Verkada

# Support Cybersecurity Maturity Model Certification (CMMC) Readiness with cloud-managed physical security

*For organizations across the Defense Industrial Base, physical security is an important part of the broader CMMC readiness picture. Verkada helps teams address specific Physical Protection requirements through facility monitoring, visitor management, physical access control, and auditability with government-grade solutions designed for secure, scalable deployments.*

## Why CMMC matters

CMMC is the Department of Defense's framework for verifying that contractors and subcontractors have implemented required safeguards for sensitive information. At Level 2, CMMC incorporates NIST SP 800-171 requirements, including Physical Protection controls related to limiting physical access, monitoring facilities, escorting visitors, maintaining physical access logs, and managing access to secure areas and devices. Under CMMC 2.0, cloud software handling Controlled Unclassified Information (CUI) must meet FedRAMP Moderate or equivalent security requirements, making physical security only one part of the broader readiness picture.

### After FedRAMP Authorized

Under CMMC 2.0, cloud software handling Controlled Unclassified Information (CUI) must meet FedRAMP Moderate or equivalent security requirements. With FedRAMP Authorization, Verkada customers may be able to inherit applicable controls rather than independently implementing them.

## How Verkada helps support physical security readiness

### Control facility access

Verkada's government-grade access control helps organizations manage who can enter sensitive areas, assign permissions by role, support PIV-related workflows, and strengthen protection for higher-security zones with options like PIN-plus-badge authentication. Teams can also centralize door management across sites without on-prem servers or complex databases.

### Monitor facilities and support infrastructure

Verkada's government-grade cameras help security teams protect and monitor facilities with 24/7 recording, FIPS 140-validated encryption, AI-powered alerts, and faster investigations across distributed sites. Teams can remotely access footage, search across people and vehicles, and share video when needed for incident response.

### Manage visitors and maintain auditability

Verkada Guest on AWS GovCloud helps streamline visitor check-ins, capture photo IDs, maintain digital records, and pair visitor activity with video context. Together with access control, Verkada can help organizations build a more auditable approach to visitor management and physical access events.

### Simplify operations across sites

Because Verkada is cloud-managed, teams can oversee users, devices, and sites from one platform, with remote access from supported browsers and devices, automatic firmware updates, and no need for NVRs or DVRs. That can reduce operational burden while helping security and IT teams stay responsive.


## Built for government-grade deployments

- Command hosted in AWS GovCloud
- FedRAMP In Process at the Moderate impact level
- Zero Trust architecture
- FIPS 140-validated devices
- TAA and FY2019 NDAA compliant hardware
- SOC 2 Type 2
- ISO 27001, 27017, 27018, and 27701
- Granular roles and permissions
- Remote management across distributed sites

**Hosted in AWS GovCloud**

**TAA Compliant**

**FIPS 140 Validated**

**SOC 2 Type 2**

**FedRAMP Authorized**

**FY2019 NDAA Compliant**

**Zero Trust Architecture**

**ISO 27001, 27017, 27018, and 27701**

Learn how Verkada helps defense contractors and government-focused organizations modernize physical security with government-grade video security, access control, visitor management, and centralized cloud-based management.

**Disclaimer**

*This document is available for informational purposes only, and does not, and is not intended to, constitute legal advice. Verkada helps support physical security requirements as part of a broader CMMC readiness strategy. CMMC assessments and certifications are determined at the organization and system level and may vary based on contract requirements, environment, and scope. Consult your legal team for specific compliance guidance.