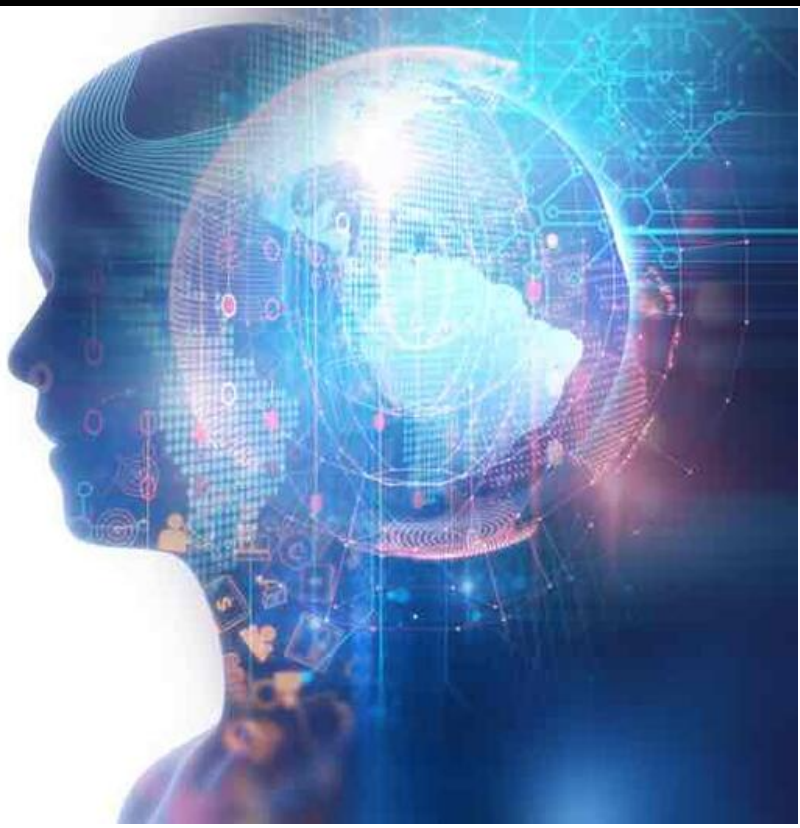
DevilDog CYBERSECURITY AUTHORIZED DEALER

ignite AI Transformative Intelligence

Automation That makes a Difference

Cyber Security-CMMC Compliance for DOD CONTRACTORS and Sub CONTRACTORS



www.ignite-ai.com

If you do any work with the U.S. Department of Defense (DoD), then you have surely heard about the Cybersecurity Maturity Model Certification (CMMC). With requirements beginning to show up in projects as early as September, you may have questions about compliance and requirements so you don't lose out on future contracts with the DoD.

We have provided an overview of the standard and laid out the steps you need to take now to make sure you're checking off all of the CMMC boxes.

What is the Cybersecurity Maturity Model Certification (CMMC)?CMMC is a unified standard for implementing cybersecurity across the defense industrial base (DIB). With more than 300,000 companies in the supply chain, there is a large number of companies that need to comply with this new standard.

Prior to the CMMC standard, contractors were responsible for the implementation, monitoring, and security certification of their IT systems, as well as any confidential or sensitive information stored on or transmitted by their systems. Much of this was covered by the Defense Federal Acquisition Regulation Supplement (DFARS). DFARS has been in effect since 2016 as a means to better protect Controlled Unclassified Information (CUI).

All DoD contractors and subcontractors must meet DFARS regulations, and compliance is relatively simple to understand—organizations must have the proper security protocols in place to protect CUI, and you must have a process in place to report cybersecurity events.

CMMC is similar to DFARS in many ways, but compliance is divided into maturity levels and companies must undergo an assessment by a third party (self-assessment is no longer an option). The assessment will ensure they are compliant with certain practices and procedures to certify that the proper controls are in place to protect sensitive data. The goal is to make sure that contractors are capable of defending against and responding to the ever-changing cybersecurity landscape, as new threats constantly emerge. While details are still being ironed out, all indications are pointing to CMMC eventually completely replacing DFARS as the requirement needed for DoD contracts.

CMMC compliance standards consist of several pre-existing compliance processes and procedures combined into one framework:

NIST SP 800-171—Governs CUI in non-federal information systems and organizations. CUI is information that is sensitive, but not classified. NIST SP 800-53—Provides standards and guidelines for federal agencies to architect and manage their information security systems. ISO 27001—Provides requirements for an Information Security Management System (ISMS). ISO 27032—Provides guidance for improving the state of cybersecurity.AIA NAS9933—Regulates the requirements for aerospace cybersecurity.Federal Information Security Management Act (FISMA)—A law requiring federal agencies to develop, document, and implement an information security and protection program.The standard has been in the works for several years, and the first version of the CMMC was finally released on January 31, 2020. By September of 2020, contractors should expect to see CMMC requirements in the Request for Proposal (RFP) process. Starting in October, DoD contractors will need to get certified by an accredited assessor.

While a full timeline of compliance is not yet available, CMMC requirements will apply to all DoD contractors, including all companies throughout the supply chain. There is a chance that smaller contractors or subcontractors may not be required to obtain the highest level of compliance, but our best advice is to prepare for a high level of compliance now so you don't risk missing out on projects.

The CMMC Accreditation Body (CMMC-AB) is in charge of developing procedures to certify Third-Party Assessment Organizations (CP3AOs) and assessors that will be in charge of evaluating compliance levels. The CMMC will also set up a CMMC Marketplace where companies will be able to go and find an accredited C3PAO and schedule an assessment.

Assessments will be based on the level designated by the requesting company. There are five levels of CMMC certification:

Level 1: Basic cyber hygieneLevel 2: Intermediate cyber hygieneLevel 3: Good cyber hygieneLevel 4: ProactiveLevel 5: Advanced/ProgressiveEach level builds upon the one beneath it, meaning that in order to meet Level 2 compliance, a company must also meet all Level 1 requirements.

The CMMC model as a whole consists of 17 domains.

Access control Asset ManagementAwareness and training Audit and accountability Configuration management Identification and authentication Incident Response Maintenance Media protection Physical protection Personnel security RecoveryRisk managementSecurity assessment Situational awarenessSystem and communications protection System and information integrity

The distribution of practices within each domain varies across the compliance levels, but the majority of all practices required fall under access control, Audit and accountability, incident response, risk management, system and communication protection, and system and information integrity.

Ignite-AI specializes in making cybersecurity easy with complete customized security solutions from start to finish with our preferred partner. Our customized solutions are cost-effective and can be expedited depending on your timeline. Ignite AI's cyber partnership offers a full suite of services that include vulnerability assessments, scanning, pen testing, managed services, compliance audits, authentication and cloud security solutions. In addition, we can also implement a robust cyber security program that can manage your whole infrastructure with 24/7 monitoring or even create a custom solution in the cloud that meets all government compliance regulations. Understanding Compliance Compliance regulations are confusing, and many companies do not know where to start. We have access to many subject matter experts in cybersecurity compliance. Our team understands government regulations and knows exactly what your firm will need to be compliant. We can help your business to meet all regulation standards quickly and prepare your company to pass any audit..

A partnership with Ignite-ai begins with a free compliance assessment and Gap Analysis Report. This includes a vulnerability assessment to find any glaring holes in your IT infrastructure or DNA (Databases, Networks and Applications).

The Gap Analysis Report gives clients a step-by-step roadmap to meet government specifications and addresses all current pressing issues. This report shows firms their current cybersecurity posture and how to meet government standards.

Here's how a partnership with Devil Dog& Ignite-AI works. Once we have done our initial assessment and implemented a solution for compliance, we show up every three months for a Quarterly Business Review (QBR) that outlines your current status in compliance. During our QBR we scan, re-assess and provide you with a current report. Then we help you with updates, plug the holes and fix any issues. We assess your DNA – databases, networks and applications. A relationship with our Cyber Partner will ensure a resilient cybersecurity posture and maintain your compliance standards.

CMMC

ISO 27000

NIST 800-171

NIST 800-53

FISMA

FedRAMP

FIPS 199 & 200

GDPR

Data Privacy

HIPAA

SOC-Security Operations Center

Industry Leading SLA's

24/7/365 Eyes-on-Glass Monitoring

Dedicated Security Analysts

Real-Time Threat Detection and Response

Cloud SIEM Correlation and Analytics

Security Best Practices Training

Onsite & Web Based Training

Customized Training

Cybersecurity Policy Development

Risk Management Frameworks & Policy

Documentation & Attestation

Secure Authentication Frameworks

Secure Identity Policy Development

Multi-Factor Authentication

Single Sign On

Multi-Platform Authentication

Administrative Security Controls

Technical Security Controls

Compliance Specific Controls

Compliance Solutions for DoD Contractors and Subcontractors

ABOUT Ignite-AI

OUR MISSION

Ignite-AI has developed full Cyber Security partnerships specializing in compliance for DoD Contractors and Subcontractors. Our solution can get most firms NIST 800 171 and CMMC compliant in as little as three months. We offers a cost-effective subscription model that makes compliance both easy and affordable. Our current promotion for DoD contractors and subcontractors includes a Free Vulnerability Assessment and Gap Analysis.

FREE VULNERABILITY ASSESSMENT AND GAP ANALYSIS REPORT The Gap Analysis Report gives subcontractors a step-by-step roadmap to compliance and addresses all current pressing issues in your cybersecurity. This report shows you where your company's cybersecurity posture currently stands, and how to get compliant.

AFFORDABLE SUBSCRIPTION MODEL DevilDog's subscription model allows companies to achieve compliance right away, and ensures that compliance is maintained throughout the entire term of the subscription. We offer a wide range of affordable solutions to secure your infrastructure and provide you with all supporting documentation.

QUARTERLY REVIEW Every quarter our clients undergo a formal cyber security review. This review is designed to ensure your continued compliance due to new threats, changing environments, and investigates any malicious activity. This Quarterly Cyber Report also includes multiple vulnerability scans at different time intervals. The report is designed to assess any activity and updates that may have occurred over the quarter. 800.498.1295 devildogcyber.com 1401 Lawrence St, Suite 1600 Denver, CO 80202

HOW WE SIMPLIFY COMPLIANCE

COMPLIANCE IN 3 MONTHS Our solutions are fast, robust, resilient and ever-evolving to ensure your company passes any audit. DevilDog's cybersecurity consultants first analyze your infrastructure and systems. Once the analysis is complete, we begin creating the documentation and implementing the necessary protocol to ensure that your firm is compliant ASAP.

Our goal at Ignite-AI is to provide DoD contractors and subcontractors with a fast, affordable and robust solution in order to obtain and maintain compliance. We are your cybersecurity watchdog so your company can focus on its core business.

Ignite-ai can help you with:

Government Compliance Risk Assessment

Network Security Monitor 24/7

Cloud Services Training & Education

Policy Documentation Authentication Solutions

- **Information Security Policy,** defining the standards and processes your business uses to secure your network and data.
- **Technology Acceptable Use Agreement,** articulating acceptable employee uses of your business's technology, in addition to the consequences of misuse.
- **Business Continuity Plan,** demonstrating to your clients, shareholders and partners that your business is prepared for the worst.
- **Tabletop Business Continuity Exercise,** challenging the integrity of your plan in a safe environment, with a written recap advising opportunities for improvement.

CLOUD SECURITY MADE EASY

- The WatchDog Cloud is one of the simplest turn-key solutions for organizations looking to migrate to the cloud. With this solution, we can have your business totally compliant and secure in our WatchDog Cloud Solution for your Databases, Networks and Applications (DNA). Our simple solution will help you migrate and run your IT infrastructure from a cloud that meets all government compliance requirements.
- Cloud technology provides convenient access to data anywhere, anytime on any device. The security team goes to great lengths to make sure your data and operations in the cloud are secure. There are different cloud providers in the marketplace and our turn-key cloud solution is compatible with all of them.

- CLOUD PARTNERS
- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform
- IBM Softlayer
- Rackspace

AUTHENTICATION & IDENTITY ARCHITECTURE

In the current market, traditional IT cybersecurity countermeasures are not sufficient to protect against attacks. In some cases, countermeasures can trigger network compromises, denial of services and security breaches.

Cybersecurity risks are created in a multitude of ways, but some of the most common risks are introduced by:

- personnel, disgruntled employees, contractors and insiders who seek to damage systems and steal intellectual property
- professional cyber thieves who steal and sell information
- adversarial nations or groups who use the Internet for cyber warfare, IP theft and civil disobedience

Insiders pose a serious threat because they often already have access to the system and sometimes possess legitimate reasons to misuse computer systems, extend their privileges, and impersonate other users. Outsiders can use the Internet, remote access, and partner network tunnels to penetrate your network and even you facilities. Attackers exploit any and all vulnerabilities by using a variety of techniques and tools to probe networks, publicize targets, stifle operations, gain business advantage and promote causes.

IDENTITY SOLUTION

AAA

Federated Identity

SSO

SAML

Oauth

OpenID

Kerberos

Active Directory

OpenLDAP

Biometrics

Multi-Factor Authentication

Context-Aware Authentication

Smartcards

Tokens

DATABASE, NETWORK & APPLICATION (DNA) SECURITY

You are likely familiar with security devices such as Firewalls, IDS/IPS, Anti-Virus, etc. Perhaps you even have dedicated staff members who manage those devices. If so, that's great! We can work with your team to make necessary adjustments and ensure compliance. If not, we will deploy, configure and manage the entire IT infrastructure and make sure it is compliant and up to speed.

Our people, processes and technology can provide your business with Confidentiality, Integrity and Availability (CIA) in all your daily operations - databases, network and applications. Our CIA Triad is the cornerstone to any effective cybersecurity policy.

The CIA Triad may sound abstract, but it is actually quite tangible. We work with your organization to implement multiple types of security controls.

- Physical controls, which are things like fences, locks, badges and even fire extinguishers.
- Technical controls, such as firewalls, intrusion prevention systems, mobile device management, secure networking devices and workstation protection tools.
- Administrative controls, including policies and procedures that show how you comply with the government regulations.

We'll handle all of this for you, and continuously monitor the system while you work.

SECURITY CONTROLS

Firewalls

Maintenance

Fencing

Badge systems

Surveillance cams

Identity and access Management

Intrusion Prevention Systems

Anti-Virus

E-mail security

Database security

Data in transit and at rest security

Website protection

OSI Layers 1-7 protection

SIEM-Security Information Event MGMT

Configuration management

Vulnerability scanning & Management

Red teaming, blue teaming, purple teaming

Table-top exercises

SOC-Managed Security Operations Center

Security and Awareness Training

Server, workstation & mobile device security

CONTACT US

ADDRESS

13395 Voyager Parkway #130
Colorado Springs, CO 80921

HOURS

Mon-Fri 8AM to 5PM MST Weekends closed

E-MAIL

djoddy@ignite-ai.com

WEBSITE

www.ignite-ai.com

Automation that makes a difference

PHONE

(720)436-2152

ignite AI
Transformative Intelligence