Preparing for CMMC: A Primer for Contractors Working in the Defense Industrial Base

As the leading provider of project management information systems (PMIS) to the federal government and as the first full-featured PMIS provider to achieve FedRAMP authorization, Kahua is best positioned to help U.S. contractors properly secure project data.

Working with our ecosystem of partner companies, Kahua can help contractors meet the Cybersecurity Maturity Model Certification (CMMC) requirements, which will be rolled out in 2025.

CMMC is a security framework designed to protect sensitive unclassified information, such as Controlled Unclassified Information (CUI), that is shared with defense contractors. CMMC builds upon existing cybersecurity frameworks, including NIST SP 800-171, and introduces a maturity model with three levels of cybersecurity practices.

In many cases, CMMC also mandates third-party certification, ensuring that contractors have implemented appropriate cybersecurity measures. Starting in 2025, all DoD contractors and subcontractors will be required to achieve a certain CMMC level, depending on the nature of their contracts.

FedRAMP provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services used by federal agencies. The primary goal of FedRAMP is to ensure that cloud service providers (CSPs) meet stringent security requirements to protect federal data. FedRAMP streamlines the process for agencies to adopt cloud services, ensuring that these services comply with federal security standards.

FedRAMP's requirements are based on the National Institute of Standards and Technology (NIST) Special Publication 800-53, which outlines security and privacy controls for federal information systems and organizations. The program categorizes cloud services into three impact levels: Low, Moderate, and High, each with specific security control baselines. CSPs must undergo rigorous assessment by a third-party assessment organization (3PAO) to achieve FedRAMP authorization.

By leveraging FedRAMP-compliant software like Kahua to manage project information, construction industry contractors and subcontractors can streamline their path to CMMC compliance. As Shane Peden – Managing Director of Information Assurance Services at Aprio –said,

> **"Kahua provides a CMMC-compliant solution to help you achieve scope reduction and accelerate your path to CMMC compliance."**

Let's look at some practical steps that you can take so that your organization is prepared for the forthcoming requirements.

Practical Steps for Construction Contractors

To leverage the benefits of FedRAMP compliance in meeting CMMC requirements, construction industry contractors should consider the following steps:

1

Evaluate Current Cybersecurity Posture

Conduct a thorough assessment of your current cybersecurity practices and identify any gaps relative to CMMC requirements. This assessment will help prioritize areas for improvement and guide the selection of FedRAMP-compliant software solutions.

2

Choose FedRAMP-Compliant Cloud Services

Select cloud service providers that have achieved FedRAMP authorization. These providers have already demonstrated their ability to meet stringent security standards, reducing the burden on contractors to establish and maintain these controls independently.

Learn more about FedRAMP-authorized solutions at https://marketplace.fedramp.gov/products. Use the filters at this site to distinguish between solutions authorized and those seeking authorization. There's a big difference.

3

Develop Comprehensive Documentation

Ensure that all security controls and processes are well- documented. This documentation will be essential for CMMC assessments and can leverage the existing documentation provided by FedRAMP-compliant CSPs.

4

Implement Continuous Monitoring

Adopt continuous monitoring practices to maintain the security of your systems over time. This approach aligns with FedRAMP requirements and supports the ongoing improvement of cybersecurity practices outlined in CMMC.

5

Engage with C3PAOs for CMMC Certification

Begin the process of engaging with CMMC Third-Party Assessment Organizations (C3PAOs) to schedule assessments and achieve the required maturity level. Early engagement can help ensure a smooth transition to CMMC compliance.

To learn more about C3PAOs and find a list of authorized providers visit cyberab.org.

Conclusion

CMMC requirements are coming and will be required starting in 2025. Compliance is a stringent and expensive process, but using a FedRAMP PMIS reduces this effort. Kahua is the leading PMIS to the federal government, already serving dozens of agencies, and is the first FedRAMP authorized provider. Connect with Kahua and our ecosystem of partner companies to start a conversation that will help your company get ready to win while your competitors struggle to meet these standards.

Choose Kahua

Kahua is a leading provider of capital program and construction project management software, enabling innovation that is changing the way that capital programs are planned and delivered. Global organizations use Kahua's collaborative solution to improve efficiency, lower costs and reduce project risk throughout the entire lifecycle of their capital programs. Our purpose-built solutions for owners, program managers and contractors enable rapid implementation that minimizes time-to-value and enhances user adoption. With the industry's only low-code application platform, customers can easily customize existing Kahua apps or even build their own new apps to run their business at peak efficiency today and rapidly adapt as business conditions dictate.

Learn more and request a demo today or email us at: connect@kahua.com

OCT 2024