-16) directed agencies to collect attestations for "critical" software within 3 months of finalization of the Common Form, and within 6 months for all other software, which put pressure on agencies to collect attestation forms for critical software by June 8, 2024, and all other software by September 8, 2024.

Some agencies have reached out directly to companies demanding attestation forms outside of any contractual obligation, and the General Services Administration (GSA) issued an Acquisition Letter stating it would update its IT policies and begin collecting attestation forms for new contracts and the exercise of contract options starting June 8, 2024 for all software.

What to Expect in 2025

We are still awaiting finalization of the open FAR case (No. 2023-002), which implements Section 4(n) of the Executive Order, requiring "suppliers of software available for purchase by agencies to comply with, and attest to complying with, applicable secure software development requirements." The Executive Order and subsequent OMB memoranda are directed at agencies and are not binding on contractors. Companies may choose to provide the attestations upon request by agencies, but should consider the risks and benefits of doing so where they do not yet have a contractual or legal requirement in place. For those that have not yet provided any attestations, contractors should review the Common Form and consider the scope of attestations they and their suppliers may need to provide once these requirements are firmly in place.

03

FedRAMP & Security in the Cloud

Last year, we described 2023 as a transformative year for the Federal Risk and Authorization Management Program (FedRAMP), the federal government's program for security authorizations for cloud service offerings. This FedRAMP transformation continued in 2024, headlined by the Office of Management and Budget (OMB) publishing its final memorandum on modernizing FedRAMP. The FedRAMP Program Management Office (PMO) also published its roadmap with strategic goals for 2025 and released its final Emerging Technology Prioritization Framework. Additionally, it announced its Agile Delivery pilot program and a new technical documentation hub (automate.fedramp.gov) that focuses on providing support to cloud service providers in the development of digital authorization packages.

OMB Memo Modernizing FedRAMP

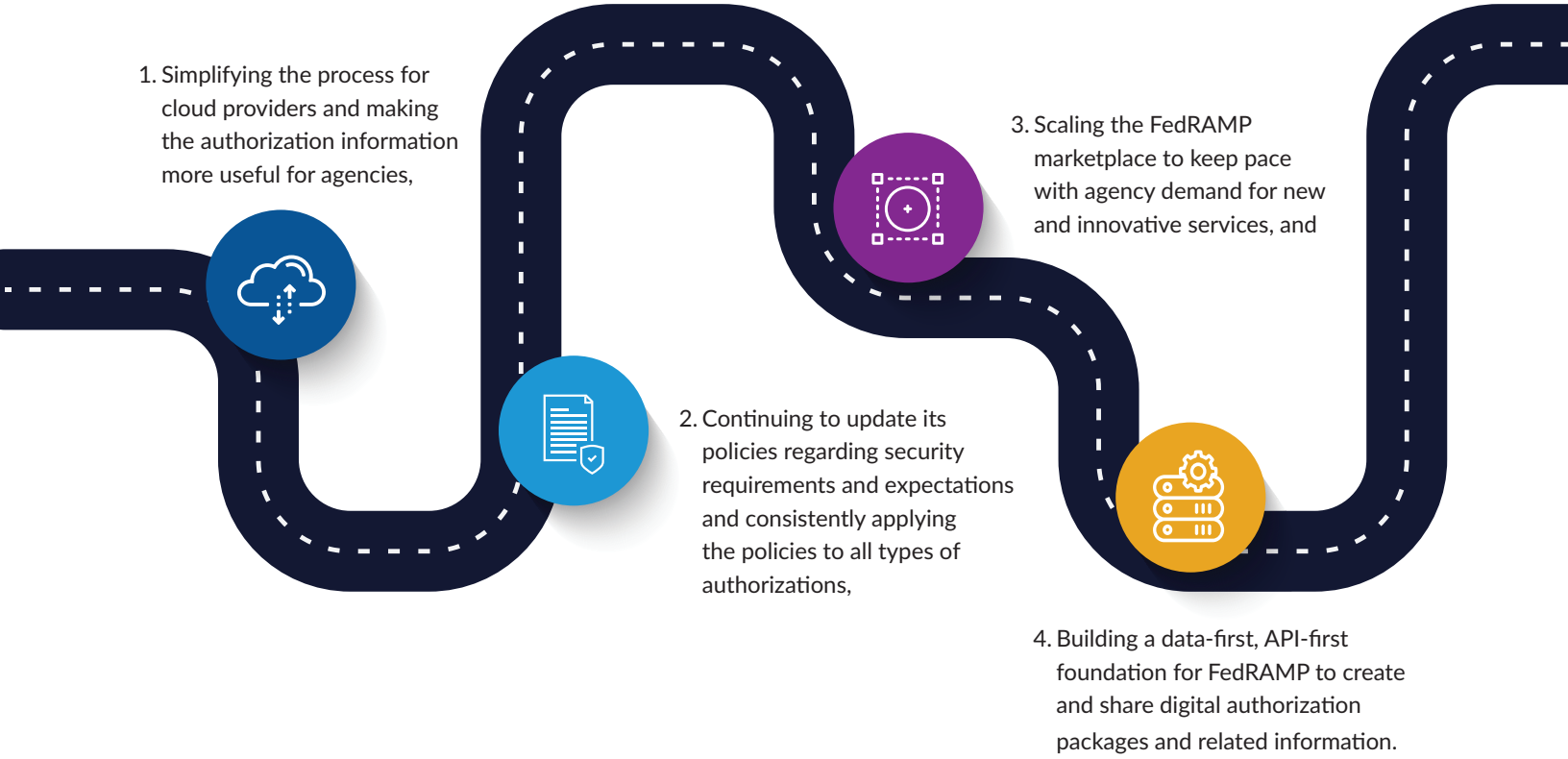
Following a nearly eight month review of 290 comments on its draft memo, the OMB published a final version of the FedRAMP OMB Memo. The OMB Memo revamps FedRAMP through changes to the authorization paths and continuous monitoring and incident response processes, as well as enhancements through automation. Below are a few key points from our article (check it out for more detail on the OMB Memo and other notable FedRAMP updates in 2024):

- The FedRAMP OMB memo emphasizes the need for federal agencies to leverage shared infrastructure.
- The FedRAMP OMB memo revamps the authorization paths, replacing the Joint Authorization Board (JAB) authorization path with a "program authorization" path.
- The FedRAMP PMO plans to use "red-team" assessments at any point during or following the FedRAMP authorization process.

Federal agencies had 180 days to update their agency-wide policies to align with the FedRAMP OMB Memo requirements and promote the use of cloud computing products and services that meet FedRAMP security requirements. Additionally, the FedRAMP OMB Memo prescribes 18 months for the General Services Administration (GSA) to enable authorization and continuous monitoring through machine-readable and automated means, and two years to ensure that governance, risk and compliance and system-inventory tools can ingest and produce artifacts using Open Security Controls Assessment Language (OSCAL). We will be monitoring progress on these deadlines in 2025.

FedRAMP Strategic Goals Roadmap

On March 28, 2024, FedRAMP published a roadmap that outlines FedRAMP's strategic goals for 2025. Additionally, the roadmap seeks to respond to feedback regarding FedRAMP's growth and meeting the needs of the market. The roadmap outlines four primary goals:



1. Simplifying the process for cloud providers and making the authorization information more useful for agencies,
2. Continuing to update its policies regarding security requirements and expectations and consistently applying the policies to all types of authorizations,
3. Scaling the FedRAMP marketplace to keep pace with agency demand for new and innovative services, and
4. Building a data-first, API-first foundation for FedRAMP to create and share digital authorization packages and related information.

The FedRAMP PMO also is committed to sharing updated information regarding the authorization process (specifically, the timeline for authorization and cost) and to moving to digital authorization packages by defining machine readable packages and providing guidance to customers to create and share them. The roadmap includes a timeline with milestones for FY25 Q1-Q2 and FY25 Q3-Q4 that provides insight into what we should expect this year and in the coming years.

FedRAMP Emerging Technology Prioritization Framework

On June 27, 2024, the FedRAMP PMO published the final Emerging Technology Prioritization Framework (we discussed the Draft version from January 26, 2024 here). The Emerging Technology Prioritization Framework outlines efforts to prioritize generative AI capabilities for FedRAMP authorization beginning with (1) chat interfaces; (2) code generators and debugging tools; and (3) prompt-based image generators. These prioritized offerings will have reduced waiting time for beginning the authorization process by "cutting the line," but the authorization process will not be accelerated. Notably, no more than three capabilities will be prioritized at any time and once three cloud service offerings whose primary purpose is to offer one of the prioritized capabilities have achieved FedRAMP authorization, the capability no longer will be prioritized. The application window for the first series of applications closed on August 31, 2024. The next application window has not been announced, so we expect FedRAMP will open the next window in 2025.

Agile Delivery Pilot Program

On July 10, 2024, FedRAMP launched a new pilot program seeking to eventually replace the "significant change request" process with an approach that does not require advance government approval in order for cloud providers to make certain changes relating to their environments. This will permit cloud providers to continually improve their products without the unpredictability and delay that may arise under the current structure. FedRAMP announced in September 2024 that it selected six cloud service offerings for initial participation in the pilot program. FedRAMP plans to expand the pilot to include additional cloud service offerings over time.

Automation Efforts

On July 11, 2024, FedRAMP launched a new technical automation hub (automate.fedramp.gov), which is "designed specifically to support cloud service providers (CSPs) in the development, validation, and submission of digital authorization packages, and the developers of governance, risk, and compliance (GRC) applications and other tools that produce and consume digital authorization package data." The goal is for this webpage to make the FedRAMP authorization process more efficient and accessible through faster and more frequent documentation updates, providing a wider range of available technical documentation, improving the user experience, and establishing a collaborative workflow for supporting the improvements to documentation. This website demonstrates a focus on automating the submission and review of authorization packages, which now is available for digital authorization packages.

What to Expect in 2025

As we suspected, there were many changes relating to FedRAMP in 2024 and we continue to expect more of the same in 2025 as the modernization of FedRAMP continues. We expect updates on FedRAMP automation efforts, which hopefully will speed up the authorization process in the future. Additionally, we are interested to see how the change in administration will affect FedRAMP, if at all, given its focus on cybersecurity.

04

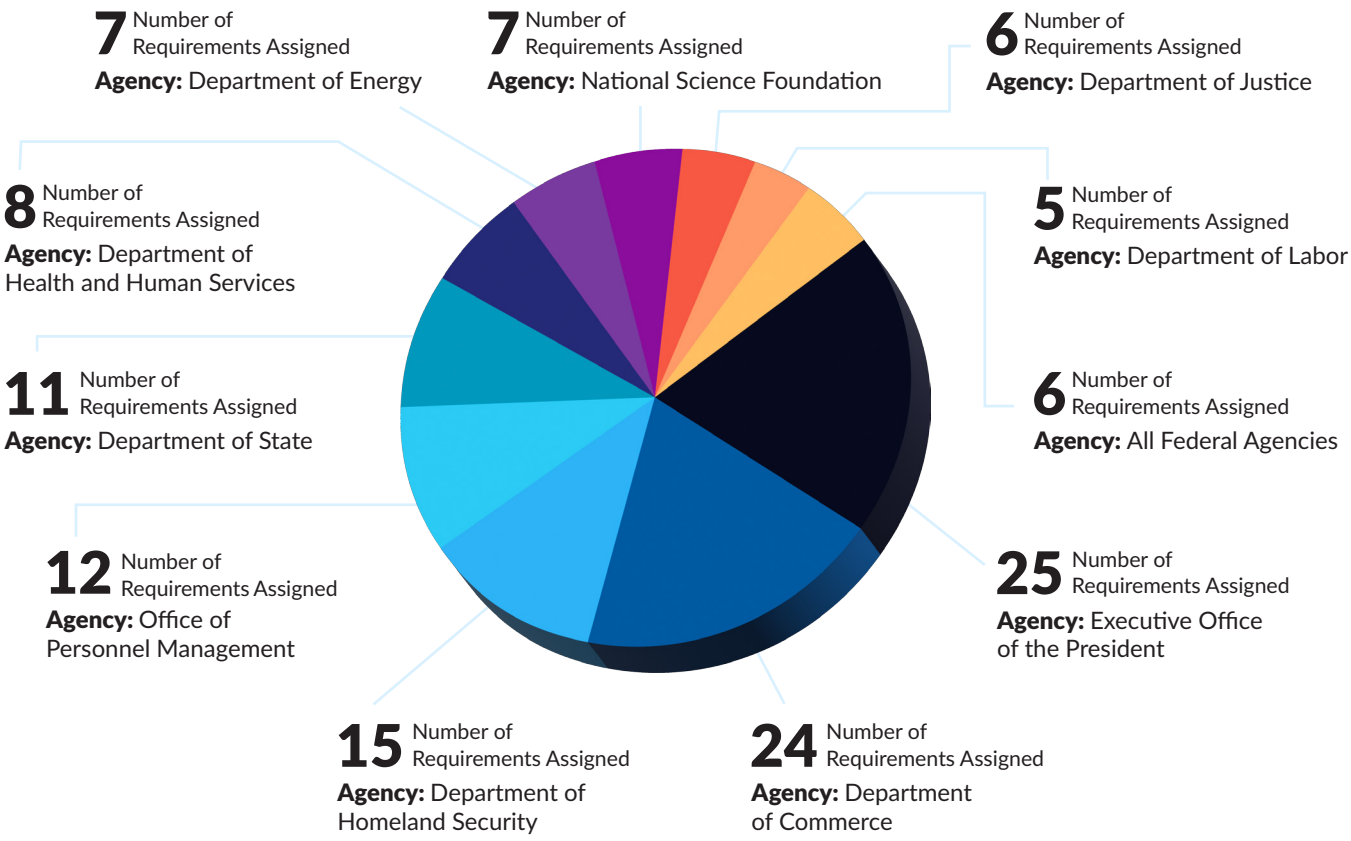
Artificial Intelligence

Executive Order on AI

At the end of 2023, the White House issued Executive Order 14110 (EO) on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (read our blog here). The goal of the EO is to ensure the responsible development and deployment of AI technology and it focuses on safety, innovation, workers, civil rights, consumers, privacy, government, and international efforts. The EO outlines over 150 actions to be taken across federal agencies. The pace to accomplish these actions was quite quick, with 94% of deadlines falling within one year. As of its one year anniversary, agencies have reported 100% compliance with deadlines outlined in the EO. For more information on the EO and agency initiatives, see our Flash Briefing on the Executive Order covering the scope, likely impacts, and prior U.S. initiatives on AI.

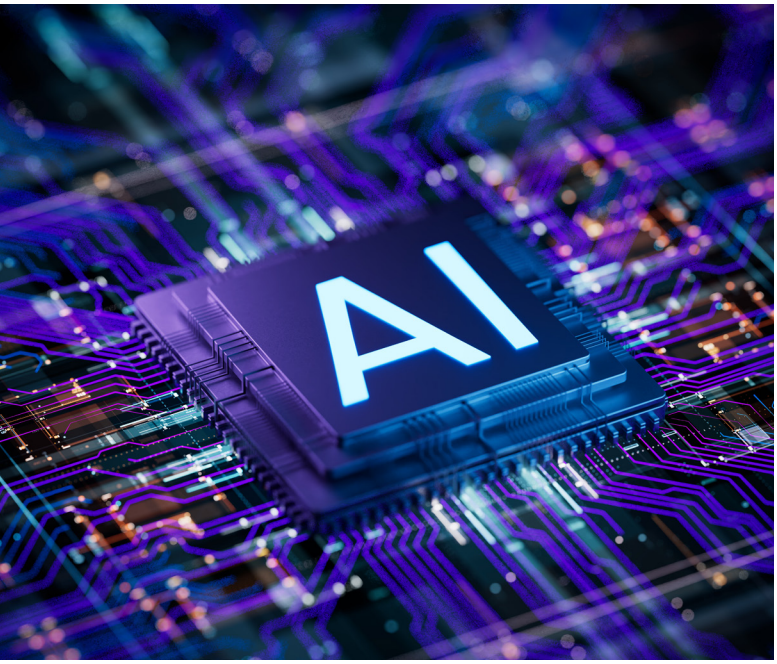
The White House released a fact sheet summarizing progress under the EO after one year. The sweeping requirements and quick agency adoption prove that the federal government has embraced AI and it is not going anywhere anytime soon.

Distribution of Requirements Across Federal Entities*



Source: By the Numbers: Tracking the AI Executive Order.

*Note: Counts reflect only unambiguously assigned requirements-there may be additional requirements for various entities. Also, only entities with five or more requirements are included in this chart.



OMB

One of the most noteworthy actions under the EO is the White House Office of Management and Budget (OMB) government-wide policy on AI, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence (M-24-10). This memo outlines minimum practices for managing risks associated with the use of AI in the federal government. The minimum practices require an agency assessment, testing, and evaluation before authorizing use of the AI, and ongoing monitoring and oversight after authorization to ensure the use of the AI remains within the acceptable levels of risk.

M-24-10 also provides recommendations for managing AI risks in federal procurement of AI. These requirements include ensuring agency rights in data used to design, develop, and deploy AI, promoting competition and interoperability of procured AI, and requiring adequate testing and safeguards particularly for the procurement of generative AI. Especially noteworthy for government contractors, OMB also published Advancing the Responsible Acquisition of Artificial Intelligence in Government (M-24-18). This memo aims to ensure that federal agency AI acquisition is done responsibly, with three strategic goals: (1) appropriately manage risks and performance, (2) promote a competitive marketplace, and (3) implement structures to govern and manage agency business processes related to acquiring AI.

NIST

The National Institute of Standards and Technology (NIST) released significant guidance under the AI EO. Final publications include:

1. The AI Risk Management Framework: Generative AI Profile (NIST AI 600-1)
2. Secure Software Development Practices for Generative AI and Dual-Use Foundation Models (NIST SP 800-218A)
3. A Plan for Global Engagement on AI Standards (NIST AI 100-5)

Additionally, NIST published an initial public draft of AI Safety Institute guidelines on Managing Misuse Risk for Dual-Use Foundation Models (NIST AI 800-1), which outlines voluntary best practices for how foundation model developers can protect their systems from being misused to cause deliberate harm to individuals, public safety, and national security. Comments on this draft were due by September 9, 2024 and a final publication is pending. Lastly, NIST published an open-source software called Dioptra (available for free download) that is designed to allow businesses to conduct evaluations and assess AI developers' claims about system performance.

GSA

Another resource that has emerged from the EO is the GSA Generative AI and Specialized Computing Infrastructure Resource Guide. This guide aims to assist the acquisition workforce in acquisition of generative AI technologies across agencies. Further, this guide breaks down complex technical and AI concepts for those with a non-technical background and incorporates unique agency considerations, such as defense, national security, and intelligence community requirements.

DHS

DHS also addressed AI safety for critical infrastructure in a framework published in November 2024, Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure. This framework is a product of collaboration between government and industry and includes voluntary responsibilities for the safe and secure use of AI in critical infrastructure, evaluates the roles across various responsibility areas, and provides technical recommendations to enhance the safety, security, and trustworthiness of AI systems in critical infrastructure sectors.

AI and National Security

On October 24, 2024, President Biden signed the Memorandum on Advancing the United States' Leadership in Artificial Intelligence; (available here). This memorandum, also a product of the AI EO, is the most comprehensive guidance yet on the role of AI in U.S. national security and provides insight into the government's strategy and policy towards AI. The memorandum emphasizes the importance of U.S. leadership in the development and deployment of AI technology.

What to Expect in 2025

With a new administration in 2025, we are likely to see a shift in the federal government's AI priorities (as well as a new Executive Order) although we expect the federal focus on AI and many of the current initiatives to continue. We expect the new administration will continue to prioritize national security and an America-first mindset, including fostering U.S. AI technology development and ensuring U.S. competitiveness abroad, likely with less focus on regulatory and reporting provisions that may be seen to hamper innovation.

As the technology and government integration of AI continues to evolve, it will be important for government contractors to stay abreast of the changing landscape. Specifically, government contractors should stay up to date on new publications and be on the lookout for new AI guidance and eventual regulations, which may impact federal acquisition of AI technology. Additionally, it will be important to ensure AI performance metrics, standards, and obligations are clearly defined in any contract involving AI, to include required disclosures or descriptions regarding contractor AI use. AI is one area we are closely monitoring going into the new year, especially considering a likely new approach under the incoming administration. We will be providing updates as they occur.

05

Critical Infrastructure Reporting & National Security

Cyber Incident Reporting for Critical Infrastructure

This year, we saw proposed regulations from the Cybersecurity and Infrastructure Security Agency (CISA) for new incident reporting requirements under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Under the Act, CISA had two years to issue the proposed regulations, which came out in April 2024 and went through a public comment period this year. Notably, these regulations are not going to be part of the FAR or DFARS, but will be published in Part 6 of the Code of Federal Regulations, in a new Section 226, as part of the Department of Homeland Security's regulations on Domestic Security (so they will apply regardless of incorporation in a government contract or agreement). Final regulations are expected by October 2025. See our discussion of the proposed rule here.

The new regulations will require covered entities in each of the sixteen critical infrastructure sectors to report "substantial cyber incidents" to CISA within 72 hours and ransom payments within 24 hours. Covered entities include all large businesses as well as any entity that meets certain threshold criteria in the rule, regardless of size. Businesses that are small per the Small Business Administration's size standards not otherwise covered by the threshold criteria are excluded from the definition.

U.S. Critical Infrastructure Sectors


Chemical Sector


Healthcare and Public Health Sector


Communications Sector


Information Technology Sector


Critical Manufacturing Sector


Nuclear Reactors, Materials, and Waste Sector


Defense Industrial Base Sector


Transportation Systems Sector

Emergency Services Sector


Water and Wastewater Systems Sector


Energy Sector

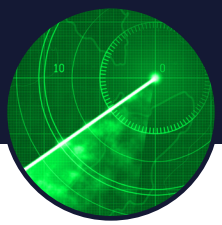

Commercial Facilities Sector


Financial Services Sector


Dams Sector


Government Facilities Sector


Food and Agriculture Sector


Most relevant to government contractors are the threshold criteria for the below critical infrastructure sectors:

- **Communications Sector** – any entity that provides communications services by wire or radio communications to the public, business, or government.
    - This includes one-way communications service providers (e.g., radio and TV broadcasters, cable TV and satellite operators) and two-way communications service providers (e.g., telecom carriers, wireless service providers, internet service providers).
- **Defense Industrial Base Sector** – any entity that is a contractor or subcontractor required to report cyber incidents to DoD per DFARS regulations.
- **Information Technology Sector** – any entity that meets one or more of four criteria:
    1. Any entity that knowingly provides IT hardware, software, systems, or services to the Federal government;
    2. Any entity that has developed and continues to sell, license, or maintain any software that meets the definition of "critical software" as defined by NIST;
    3. Any entity that is an OEM, vendor, or integrator of OT hardware or software components; and
    4. Any entity that performs functions related to domain name operations.

Companies that fail to report in accordance with the rule may be subject to enforcement mechanisms by CISA such as (1) issuance of an RFI for more information; (2) issuance of a subpoena; (3) referral to the Attorney General for potential civil court action; and (4) initiation of suspension and debarment procedures. False or fraudulent statements in a CIRCIA Report or other response to CISA could result in penalties under 18 U.S.C. § 1001, a criminal statute.

In order to harmonize and reduce the burden of multiple cyber incident reporting requirements, CISA is reportedly working on agreements with other agencies (such as DoD and HHS) to provide an exception to the requirements where a company is already required to report cyber incidents under current regulations.

What to Expect in 2025

CISA has faced some pushback on the proposed regulations, so we could see changes in the final version of the rule. As noted above, the final rule is required to be released by October 2025 and likely will become effective shortly thereafter. Entities in the sixteen critical infrastructure sectors should review their incident response procedures and be prepared to update them in accordance with the final rule.

Restrictions on Bulk Sensitive Personal Data

This year, the Department of Justice (DOJ) published a Proposed Rule outlining prohibitions and restrictions on certain transactions involving U.S. data stemming from E.O. 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." There are two classes of data that would be regulated: (1) bulk U.S. sensitive personal data (as defined in the rule) and (2) certain U.S. Government-related data. Under the Proposed Rule, transactions involving those data types and a country of concern would be either prohibited (requiring a license from the government to proceed) or restricted (requiring the implementation of cybersecurity requirements from CISA and other compliance obligations).

Bulk U.S. sensitive personal data includes six data types (the bulk threshold must be met for the data to be covered)

1. covered personal identifiers;
2. geolocation and related sensor data;
3. biometric identifiers;
4. human genomic data;
5. personal health data; and
6. personal financial data.

For U.S. Government-related data, there is no bulk threshold, and instead, the regulations apply to certain transactions related to *any* data that is either (i) precise geolocation data for certain U.S. Government locations identified pursuant to the rule or (ii) sensitive personal data marketed as linked or linkable to certain government employees or contractors.

Transactions with covered parties for the sale of this data ("data brokerage transactions") as well as for the sale of human genomic or biospecimen data, would be *prohibited*. Likewise, vendor agreements, employment agreements, and investment agreements will be *restricted* when those transactions involve access or potential access to covered data by a covered party.

What to Expect in 2025

The Proposed Rule went through a comment period, so we could see a final rule in 2025. With the new incoming administration, there could be changes to how this regulation is finalized and/or administered. For example, we may see administration of the rule shift from the DOJ to the Department of Commerce. Also, where the new administration likely will focus on de-regulation in some areas, eventual compliance requirements may become less stringent. At the same time, national security interests and maintaining protections for U.S. sensitive data remain strong, so we expect that some form of this regulation will become effective in 2025.

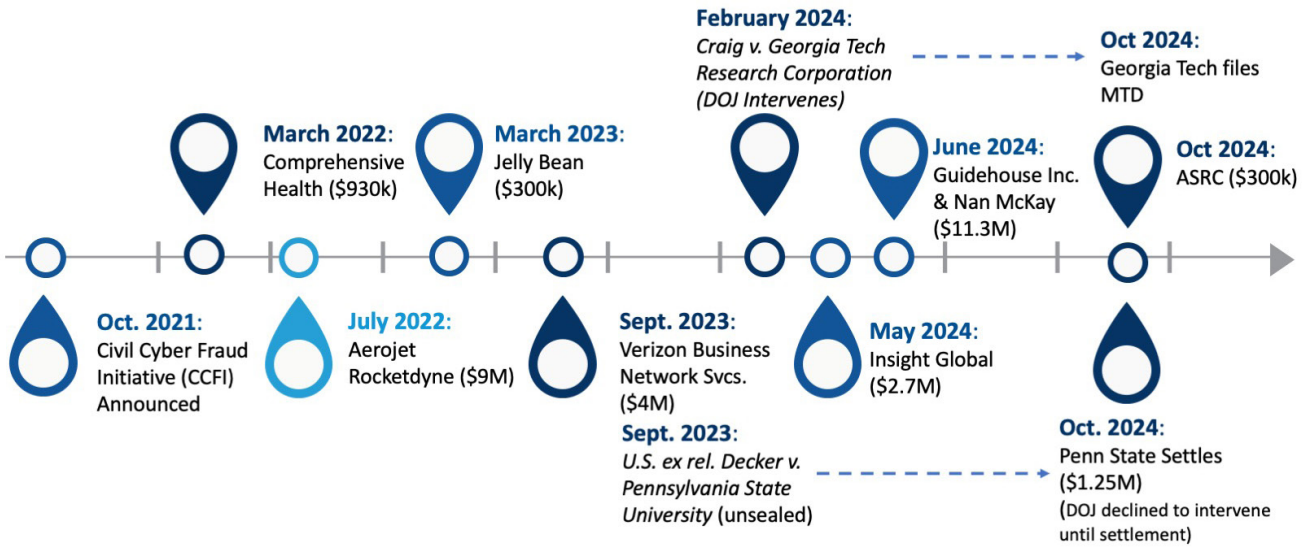
For more information, see our Data, Deals, and Diplomacy article.

06

Cybersecurity Fraud & Enforcement

As anticipated, 2024 was a big year for government enforcement related to cybersecurity practices. In particular, we saw significant actions from the Department of Justice (DOJ) (via its Civil Cyber Fraud Initiative, or CCFI).

On October 6, 2021, the DOJ announced the creation of its CCFI to enforce cybersecurity standards and reporting requirements among federal contractors (as we previously discussed here). The following timeline shows the enforcement actions attributed to the CCFI since its inception in 2021:



As the timeline shows, there has been significant activity in 2024, including:

- **Craig v. Georgia Tech Research Corporation Intervention & Motion to Dismiss** – The original whistleblower suit was initiated in July 2022 by former senior members of Georgia Tech's Cybersecurity team. Following a lengthy investigation, the DOJ intervened in the case in February 2024 and the original complaint was unsealed. In August 2024, the DOJ filed its Complaint in Intervention, alleging the defendants knowingly failed to meet contractual cybersecurity requirements in connection with various DoD contracts. We discussed DOJ's complaint in intervention in more detail here. Additionally, in October 2024, Georgia Tech Research Corp. filed its Motion to Dismiss, arguing (among other things) the DoD cybersecurity regulations do not apply to systems used to perform fundamental research (*i.e.*, the systems do not house covered information); strict compliance with the cybersecurity controls was not material; and there was no harm to the Government.
- **Guidehouse Inc. & Nan McKay Settlement** – In June 2024, the DOJ CCFI announced a settlement that resulted in a total of $11,300,000 in payments from two consulting companies (Guidehouse, Inc., the prime contractor, which paid $7,600,000; and Nan Kay and Associates, the subcontractor, which paid $3,700,000) to resolve allegations the two companies violated the False Claims Act by failing to meet cybersecurity requirements in state-level contracts (that were federally funded). We discussed this settlement in more detail here.

- **U.S. ex rel. Decker v. Pennsylvania State University settlement** – In October 2024, the DOJ CCFI announced the Pennsylvania State University (Penn State) agreed to pay $1,250,000 to settle a FCA case brought against the University approximately two years prior. The whistleblower in the case, former Chief Information Officer of the Penn State Applied Research Laboratory, alleged that Penn State failed to comply with cybersecurity requirements in fifteen contracts and/or subcontracts with the Department of Defense (DoD) and National Aeronautics and Space Administration (NASA) between 2018 and 2023. We discussed the settlement in more detail here.

Overall, the 2024 enforcement activity demonstrates the breadth of the CCFI's scope. In particular, it is not limited to federal contracts (it also includes contracts funded with federal dollars), it is not limited to prime contractors (it also includes subcontractors), and it is not limited to a particular industry. Additionally, as the Penn State settlement shows, *any* misrepresentation (including relatively minor ones such as timelines associated with the implementation of plans of action and milestones) can be the subject of an enforcement action. Accordingly, anyone doing business with the government (in any capacity) should be mindful of cybersecurity obligations and maintaining accurate documentation to demonstrate compliance.

What to Expect in 2025

We expect to see a continued increase in cybersecurity enforcement activity in 2025. In the meantime, contactors should review their cybersecurity obligations, ensure internal policies are updated appropriately, promptly investigate internal complaints, timely assess and report (if required) cybersecurity incidents, and take care not to misrepresent their cybersecurity practices. This will be especially important as we expect to see the Cybersecurity Maturity Model Certification requirements, which include certification requirements at all levels, become effective in 2025.

About the Governmental Practice Cybersecurity & Data Protection Team

Cybersecurity and data protection have never been more important for government contractors and their vendors. Sheppard Mullin's Governmental Cybersecurity and Data Protection Team understands the government's approach to cybersecurity, in its own systems and those of its contractors. Our team combines experts in cybersecurity, data protection, data privacy, and government contracts law to provide unparalleled advice to companies that sell products and services to the government (whether directly or indirectly), as they face rapidly changing cybersecurity standards and requirements from a variety of government agencies. With deep relationships to government officials, we are called on by some of the largest and most prominent government contractors to guide them through the maze of laws, standards, and agency regulations regarding cybersecurity and cloud computing and assist them with government-specific aspects of incident response. Click here to read more about the team.

Governmental Practice Cybersecurity and Data Protection
2024 Recap & 2025 Forecast Alert

SheppardMullin