PROCORE | CONSTRUCTIONDIVE

Custom content for Procore by Studio by Informa TechTarget

How to Win Government Work:

Ease the Heavy Lift of Meeting CMMC Compliance Standards

SPEAKERS



Kris Lengieza
FIELD COO
PROCORE



Marti Smith
CIO
BRASFIELD AND GORRIE



Aaron Geiger
FIELD CTO
PROCORE

A recent influx of federal funding into public projects has increased interest in pursuing government contracting opportunities. However, bidding on federal jobs involves data security requirements that differ from most commercial work. Many contractors are unsure of the requirements to qualify for government contracting work, much less the changes required in their processes and workflows before they can bid.

In a recent Procore-sponsored Construction Dive webinar, Procore Field COO Kris Lengieza spoke with panelists Aaron Geiger, Field CTO at Procore, and Marti Smith, CIO at Brasfield & Gorrie, to discuss how contractors can set themselves up for competitive bidding on government contracts.

CERTIFICATION REQUIREMENTS

By Oct. 31, 2026, all contracts with the Department of War / Department of Defense will require the appropriate Cybersecurity Maturity Model Certification (CMMC) certificate.

CMMC is a defined set of cybersecurity requirements designed to protect sensitive government data from threat actors around the world.

There are three levels of compliance under CMMC. Level one is a basic level of security compliance. Level two involves what contractors will most commonly see on federal projects, known as controlled unclassified information (CUI). The third level involves "higher-level protection of CUI against advanced persistent threats," according to the Department of War.

For level two contractors, CMMC contains restrictions that differ from most commercial projects, including stricter controls regarding printing materials and inserting storage devices into computers. Furthermore, CMMC compliance rules apply not only to the general contractor, but also to every person and company touching project data, all the way down the supply chain.

Cybersecurity Maturity Model Certification

LEVEL 1
BASIC SECURITY COMPLIANCE

A foundational level of cybersecurity hygiene required for any contractor handling federal contract information (FCI).

LEVEL 2
CONTROLLED UNCLASSIFIED INFO

Most commonly seen on federal projects. Stricter controls than commercial work, including restrictions on printing materials and inserting storage devices into computers.

Applies throughout the entire supply chain: Compliance rules extend to every person and company that touches project data, not just the general contractor.

LEVEL 3
ADVANCED THREAT PROTECTION

Higher-level protection of CUI against advanced persistent threats, according to the Department of War.

Geiger shared an example of the increased requirements for government work: Bonding requirements for government projects have lower triggers than commercial projects and demand greater financial scrutiny. Beyond those initial requirements, agencies layer on their own processes that must be followed.

Contracting organizations must have their people, processes and technology nailed down to meet the higher-level requirements for government work, win bids and continue on to deliver successful government projects.

Lengieza pointed out that contractors who regularly work on government projects become extremely knowledgeable about the various requirements of agencies and municipalities, as well as what's needed to be successful. Fortunately, what makes contractors successful on government projects, in many cases, lines up with standard good business practices.

"Every owner is ultimately trying to answer the same question, whether they're government or commercial: Can I trust this contractor to manage my project?" Smith said.

> **"The contractors who consistently win the contracts are the ones that can prove that they have their processes, technology and people in good order."**
>
> MARTI SMITH, CIO, BRASFIELD AND GORRIE

Knowing that, Smith said, Brasfield & Gorrie made the conscious decision to raise baseline security protocols on their business practices across projects, including tighter data handling and stronger access control. Then, the firm only needed to add specific requirements for the federal groups, teams and projects that required them.

Change Management

Making fundamental changes within a big company is a huge undertaking. The first step is to reframe the challenge to get buy-in across the company. Make it clear that CMMC compliance is not just an IT project. While technology is critical to the change, it serves a supporting role to the behavior changes that need to occur. When Brasfield & Gorrie brought in the risk department as a true partner, Smith said, it changed the way everyone saw the compliance process.

Furthermore, the systems and technology aren't standalone compliance fixes. Workers at all levels need to understand the value in the changes so they'll willingly participate in and even help set up the systems that keep the company compliant.

"The advantage in construction is that our business is managing risk. When you frame it as a risk project, the business knows how to attack it.

AARON GEIGER, FIELD CTO, PROCORE

To navigate this transition effectively, consider the following approach:

FIND PEERS AND MENTORS

Geiger and Smith each suggested an essential first step in a company's transition to CMMC compliance: Find peers and mentors who can help avoid the larger pitfalls. Consultants or other experienced partners can offer guidance and expertise to take the pressure off employees.

"You have to map your document flows. Understand where CUI information enters, who touches it and where it goes. That exercise will surface your highest-risk behaviors."

MARTI SMITH, CIO, BRASFIELD AND GORRIE

BREAK THE PROCESS INTO MANAGEABLE STEPS

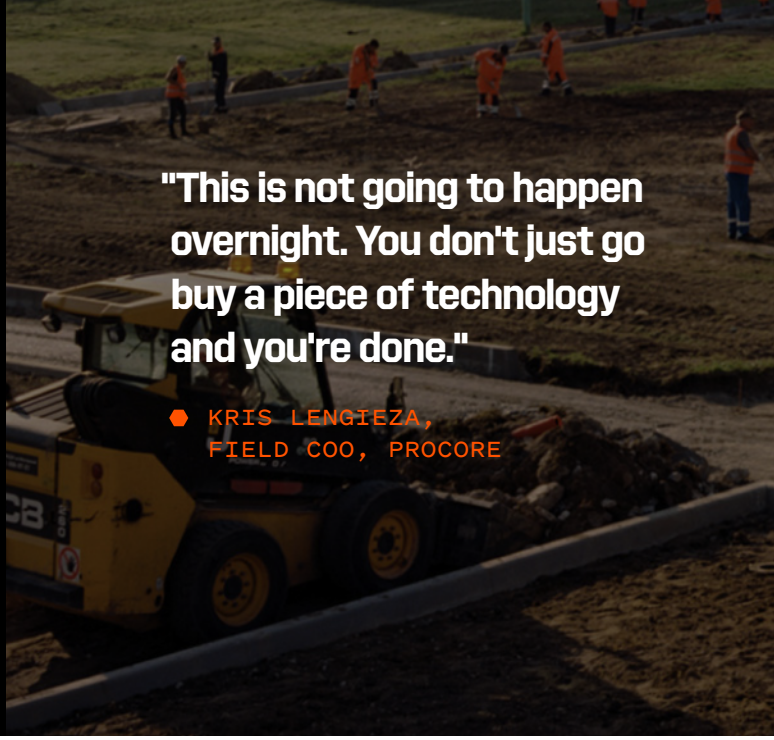
Once you have the right support in place, Smith suggested following a three-part certification process towards compliance:

1. Build a solid technology foundation. This helps improve business practices across the board. "We did a complete evaluation of where we were against that CMMC-compliant environment," Smith said.
2. Create a compliant enclave. With that baseline established, the team then created a separate enclave that met CMMC standards and, finally, compared the rest of their operations to it.
3. Compare and assess. Beyond the technical infrastructure, field teams can have a huge impact on designing and adapting new compliant processes that won't disrupt the flow. Once processes are established, all employees need to feel comfortable handling CUI appropriately, with ingrained habits around how they share, store and move information. Training should include scenarios inside a protected enclave that test team members' ability to handle CUI.

As part of the process, Smith's team underwent a third-party assessment to judge their readiness for a CMMC compliance review.

TREAT IT LIKE A PROJECT WITH PHASES AND MILESTONES

Most organizations are adept at planning and executing projects, so CMMC compliance should be treated like any other project, complete with phases and milestones. "It's not something you just flip the switch on," Lengieza said. Instead, the process will require ongoing auditing and training as the business acclimates to the new procedures.



> **"This is not going to happen overnight. You don't just go buy a piece of technology and you're done."**
>
> KRIS LENGIEZA, FIELD COO, PROCORE

How Technology Can Help

Many contractors manage the increased compliance requirements for government work by simply separating the protected documents. They use a management platform to handle their processes and project management, and place documents with higher security needs in a protected file storage system. The challenges with this approach are similar to any other disconnected management method: The resulting lack of visibility and collaboration can create errors, add costs and create delays. In these legacy systems, it's also common to have a specific subset of staff trained and working on government projects.

With a fully connected, FedRAMP® Class C Certified construction management platform like Procore for Government, teams can use the same platform they're familiar with, with a few changes to meet the more stringent security requirements. People and projects are connected for better quality data, collaboration and outcomes.

For more insights from this discussion, including best practices for adopting technology solutions, access the full webinar from Construction Dive's resource library.

Watch Webinar

PROCORE | CONSTRUCTIONDIVE