MAIKA'I SOLUTIONS

CMMC OR BUST

April 30, 2025

Imagine if $5.2 billion disappeared from Hawaii's second largest industry. Based on state government numbers from Hawaii Defense Economy, that's how much the U.S. Department of Defense awarded to Hawaii's prime contractors in 2024, representing significant economic risk if all of them decided to wait until the last minute to implement actions to comply with Cybersecurity Maturity Model Certification (CMMC) contract requirements. Not to mention the socio-economic cost of losing the 66,400 jobs provided by these contractors, their subcontractors, and their families.

With increasingly sophisticated cyber-attacks targeting the defense sector, CMMC compliance helps protect sensitive information and supports national security. CMMC is designed to certify that contractors adequately protect Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). Contracts requiring CMMC will begin to appear in early 2025, with full CMMC implementation expected by October 2025. Without a valid CMMC certification, companies risk losing existing contracts or being ineligible for future opportunities.

"Contractors who don't abide by the CMMC requirements unfortunately won't be awarded new contracts," says John Greene, Deputy Director for the Military and Community Relations Office, a Hawaii-based office funded through the Office of the Secretary of Defense. Greene emphasizes that there are no exceptions. "From a prime contractor's perspective, the CMMC clauses are what's called 'flow-down' clauses, so they apply to their subcontractors as well,'" he says.

It's a myth that only contractors who handle classified information are subject to this regulation. "You could be landscaper, and even though you're not necessarily working on secure information, you're still beholden to Federal Acquisition Regulations (FAR), which contain basic cybersecurity requirements." That applies across the board for all federal contracts, not just the Department of Defense. Information needing protection could include where the contractor performed the work, where they stored records, what systems they had in place, and who has access to those systems.

"It's incumbent upon our local contractors to understand the types of contracts that they currently have or want to pursue. You don't want to, one, lose an existing contract, and you certainly don't want to lose opportunities for future contracts because you haven't done your work to be compliant in time," says Greene.

“While I’m not 100% certain that noncompliance will totally remove Hawaii businesses, that does give greater opportunities for mainland businesses to come in and get those contracts previously provided to local businesses,” Greene noted, adding that there is no federal procurement requirement that a contractor be located where the scope of services are going to be performed. “So there's always that potential that contracts can be awarded to the mainland businesses.”

This has happened before, as non-compliance with government regulations similar to CMMC have lost bids for large projects. For example, contractors bidding on hundreds of millions of dollars in cleanup work for the Lahaina wildfires were required to attest to complying with NIST 800-171 requirements, the baseline security standard for CMMC certification. Those unable to do so were deemed unqualified. Before CMMC becomes enshrined in contract requirements, the DoD can ask contractors to self-attest compliance with NIST SP 800-171 and ask for a System Security Plan.

Serious Enforcement

Eventually, all companies on contract with the DoD will need at least CMMC Level 1 certification. Certification cannot be outsourced to just any consultant. “You can't just become a certified third party because you said you are,” says Greene. Independent companies called Certified Third-Party Assessment Organizations (C3PAO) must certify companies against the different CMMC standards/levels. The Cyber AB is the official accreditation body for C3PAOs, providing a list of assessors on its website.

Greene says that the good news is that the federal government’s cybersecurity standards are consistent. “Every contractor has to meet the same requirements, and every C3PAO certified third party assessor is using the same assessment to do your assessment. They're looking at the same qualifications, the same boxes that need to be checked for every small business or every business regardless of size.”

For those who are still on the fence, he warns that the Department of Justice’s Civil Cyberfraud Initiative has already begun pursuing contractors who don’t comply with stringent cybersecurity requirements imposed by the federal government. “There’s actual enforcement going on here. It’s not just a check-the-box kind of requirement,” says Greene. Pennsylvania State University, for example, agreed to pay $1.25 million for failing to implement NIST SP 800-171 controls required for safeguarding Controlled Classified Information (CUI). The DOJ has also filed suit against Georgia Tech, alleging that the university knowingly failed to meet contractual cybersecurity requirements “If it can happen to large universities who have hundreds of millions of dollars in resources, it can certainly come to large and small businesses who are contractors and subcontractors for DoD projects,” he adds.

He has seen this complacency throughout his career assisting businesses with federal contracts. “Don't be surprised if you lose your contracts or you're not able to compete for future contracts. Someone else will take your place,” says Greene. He warns that contracting officers can consider noncompliance the same as not performing under the terms of the contract. “Contracting officers look at your past performance. Chances are that they are going to see that and say, ‘I'm not going to risk giving a contract to someone who's been non-compliant in the past,’” he says.

The DoD confirmed in January 2025 that CMMC requirements will be assessed at the pre-award phase. Additionally, CMMC Level 1 and Level 2 SPRS reporting is now open, meaning businesses can start submitting their self-assessments. The big caveat here is that a Senior Official from the company with the authority to affirm their continuing compliance with the security requirements for their organization must sign the attestation. Signing the attestation is a formal declaration that the senior official is taking personal responsibility for the accuracy of this statement, stating that they are actively engaged in compliance matters. Questions about the validity of this declaration can have legal consequences.

Opportunities for Early Adopters

Companies that don't work directly on classified information may not think that they are affected by this contract requirement. However, NIST 800-171 has been a contract requirement since 2017 [DFARS 7012 and 7020]. Early adopters should start with this baseline requirement.

For those who need more information, Greene says CMMC compliance resources are readily available online. "It's not just the DoD, you have other federal agencies like the Department of Energy, Department of Homeland Security, that are also making sure contractors are CMMC compliant. So if I was a small business, even if I don't currently work with controls on classified information, I certainly want to be aware of what the requirements are, if I wanted to compete in that arena." Within the state, DBEDT sponsors a program called CyberSafe Hawaii that assists all eligible small businesses with the basics of cybersecurity.

He advises those with existing contracts to communicate with their contracting officer or representative handling the work performed on that contract to find out what is changing in the contract. "I would say, at least 90 days out, my recommendation is to have that conversation with the contracting officer and say, 'Hey, are there things changing with regards to CMMC compliance that I should be paying attention to now?'"

In return, early adopters of CMMC compliance may gain a competitive edge if others decide to wait. "We don't necessarily see defense spending in our state decreasing. In Hawaii, there are large projects that are currently ongoing. We anticipate some of them to continue, and new projects to come into Hawaii," he says. Meeting the federal government's stringent cybersecurity standards could help contractors diversify their client base across the private sector as well, he added: "I would say, if you are CMMC-compliant, it probably gives you an advantage over your competition. If you're in the private sector and you already met those requirements for the federal government, you're probably more attractive contracting partner to financial institutions or healthcare institutions."

"Don't be surprised if you lose your contracts or you're not able to compete for future contracts. Someone else will take your place," says Greene.

For small and mid-sized contractors, the path to compliance isn't always straightforward, and not all providers get it right. Many firms sell "compliance in a box," but the reality is far more nuanced. Getting it wrong can cost you contracts, credibility, and your future in the federal space.
Maikaʻi Consulting Solutions understands what's at stake and how to get it right. If you're serious about staying competitive and secure, let's talk.