CYBER SECURITY
SOLUTIONS

Solution Guide: CMMC Compliance

Implementing Security and Compliance Services for Government Contractors

CMMC@securedbycss.com || www.securedbycss..com || (813) 336-8175

Introduction

Today there are cybersecurity threats that occur across all industries, but government contractors are often times targeted and impacted the most. With adversary attacks on the rise, and happening in to higher profile companies, the government is placing more strict security measures in play. It is to no suprise that this is happening, from 2016 to 2018 nearly 6 percent of US military and aerospace contractors reported data breaches.

NIST SP 800-171 was a good start to laying out proper security requirements, however due to self-certifications and much needed updates to enforce additional controls we are now entering the CMMC era. CMMC is the new Cyber Security certification that is taking the Department of Defense (DoD) by storm. The new mandate requires all Federal contractors, prime and subcontractors, to be validated by a CMMC Accreditation Board (AB) approved Certified Third-Party Assessment Organization (C3PAO).

The days of being “self-certified” to NIST 800-171 standards are a thing of the past, now the 300,000+ organizations registered to bid on RFP’s for the DoD must become CMMC compliant. There are 5 levels of CMMC certification, the level you obtain compliance with is determined by the scope of work your organization normally develops proposals for.

What to Know About CMMC

Cost of Implementation

There are associated costs to implement CMMC. A few to consider are: initial audit, SSP and POA&M development, policy and procedure updates, CUI protection plans, future maintenance plans, network monitoring, equipment upgrades, cyber training, final C3PAO audit for certification, etc.

Official Audit Required for Certification

One of the biggest changes from NIST SP 800-171 to CMMC accreditation is the new format for certification audits. The CMMC Accreditation Board will approve CMMC Third Party Assessment Organizations (C3PAOs) to conduct final audits for certification.

Levels of Implementation

There are now 5 different levels of implementation, where each level adds additional security measures and controls. While DoD is requiring companies to meet Level 1 at minimum for RFP response, the level your organization chooses to implement depends on the security requirements of the contracts that your company pursues.

Additional Security Control Implementation

Levels 1 & 2 do not add any additional controls outside of the 110 NIST SP 800-171 requirements. Level 3 requires a total of 130 controls, Level 4 requires 156, and the top tier Level 5 requires a total of 171 controls. It is important to research the newly added CMMC controls to understand any additional practices that your organization may face.

Implementation Risk Reduction via Outsourcing

DoD contractors who have the necessary resources can opt to prepare for CMMC in-house. If you don't have the skills or resources to address NIST and CMMC requirements, it may be time to consider outsourcing the job to a capable cybersecurity firm like Cyber Security Solutions (CSS).

How Government Contractors Obtain and Maintain Compliance

It is safe to say that if you are compliant with NIST SP 800-171 that there is a good chance that you are compliant with nearly two-thirds of the CMMC requirements. The next few pages introduce the services and solutions that Cyber Security Solutions (CSS) can provide to help your organization obtain and maintain CMMC compliance.

CSS CMMC Services

Complimentary Network Vulnerability Scan

That's right you read it correctly, complimentary! While our competitors are charging thousands, some tens of thousands, we are offering our initial scan for free to show you where your network and compliance stands before we get started. We have noticed that many of our customers believe that they are closer to compliance than what our initial scan discovers. This often comes from organizations using their existing IT team to implement security measures, instead of staffing or outsourcing to cybersecurity experts. Contact CSS today to schedule your complimentary network scan!

System Security Plan (SSP) and Plan of Action and Milestones (POA&M)

NIST, and now CMMC, requires contractors to have an SSP describing how they are meeting compliance requirements and a POA&M indicating how any unimplemented security requirements will be met in the future.

These documents have to take a specific form and may be requested during the pre-procurement process, as part of bidding, or after the contract is awarded. They're living documents—the SSP should be reviewed every year and the POA&M needs to be updated at least monthly.

They could be requested by the agency you contract with at any time.
CSS has a lot of experience creating SSPs and POA&Ms for government contractors and can help ensure they contain exactly what you need for your contract. If you're an existing CSS client, we already have a good deal of information about things like your infrastructure, firewalls, and encryption. If not, we will start with gathering and documenting that data.

From there, we'll move on to discussing your employee and IT user policies to identify potential points of concern, such as employees conducting business on personal mobile devices. Finally, we'll sit down with you and run through each point on the compliance checklist to see how you're addressing it.

CSS CMMC Services cont.

Security Incident Response Plan

Your incident response plan is just what it sounds like—a plan for how you will identify and respond to incidents. We will create a detailed, individualized plan on how your organization will react. We also help clients conduct annual security incident tabletop exercises to pressure test the plan and improve it.

Depending on who your contract is with, you'll have a 24- or 72-hour period in which you need to let the agency know that you've had an incident. Later, you'll have to follow up with more details about what happened, what data was compromised, and what you did to mitigate the issue.

IT User Policy

A user policy guides your employees on how to handle different types of data, how to secure their equipment, and defines the norms of IT use in your organization. Many organizations already have this, or parts of this, as a stand-alone document or in an employee handbook, but if not, we can create it for you. As with other security policies and procedures, you should revisit this document annually.

Organization Security Policy

You should have a document that describes your organization's overall approach to IT security. The most thorough of these cover everything from ensuring appropriate encryption on data to proper locks on a server room door. CSS regularly creates these policies for clients and helps them maintain the documents through an annual review process.

Multi-factor Authentication

Multi-factor authentication is basic due diligence at this point for any organization that allows its employees to connect to systems remotely. It's a critical component of any cybersecurity plan. 800-171 requires multi-factor authentication for anyone working remotely and for IT administrators working locally. CSS currently partners with Duo for Multi-factor Authentication and is included in our solution.

Endpoint Security

A key component of any SSP is ongoing, regularly updated anti- malware technology. Our proprietary agent-based solution runs in the background, constantly scanning and updating itself in real-time with the latest virus signatures and behaviors.

CSS CMMC Services cont.

Email Anti-virus Filter

You should already have something on your desktop to block spam. What we can help you with is providing another level of security, farther away from the end user. Our solution sits in front of your mail server, screening out spam and viruses before they reach users' inboxes.

Managed Workstations and Servers

One of the single most important things an organization can do to protect itself is to ensure that its computers' security patches are up to date. A lot of businesses struggle to maintain discipline when it comes to security patches and software updates, but hackers target old versions of software, so it's vitally important for security and compliance that you don't fall behind on updating your systems. Typically, updates are done on a monthly basis, but if something is critical, we'll push it out immediately. Sometimes the updates require users to reboot their computers. In those cases, we'll send each user a message every hour until they reboot. Our automated tool keeps track of which systems have been patched.

Managed Server

Rigorous patching is just as important for servers, if not more-so. CSS monitors your servers and responds when they go offline. We also patch them after-hours on a monthly basis so that your employees never notice the work occurring in the background.

Encryption

Encryption of data in transit is essential for any government contractor and for security in general. If you handle controlled unclassified information, it must be encrypted on any kind of mobile device or when it's in transit—even if it's just on a USB device in your pocket. We provide an email encryption solution so you can email your controlled unclassified information. It's an add-on service that every government contractor will want to leverage. We also protect organization data on desktops and servers by deploying Microsoft's BitLocker encryption.

Intrusion Detection and Response

Contractors will be required to scour their networks and server logs for evidence of attackers. This is a huge challenge for companies because of the vast volume of log data —human beings just can't process it all. CSS provides at no additional cost Security Incident Event Management (SIEM) solution. A SIEM pulls all those logs together and looks for patterns that indicate an attack. Our dedicated 24x7 security team monitors the SIEM for alerts, investigates alarms, and responds to counter the attack.

CSS CMMC Services cont.

Managed Server

The most common way attackers access your data has nothing to do with vulnerable technology and everything to do with your own employees. Social engineering such as phishing is a common method of data breach. We provide phishing and security awareness training. We send simulated phishing attacks to your employees every month to give them experience recognizing attacks and help them improve their phish detecting skills. Employees who slip up receive training related to their error immediately so that the education is relevant and memorable.

Endpoint Detection and Response

Not everyone needs automated endpoint detection and response, but it's a recommended add-on for contractors who are at especially high risk of attack. An EDR solution can save you hundreds of thousands of dollars by stopping a ransomware attack in its tracks. It's becoming a very important part of a mature cybersecurity program.

CMMC Service Package

At CSS, our experts know just hat to do about your alphabet soup of regulations. We help you with a turn key solution that ensures you get and stay secure. Security is key, if you are secure you will be complaint with any regulation.

Our security and compliance plan is not the same package we would provide to a business in a less controlled industry—it will be tailored to the unique work you do.

You will be given a monthly rate for all the services and solutions you need - everything you need for security and compliance will be part of your package. It's both simpler and less expensive than putting together security solutions piecemeal.

We're not handing you a cookie-cutter solution. Your plan with CSS will be tailored to your business, budget, and compliance requirements. You have important work to do—CSS will take care of the rest!

Contact CSS and get started today by scheduling your complimentary network vulnerability scan!