Governmental Practice
Cybersecurity and Data Protection

2023 Recap & 2024 Forecast Alert

SheppardMullin

Governmental Practice Cybersecurity and Data Protection
2023 Recap & 2024 Forecast Alert

To kick off the New Year, Sheppard Mullin's Governmental Practice Cybersecurity & Data Protection Team has prepared a cybersecurity-focused 2023 Recap (including links to all of the resources the team has put out over the past year) and 2024 Forecast (that previews what we expect to see in 2024). This Recap & Forecast covers the following five high-interest topic areas related to cybersecurity and data protection:

(1) DoD and CMMC, (2) FAR Cybersecurity Updates, (3) Software Security, (4) Security & the Cloud - FedRAMP and AI Considerations, and (5) Cybersecurity Fraud and Enforcement.

Authors

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

Nikole 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

Contents

1. DoD and CMMC

Throughout 2023, we have been closely following 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 DoD's Cybersecurity Maturity Model Certification ("CMMC") program. Just in time for the new year, DoD published a Proposed Rule to implement the CMMC program on December 26, 2023 (which we discuss in more detail here). Below, we provide a high level summary of the DFARS cases, and a separate summary related to 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 31, 2024 (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. Obviously, we have been waiting a long time for DoD to publish a final rule. The Fall 2023 Unified Agenda indicates a final rule will be issued in February 2024.

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. Currently, the Defense Acquisition Regulations Council is scheduled to review the proposed DFARS rule on January 10, 2024, and the Fall 2023 Unified Agenda indicates a proposed rule to amend the DFARS will be published in March 2024.

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** – A Draft CMMC rule is published.
- **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** – The CMMC Program Proposed Rule is published.

As expected based on the CMMC 2.0 announcement, the CMMC Program Proposed Rule follows the three-tiered approach (Levels 1, 2, and 3). We discuss the requirements for each level, along with other notable provisions from the Proposed Rule, in more detail here, but there are no major surprises. A few notable additions/clarifications include:

- **Implementation** – the roll-out of the program will occur via a four-phased approach, and is more aggressive than in the previous version of the rule. It anticipates full implementation (Phase 4) will take place 2.5 years after changes to the DFARS become effective (per DFARS case 2019-D041).
- **Timing of certification** – the Proposed Rule indicates the requisite certification will be required at the contract award stage (*i.e.*, "as a condition of award"), rather than at the proposal stage.
- **Cloud Service Providers and External Service Providers** – Cloud service providers must be authorized at the FedRAMP Moderate level or provide evidence of equivalent security controls. External service providers must have controls in place for the requisite CMMC level.
- **International Entities** – Overseas companies will have to meet the same requirements as U.S. domestic suppliers. There is not yet a plan to recognize international or other cybersecurity standards.
- **Disputes** – the Proposed Rule indicates there will be two separate disputes processes: (1) for disputing an assessment by a C3PAO, and (2) for disputing the CMMC level required by a solicitation. A C3PAO assessment dispute will be escalated to the Cyber AB for resolution, whereas issues with the CMMC level requirement in a solicitation can be raised to the contracting officer (likely via a pre-award protest).

What to Expect in 2024

Comments on the CMMC Program Proposed Rule are due by February 26, 2024 (*i.e.*, 60-day comment period). Given the anticipation surrounding the Proposed Rule, and the significant impact it will have on DoD contractors, we expect there will be a large number of comments submitted. In any event, we expect a final rule (and implementing DFARS requirements) will likely very closely mirror the Proposed Rule and, as such, contractors should refocus on preparing (via self-assessments or engaging a C3PAO) in the meantime.

2. FAR Cybersecurity Updates

During 2023, we closely followed the development of new FAR rules related to cyber and supply chain security. Below, we provide a short description and status of forthcoming FAR rules (currently styled as "FAR Cases" while in development), and then provide a more fulsome update on the proposed and interim rules released last year. The forthcoming FAR rules include:

- ***Cyber Threat Incident Reporting and Information Sharing*** **(FAR Case 2021-017) –** includes requirements to increase sharing of information about cyber threats and new incident reporting and response obligations. This rule is meant to apply to contractors that provide products or services to the Government that include information and communications technology. This rule currently is in the "Proposed Rule Stage," and the public comment period is currently open until Feb. 2, 2024.

- ***Standardizing Cybersecurity Requirements for Federal Information Systems*** **(FAR Case 2021-019) –** 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. This rule currently is in the "Proposed Rule Stage," and the public comment period is currently open until Feb. 2, 2024.

- ***Implementation of Federal Acquisition Supply Chain Security Act ("FASCSA") Orders*** **(FAR Case 2020-011) –** 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 is in the "Final Rule Stage," and is currently effective with a public comment period open until Feb. 2, 2024.

- ***Establishing FAR Part 40*** **(FAR Case 2022-010)** – amends the FAR to create a new FAR part, Part 40, which will be the new location for cybersecurity supply chain requirements. This new FAR part will provide a single, consolidated location in the FAR for cybersecurity supply chain risk management requirements. The final rule is currently being processed, and we anticipate it will be published soon.

- ***Controlled Unclassified Information*** **(FAR Case 2017-016)** – implements the National Archives and Records Administration ("NARA") CUI program, which provides implementing regulations for safeguarding and handling of CUI, and will address guidance for responding to breaches involving Personally Identifiable Information ("PII"). Currently, the proposed rule is expected to be released in February 2024.

Below, we provide a high-level recap of the proposed and interim rules relating to these FAR cases published in 2023, along with links to relevant articles we have written for those of you interested in more details on each.

Proposed Rules – Cyber Threat Incident Reporting and Information Sharing (2021-017) & Standardizing Cybersecurity Requirements for Federal Information Systems (2021-19)

On October 3, 2023, the FAR Council released two proposed rules for federal contractor cybersecurity that stem from the Biden Administration's May 2021 Cybersecurity Executive Order (discussed here). We highlighted the key points to know about these Proposed Rules in two articles, accessible here and here, and in a Federal News Network podcast.

Cyber Threat Incident Reporting and Information Sharing (2021-017) – This rule applies to contractors that provide products or services to the Government that include information and communications technology ("ICT"), although note the new clause and representation provision in the proposed rule are to be included in **all** solicitations and contracts, which is likely to cause confusion among industry and government as to when and how a determination of non-applicability will be made. This proposed rule contains updated definitions, requirements, and representations relating to federal contractor cybersecurity. Generally, new requirements for federal contractors include:

- reporting any cybersecurity incident to CISA within eight hours of discovery with updates every 72 hours until remediated;
- developing and maintaining a Software Bill of Materials ("SBOM") for any software used in contract performance;
- completing Internet Protocol version 6 ("IPv6") implementation activities;
- allowing access and cooperating with CISA and other agencies for purposes of threat hunting and incident response.

- **Standardizing Cybersecurity Requirements for Federal Information Systems (2021-19)** – This rule applies to contractors that develop, implement, operate, or maintain Federal Information Systems ("FIS"). It contains updated definitions, requirements, and representations relating to standardizing cybersecurity requirements for such systems. The FAR Council estimates the rule will apply to only 84 contractors annually (both non-cloud FIS contractors and cloud FIS contractors), although hundreds of contractors that bid on these contracts will need to familiarize themselves with the new regulations. Generally, new requirements for federal contractors include the following:

- For Federal Information Systems using non-cloud computing services: Obligations relating to records management and agency access to government data, government-related data, and contractor personnel involved in contract performance; developing System Security Plans for certain systems; and conducting annual security assessments; among other requirements.
- For Federal Information Systems using cloud computing services: FedRAMP authorization at the level determined by the agency. For systems designated as FedRAMP High, all Government data must be maintained within the United States or its outlying areas, unless otherwise specified in the contract.

What to Expect in 2024:

The comment period is scheduled to close on February 2, 2024. After the comment period closes, the FAR Council will reconcile comments and begin drafting Final Rules. Final Rules could be issued as soon as the end of 2024. In the interim, contractors should plan to submit written comments before the period closes, determine likely applicability of the rules, and prepare to comply with these requirements before the Final Rules are issued.

Interim Rule – Implementation of Federal Acquisition Supply Chain Security Act Orders (FAR Case 2020-011)

On October 5, 2023, the FAR Council released an interim rule implementing requirements from Section 202 of the Federal Acquisition Supply Chain Security Act ("FASCSA"), which will require federal contractors to ensure certain products and services are excluded from the U.S. Government supply chain. Determinations regarding removal or exclusion are to be made by the Federal Acquisition Security Council ("FASC"). These requirements are applicable to all Federal contracts. We previously discussed the interim rule here.

This interim rule became effective on December 4, 2023. FAR clauses outlined in the Interim Rule were to be incorporated into all solicitations and contracts (including orders and modifications) issued after December 4, 2023.

Key highlights from the Interim Rule include the following:

- FASC can create both "exclusion" and "removal" orders, which may require contractors to "remove" items during contract performance;
- Offerors must represent compliance with applicable FASCSA orders;
- Contractors will have a continuing obligation to monitor and report throughout performance;
- New clause FAR 52.204-30 is a Mandatory Flow Down for subcontractors;
- For certain multi-agency contracts, FASCSA orders likely will apply at the order level;
- The prohibition applies both to products and to sources; and
- Waivers may be available if offerors are not able to make the representation in FAR 52.204-29.

What to Expect in 2024:

Comments submitted in response to this Interim Rule before December 4, 2023 will be considered in the implementation of the forthcoming Final Rule. This Interim Rule currently is effective and contractors should be evaluating internal processes and controls that can be used to identify covered articles and/or sources in the performance of their government contracts, and be preparing to handle FASCSA orders issued during performance.

3. Software Security

Enhancing the security of the software supply chain was a key focus of the Biden Administration's May 2021 Executive Order (the "Cyber EO") (which we previously discussed here). Below, we discuss the major steps the government has taken to implement the requirements of the Cyber EO related to software supply chain security.

Attestation Requirement

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. Relatedly –

- On September 14, 2022 OMB issued OMB M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development*, requiring federal agencies to only use software from software producers that attest to compliance with the secure software development guidance issued by NIST. Agencies are required to obtain an attestation from software producers either through a self-attestation or through a third-party assessment. Additional details are available in our article, Federal Government Outlines New Security Attestation Requirements for Software.

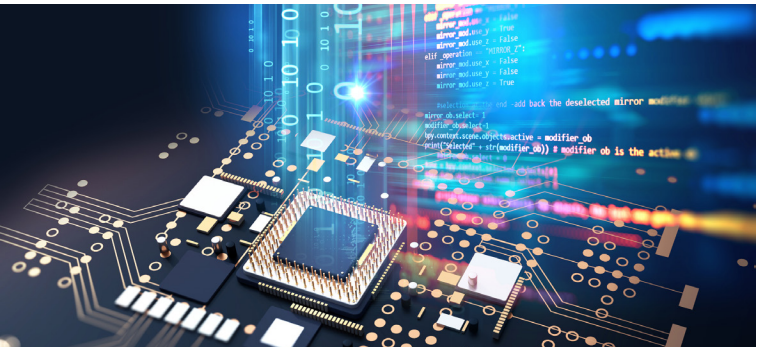
- On June 9, 2023, OMB released an update to OMB M-22-18 (OMB M-23-16) which extends the timeline for agencies to collect attestations from software producers. For critical software, agencies must collect attestations no later than three months after the CISA Secure Software Development Attestation Form is approved by OMB (more on this below). For all other software, attestations are to be collected within six months. Additional details on this memorandum are included in our article, White House Provides New Guidance & Extends Deadline for Secure Software Attestations.

Attestation Form

In May 2023, CISA released an initial draft of the Secure Software Development Attestation Form, which we discussed here. After receiving the initial round of comments, CISA revised the Form and released a notice to allow for further comments through December 2023. Key updates to the initial Attestation Form include the following:

- Adding the option for either the software producer or the verifying FedRAMP Third Party Assessor Organization ("3PAO") to attest to the software producer's conformance.
- If the 3PAO provides the attestation, the 3PAO assessment must be attached to the completed Common Form, in lieu of a signature.
- If the software producer provides the attestation, CISA limits signatory authority to only the company's CEO or COO.

Additional details on the revised Attestation Form can be found in our article, Update: CISA Seeks Additional Input from Software Providers on Security Attestation Form.



Open FAR Case – Supply Chain Software Security

The FAR Council is currently developing a new rule, FAR Case 2023-002, *Supply Chain Software Security*. This rule will implement section 4(n) of the Cyber EO, which, among other things, requires software suppliers to comply with, and attest to complying with, applicable secure software development practices, in accordance with the aforementioned OMB Memoranda. We do not have a publicly available proposed rule yet, but an initial draft supposedly is under review and so we expect it will be released early this year.

Definition of "Critical Software"

On June 25, 2021, NIST released a definition of "critical software" as required by the Cyber EO, and then on July 9, 2021, released a guidance document related to "EO-Critical Software" use. We discussed the definition and other key terms in our article, Right on Time – NIST Releases Definition of "Critical Software" Per Biden's Cybersecurity Executive Order.

What to Expect in 2024:

CISA is currently reviewing comments on the second draft Attestation Form. However, neither CISA nor OMB have provided an anticipated date for publication of the final Attestation Form, and so the timing associated with firm requirements for collecting attestations is not yet clear. In the interim, contractors should review the current draft Attestation Form, and the FAR proposed rule once available, and consider the scope of attestations they and their suppliers may need to provide.

4. Security & the Cloud – FedRAMP and AI Considerations

Last year was a transformative one for the Federal Risk and Authorization Management Program ("FedRAMP"), the federal government's program for security authorizations for cloud service offerings. Among other things, we saw major revisions to the FedRAMP guidance and control baselines, legislative updates, and a new Artificial Intelligence (AI) Executive Order, which contemplates a new framework for prioritizing certain offerings for FedRAMP authorization. Below, we highlight the major updates relating to FedRAMP and include links to relevant articles we have written for those who are looking for additional details.

Legislative Updates – FedRAMP Authorization Act

In January 2023, the President signed the FedRAMP Authorization Act (the "Act") as part of the FY23 NDAA. While FedRAMP has been around since 2011, the Act codifies the program for the first time as the authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information. Among other things, the Act also (1) created the Federal Secure Cloud Advisory Committee ("FSCAC"); (2) established a FedRAMP Board; and (3) requires incorporation of more automation solutions in security assessments and reviews.

Related to the Act, on October 27, 2023, OMB released a draft memorandum entitled "Modernizing the Federal Risk and Authorization Management Program (FedRAMP)." Among other things, the Draft OMB Memo (1) provides an updated vision for FedRAMP with strategic goals and responsibilities for implementation; (2) outlines improvements to the FedRAMP authorization and continuous monitoring processes; (3) clarifies what cloud service offerings are in-scope for FedRAMP authorization; (4) revises the pathways to FedRAMP authorization; and (5) encourages that FedRAMP avoid incentivizing bifurcation of cloud services into commercial- and federal-focused instances. Our article, Time for An Upgrade: OMB Releases Draft Memorandum Modernizing FedRAMP, provides more details about the Draft OMB Memo.

Updated FedRAMP Guidance

Following the release of NIST Special Publication 800-53 Rev. 5, the underlying security baseline for the program, FedRAMP released updated guidance in several waves to align with and reflect the changes in NIST SP 800-53. The FedRAMP guidance released includes:

- A new Collaborative ConMon Quick Guide that replaced the Guide for Multi-Agency Continuous Monitoring;
- An updated CSP Continuous Monitoring Performance Management Guide; and
- An updated System Security Plan Appendix A: LI-SaaS FedRAMP Security Controls for all security control baselines.

FedRAMP developed a webpage with all Revision 4 documents and the corresponding new Revision 5 guidance to assist cloud service providers in complying with the new and updated obligations.

In addition, FedRAMP released updated guidance for third party assessors (3PAOs) that incorporates changes from the FedRAMP Authorization Act. Our article, Reassessed: FedRAMP Releases Revised Obligations and Standards for Cybersecurity Assessors, discusses the updated guidance in more detail.

Proposed FAR Rule

The proposed FAR Rule, *Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems* (FAR Case 2021-019) (which is discussed in more detail in Section 2, "FAR Cybersecurity Updates," above) includes requirements regarding FedRAMP authorization for Federal Information Systems using cloud computing services. If this requirement remains in the final rule, agencies will require contractors maintaining Federal Information Systems in the cloud to (1) achieve and maintain FedRAMP authorization at a specified level determined by the agency; (2) institute proper controls and access limitations for Government data and Government-related data; (3) adhere to applicable security guidelines; (4) allow access by authorized government representatives; and (5) maintain certain high-impact data within the United States.

FedRAMP and AI

Last – but certainly not least – on October 30, 2023, the White House issued an Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. As relevant to FedRAMP, the Executive Order includes a requirement to develop a framework for prioritizing generative artificial intelligence and other emerging technologies offerings in the FedRAMP authorization process. On November 8, 2023, we held a Flash Briefing on the Executive Order on AI, during which (among other things), we discussed the requirements related to FedRAMP.

Following the release of the Executive Order, FedRAMP announced it is collaborating with stakeholders and industry to analyze the impact to security controls with the introduction of AI systems into a FedRAMP authorized system boundary. FedRAMP also announced it is spearheading collaboration with the FedRAMP Board, the OMB, NIST, and the FSCAC to create and gain consensus on the authorization strategy for emerging technologies.

As the use of AI continues to increase, there will be added pressure to ensure AI offerings are secure and FedRAMP authorization likely will be a focus of this effort.

What to Expect in 2024

There were many changes for cloud service providers in 2023 and we expect more of the same in 2024 as the modernization of FedRAMP continues. AI is one area we are closely monitoring going into the new year, including the use of automation by FedRAMP in security assessments and continuous monitoring activities as well as the security authorization of AI products for future use by federal agencies.

5. Cybersecurity Fraud and Enforcement

Last year we saw more government activity focused on enforcement related to cybersecurity practices. In particular, we saw significant actions from both the Department of Justice ("DOJ") (via its Civil Cyber Fraud Initiative, or "CCFI") and the Securities and Exchange Commission ("SEC"), which enacted new regulations for cybersecurity reporting by public companies.

DOJ's Civil Cyber Fraud Initiative Enforcement Actions

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). Since then, there have been four settlements announced, including:

- March 8, 2022 – Settlement with Comprehensive Health Services, LLC for $930,000 (discussed in more detail here)
- July 8, 2022 – Settlement with Aerojet Rocketdyne (on the second day of trial) for $9 million
- March 14, 2023 – Settlement with Jelly Bean Communications Design LLC for $300,000
- September 6, 2023 – Settlement with Verizon Business Network Services LLC for $4 million (discussed in more detail here).

Also in September 2023, the court unsealed a *qui tam* (whistleblower) lawsuit against Penn State University relating to allegations of non-compliance with Department of Defense ("DoD") cybersecurity obligations. So far, DOJ has declined to intervene in that case, but indicated its investigation is ongoing. We discussed the Penn State lawsuit in more detail here.

Relatedly, on November 30, 2023, the DoD Inspector General released a Report that provides an overview of common weaknesses in contractors' protection of Controlled Unclassified Information ("CUI"). The DoD IG identified these issues as a result of multiple recent audits and investigations (including investigations related to the CCFI settlements listed above). We wrote an article that provides more detail on the report and recommendations here.

SEC Enforcement & New Cyber Incident Disclosure Rule

The SEC has also been active with respect to cybersecurity enforcement. For example, on October 31, 2023, the SEC filed a much-anticipated lawsuit against SolarWinds and its Chief Information Officer ("CIO"), Timothy Brown (personally) for fraud and internal control failures related to a nearly two-year long cyber-attack known as "Sunburst." The SEC Complaint includes 10 separate claims and, among other things, alleges SolarWinds misled investors about its vulnerability to cyber-attacks.

The SEC published a new rule (which went into effect on Dec. 18, 2023) that requires publicly traded companies to disclose material cyber incidents via Form 8-K within four days of making a materiality determination. Our colleagues previously discussed the SEC rule and its new cyber reporting requirements here. Notably, the SEC rule also includes an exception that the registrant may delay providing the disclosure "if the United States Attorney General determines that disclosure [. . .] poses a substantial risk to national security or public safety [. . .]." On December 12, 2023, the DOJ issued guidance related to the process by which companies may request the Attorney General authorize delays of cyber incident disclosures under the SEC rule. We discussed the DOJ guidance, and related FBI guidance, in a recent article here.

What to Expect in 2024

We expect to see an increase in cybersecurity enforcement activity in 2024. Until now, DOJ has been responsible for most of cyber-related enforcement activity, but with the finalization of the SEC's new incident disclosure rule, we also are likely to see an uptick in enforcement from the SEC. 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 (either to the government or to investors).

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
2023 Recap & 2024 Forecast Alert

SheppardMullin