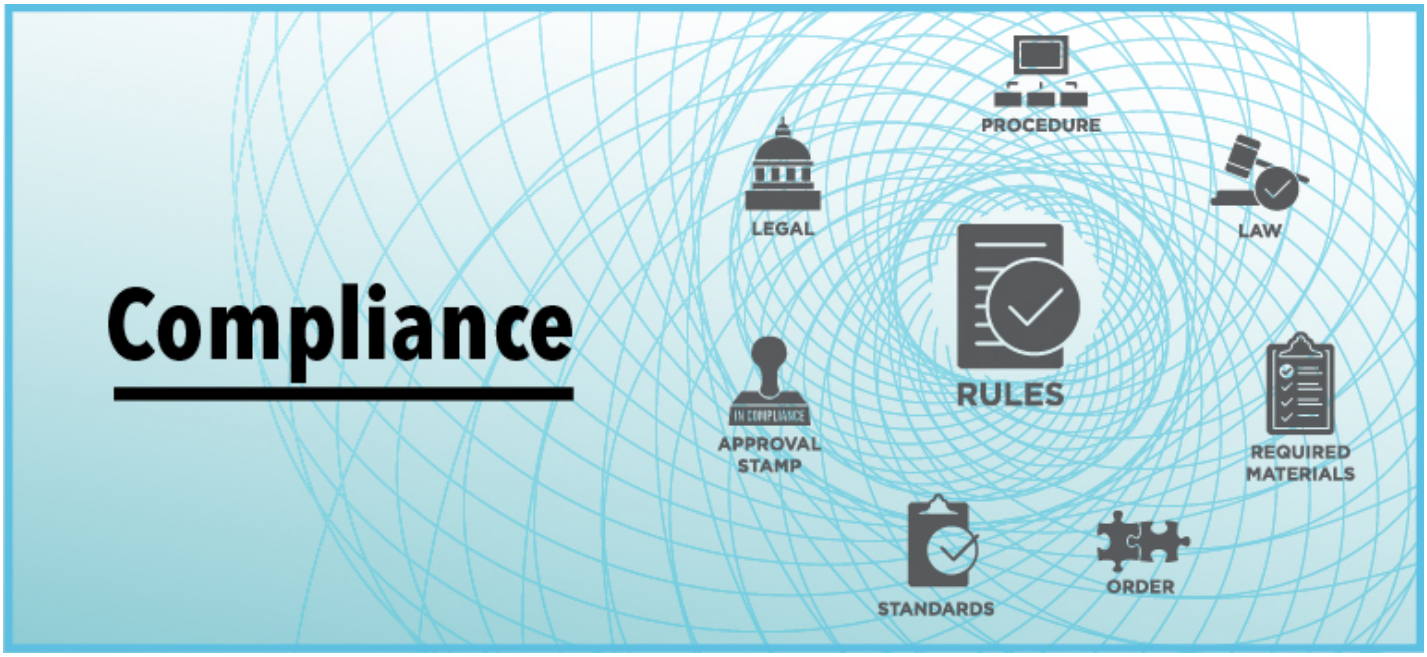
From the Fall 2019 Issue

Cybersecurity Policy

Practical Advice for DoD Contractor Cybersecurity Compliance

Glyn Cashwell
Esq., JD, CISSP, CSEP, PMP, PE | ProObject/Cashwell Legal, LLC



There are a number of questions that small businesses frequently ask about cybersecurity compliance within their organization. It is important for the DoD small business community to better understand Controlled but Unclassified Information (CUI), DFARS 252.204-7012, and Cybersecurity Maturity Model Certification (CMMC).

WHAT EXACTLY IS CONTROLLED BUT UNCLASSIFIED INFORMATION (CUI)?

CUI must be clearly marked as CONTROLLED or CUI in accordance with *Marking Controlled Unclassified Information*.[1] According to the Information Security Oversight Office, National Archives and Records Administration, "until directed by your agency's guidance, executive branch employees and contractors supporting Government agencies must not use CUI markings and other CUI requirements."[2] DoD is adding clauses to new and existing contracts requiring that certain compliance requirements, such as DFARS 252.204-7012, be in place before the government gives DoD contractors CUI.[3] CUI will replace "existing agency programs like For Official Use Only (FOUO)" and other similar markings.[4]

WHAT DOES DFARS 252.204-7012 REQUIRE?

At a high level, the DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting clause has three requirements: (1) NIST 800-171 compliance, (2) cyber incident reporting, and (3) image preservation for forensic analysis after a breach. NIST 800-171 requirements map to NIST 800-53A controls and mandate various written plans and documentation regarding how each control is satisfied with relevant implementation and configuration information. This mapping is provided in Appendix D of NIST 80-171.[5]

WHY BE CONCERNED ABOUT COMPLIANCE IF MY COMPANY ISN'T RECEIVING CUI?

i. **DFARS 252.204-7012**
DFARS 252.204-7012 is a requirement on many DoD contracts, even if those associated contractors are not yet being asked to handle CUI. This year, the DoD has strictly enforced DFARS 252.204-7012 compliance. The government has been "refusing to renew contracts with non-compliant businesses, and it's also denying new contracts to non-compliant organizations"[6]). The government could "issue a stop work-order until compliance is achieved". However, as a result, companies face the risk of "administrative, contract, civil, and even criminal penalties" for ignoring compliance.[7] Companies should look through their contracts to see if there is any language requiring DFARS 252.204-7012 compliance. Even if not in their current contracts, the requirement will likely come up in their future contracts.

ii. **Cybersecurity Maturity Model Certification (CMMC)**
In addition to requiring defense contractors to meet DFARS 252.204-7012, DoD will require them to meet a more rigorous CMMC third-party certification that contains certification levels ranging from one to five. Largely because DoD believed DFARS 252-204.7012 did not provide enough rigor for cybersecurity in DoD contractors' networks, evidenced by continued breaches, the Cybersecurity Maturity Model Certification (CMMC) was created.[8]

iii. **CMMC levels**
According to the Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification, "the level of certification required will depend upon the amount of CUI a company handles or processes"[9]

In its draft form, CMMC shows level 3 as being very closely linked to meeting NIST 800-171 controls.[10] "The intent of the CMMC is to combine various cybersecurity control standards such as NIST SP 800-171, NIST SP 800-53, ISO 27001, ISO 27032, AIA NAS9933, and others into one unified standard for cybersecurity."[11] According to Ellen Lord, DoD acquisition head, CMMC requirements will be included in Request for Proposals (RFPs) starting as early as Fall 2020.[12]

The final CMMC document is scheduled to be released in January 2020.[13]

iv. **Differences between DFARS 252.204-7012 and CMMC**
One large difference between DFARS 252.204-7012 and CMMC is which body can certify that companies' information systems are compliant. CMMC generally requires an outside certification body to validate that controls are appropriately implemented at each company. With NIST 800-171 compliance under DFARS 252.204-7012, companies can self-certify. The inherent issues with self-certification were drivers to create CMMC.

v. **Both CMMC and DFARS 252.204-7012 will likely continue to be required**
It is anticipated that both DFARS 252.204-7012 and CMMC will be separate requirements, and that both will be required by DoD contractors going forward. Also, even if a company does not have contracts with the DFARS 252.204-7012 requirements, all DoD companies will be required to be obtain CMMC certification. [14]

CAN MY COMPANY BE COMPLIANT WITH DFARS 252.204-7012 SOLELY BY USING A CLOUD PLATFORM FOR CUI THAT STATES THAT IT IS DFARS 252.204-7012, FEDRAMP, OR NIST 800-171 COMPLIANT, WITH NO OTHER WORK ON MY COMPANY'S END?

No, several DoD contractors have stated that they believe their internal information systems are compliant with DFARS 252.204-7012 simply because they are using a compliant cloud service provider. However, these cloud providers only provide a platform to theoretically enable an organization to meet the DFARS 252.204-7012 requirements. There will be further policy configuration and documentation required to be completely compliant. Specifically, DoD customers have been requesting System Security Plans (SSPs) and POAMs (Plan of Action and Milestones) that document how an organization is meeting the NIST 800-171 controls (*see for example* Table 1: Contract Data Requirements List[15]. Often times, a company can leverage their cloud provider's language for how the NIST 800-171 controls and other DFARS 252.204-7012 requirements are met, but the SSP must be specific to their organization.

Under DFARS 252.204-7012(2)(ii)(D), cloud services providers that DoD contractors use to process CUI must meet the requirements for FedRAMP Moderate impact level. "FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by the US government."[16]

i. **Some cloud platforms will have a very difficult time meeting sections of DFARS 252.204-7012 even if they can be configured to be NIST 800-171 compliant.**
Some popular cloud service providers do not meet sections (d) and (e) of DFARS 252.204-7012, which has to do with maintaining and providing images of systems that are breached during an incident to DoD.[17]

ii. **External Interfaces over which CUI Dataflow Occurs**
Often times, there are other systems that the cloud service provider interfaces with to exchange CUI, which could include local machines. The DFARS 252.204-7012 requirements must be levied on any systems that processes CUI outside of the cloud environment.

iii. **Tailored Software as a Service Cloud Providers for DoD Contractors**
Some cloud providers, such as Microsoft, have provided products tailored for the defense contractor market to meet DFARS 252.204-7012, such as Office 365 Government Community Cloud (GCC) High.[18] Such products also provide a platform to assist in International Traffic in Arms Regulations (ITAR) compliance that generally affects all DoD contractors. Naturally, these tailored products cost more per subscription.
In order to purchase Office 365 GCC High subscriptions, a company must "go through a validation process to ensure eligibility before an environment is established."[19] This validation process requires that each company show that it is a DoD contractor "with a requirement to manage CUI / ITAR data or who have the DFARS 7012 clause in one of their contracts."[20] This could be challenging for some small businesses that want to enter the DoD contracting space, but currently do not have any DoD contracts. Even these tailored cloud products generally require special configurations and continuous monitoring outside of the cloud provider's base offering.

WHAT COMPRISES THE SYSTEM BOUNDARY? DO ALL OF MY SYSTEMS HAVE TO MEET DFARS 252.204-7012 REQUIREMENTS?

i. **DFARS 252.204-7012**
The system boundary for DFARS 252.204-7012 could consist solely of a single workstation for a small organization. According to DFARS 252.204-7012(a), "'covered contractor information system' means an unclassified information system that is owned, or operated by, or for, a contractor and that processes, stores, or transmits covered defense information".[21] "Covered defense information" generally refers to CUI. A description of what constitutes the system boundary should be included in the SSP for the company's information systems that are intended to process CUI.[22]
It is also possible to have separate cloud-based services specifically for handling CUI. For instance, an organization that does a significant amount of commercial work might want to purchase a commercial Office 365 subscription for a majority of its commercial employees and purchase separate GCC High subscriptions for those employees who are working with DoD contracts. This approach would save the company money in subscription costs by only purchasing the more expensive GCC High subscriptions for those who are likely to access CUI.

Unfortunately, the Office 365 GCC High subscriptions will be treated as a separate tenant from the commercial Office 365 subscription.[23] This would require that those on the GCC High subscriptions use a different domain than those using the commercial Office 365 subscription. Also, documents will likely be harder to share across the tenants – the difficulty level associated with this will depend on the administrative configurations within each Office 365 environment.[24]

ii. **CMMC**
Unfortunately, there is still some uncertainty about the system boundary that will be required in CMMC.[25]

CONCLUSION

Even if a DoD contractor is not receiving CUI currently, there is a high chance that it either already needs to meet DFARS 252.204-7012 or will need to do so in the near future. CMMC will levy additional cybersecurity requirements. Additionally, a certain level of certification will be required in RFPs starting as early as Fall 2020. Generally, CMMC will require third party certification. Although cloud-based service offerings claim to be NIST 800-171 and DFARS 252.204-7012 compliant, additional work will be required on the part of the contractor to document compliance and implement appropriate administrative policies within the cloud service provider environment.

[1] https://www.archives.gov/files/cui/documents/20161206-cui-marking-handbook-v1-1-20190524.pdf

[2] https://isoo.blogs.archives.gov/2017/11/07/questions-and-answers-marking/; https://www.archives.gov/cui/registry/category-list

[3] https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf

[4] https://isoo.blogs.archives.gov/2017/10/23/questions-and-answers-cui-program/

[5] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

[6] https://www.doxnet.com/2019/04/government-cracking-down-on-dfars-nist-regulatory-compliance/

[7] https://www.doxnet.com/2019/04/government-cracking-down-on-dfars-nist-regulatory-compliance/

[8] https://www.insidegovernmentcontracts.com/2019/07/dod-announces-the-cybersecurity-maturity-model-certification-cmmc-initiative/

[9] https://www.acq.osd.mil/cmmc/faq.html

[10] https://www.acq.osd.mil/cmmc/draft.html; https://www.wileyrein.com/newsroom-articles-DOD-Releases-Draft-of-the-Cybersecurity-Maturity-Model-Certification-CMMC-Plan-Industry-Input-Sought.html

[11] https://www.acq.osd.mil/cmmc/faq.html

[12] https://defensesystems.com/articles/2019/09/05/dod-cyber-cmmc-rules-williams.aspx

[13] https://www.acq.osd.mil/cmmc/faq.html

[14] https://www.acq.osd.mil/cmmc/faq.html

[15]https://www.acq.osd.mil/dpap/pdi/cyber/docs/Assess%20Compliance%20and%20Enhance%20Protection%20of%20Contractor%20System%20%20with%20Attachments%2011-6-2018.pdf; https://www.sysarc.com/cyber-security/how-to-create-a-system-security-plan-ssp-for-nist-800-171/).

[16] https://www.fedramp.gov/cloud-service-providers/

[17] https://medium.com/@summit7sys/where-should-i-deploy-for-dfars-7012-compliance-office-365-commercial-or-office-365-gcc-high-b56dd5b0ef8d https://info.summit7systems.com/blog/compliance-decisions-platforms-part-1-does-google-g-suite-meet-dfars-nist-and-itar-security-requirements

[18] https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/office-365-us-government/gcc-high-and-dod

[19] https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/office-365-us-government/gcc-high-and-dod

[20] https://medium.com/@summit7sys/where-should-i-deploy-for-dfars-7012-compliance-office-365-commercial-or-office-365-gcc-high-b56dd5b0ef8d

[21] https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm

[22] https://www.complyup.com/3-steps-nist-800-171-compliance/

[23] https://info.summit7systems.com/what-is-office-365-gcc-high

[24] https://docs.microsoft.com/en-us/office365/enterprise/office-365-inter-tenant-collaboration

[25] https://www.wileyrein.com/newsroom-articles-DOD-Releases-Draft-of-the-Cybersecurity-Maturity-Model-Certification-CMMC-Plan-Industry-Input-Sought.html