CMMC

IMPORTANT THINGS YOU SHOULD CONSIDER

CYBER SECURITY SOLUTIONS

Introduction

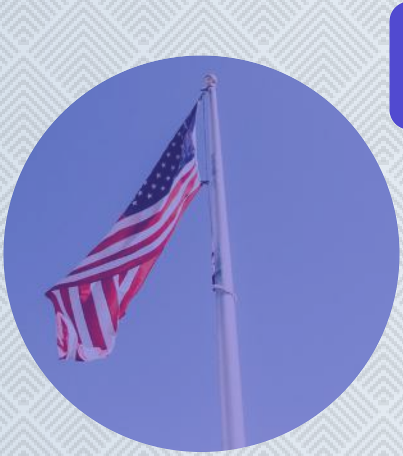
With Government agencies and top enterprises spending the necessary funds on their cybersecurity programs and employee training, hackers have shifted their focus to Small and Medium businesses that have less stringent network security as their prime targets. The Department of Defense (DoD) has issued the Cybersecurity Maturity Model Certification (CMMC) as an effort to mandate more mature cybersecurity practices, and to apply mandatory audits to ensure companies have successfully implemented requirements. CMMC builds upon DFARS and has five levels of maturity from Basic to Advanced Cyber Hygiene. CMMC certification is the future for the DoD supply chain and will be a requirement in future Request for Proposals (RFPs) for organizations that wish to conduct business with the DoD.

The DoD is not "BLUFfing"...... so here's the Bottom Line Up Front

CMMC certification will become a requirement prior to contract award.

By FY26 all DoD contracts will have CMMC as a requirement

CMMC requires a formal audit by a Certified Third-Party Assessment Organization (C3PAO)

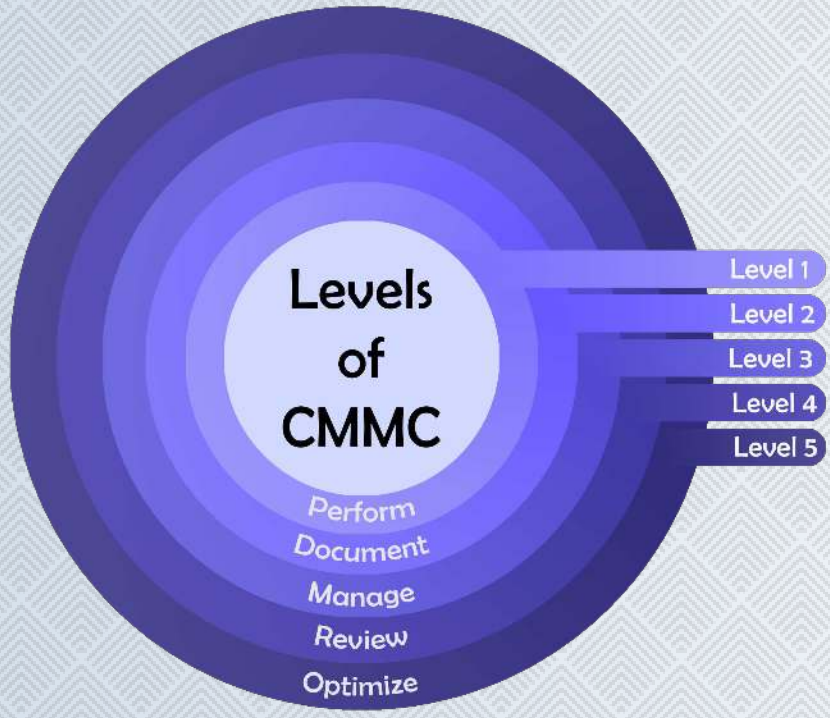


CMMC will not allow a Plan of Action and Milestone (POAM) in place of certification

Tell me more about Levels 1-5

Now that we know that the DoD is mandating CMMC and there are 5 Levels, lets dig in! CMMC incorporates pre-existing requirements such as NIST SP 800-171. 48 CFR 52.204-21, DFARS clause 252.204-7012, and various other requirements into a single set of unified best practices for cybersecurity. These requirements are laid out across 17 different domains, range from certification levels of 1-5, and total 171 cybersecurity best practices.

The necessary level of certification depends on the degree of requirements for the contracts your organization seeks. For example Level 1 is more about being able to show that your organization can perform specified practices and may not rely on documentation, as process maturity is not assessed for Level 1. However, higher levels require that proper processes and procedures are in place. Levels 4-5 take it a step further and require that your organization can protect your Controlled Unclassified Information (CUI) from Advanced Persistent Threats (APTs).



L1 **Basic Cyber Hygiene** — **17 Practices**

Focuses on the protection of Federal Contract Information. Only basic safeguarding practices are included to meet requirements defined in 48 CFR 52.204-21.

L2 **Intermediate Cyber Hygiene** — **72 Practices**

Includes a subset of security requirements specified in NIST SP 800-171. Organizations should establish and document information security practices and policies.

L3 **Good Cyber Hygiene** — **130 Practices**

Includes all security requirements specified in NIST SP 800-171. Organizations should establish, maintain, and resource an information security plan that addresses how Controlled Unclassified Information is protected.

L4 **Proactive** — **156 Practices**

Focuses on protection of Controlled Unclassified Information from Advanced Persistent Threats and introduces security requirements from NIST SP 800-171B. Organizations should regularly review and measure practices for effectiveness.

L5 **Advanced/Progressive** — **171 Practices**

Focuses on protecting Controlled Unclassified Information from Advanced Persistent Threats using additional practices that increase the depth and sophistication of the organization's cyber security capabilities.

Now that I understand the 5 Levels... tell me more about the controls.

As mentioned previously there are 5 different levels of CMMC. from Basic to Advanced Cyber Hygiene, but many people ask questions surrounding the seventeen different Capability Domains. What are they? How do I satisfy each area? Do I really have to go through every domain and requirement for certification?

Each domain has separate requirements that must be met before you can achieve compliance for your desired level of certification. It is important to note that not every company that approaches you offers a solution that meets the full intent of all seventeen controls... **spoiler alert: we do!** Their approach forces you to manage multiple different vendors to piecemeal a solution to meet CMMC compliance.

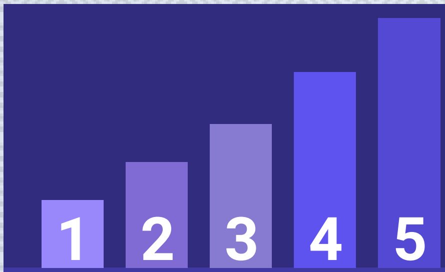
Here is a look at the seventeen required controls that we satisfy for our customers:

- Access Control (AC)
- Incident Response (IR)
- Risk Management (RM)
- Asset Management (AM)
- Maintenance (MA)
- Security Assessment (CA)
- Awareness and Training (AT)
- Media Protection (MP)
- Situational Awareness (SA)
- Audit and Accountability (AU)
- Personnel Security (PS)
- System and Communications Protection (SC)
- Configuration Management (CM)
- Physical Protection (PE)
- System and Information Integrity (SI)
- Identification and Authentication (IA)
- Recovery (RE)

What does the process look like?

So now that you understand what the CMMC requirements consist of, lets talk about the process. Remember, there is no longer self-attestation like there was with NIST 800-171. CMMC requires a formal audit, by a C3PAO, and requires re-certification every three years. It is important to know that CMMC requires a cultural change for your organization and the way that you protect your data.

Here is a look at the process to obtain and maintain CMMC compliance:



Identify the appropriate CMMC security level.

It is important to identify the level that best suites your organization, based on the contracts you pursue.

Identify & address any non-compliance between your organization's security & CMMC requirements.

This is a critical step in the process, how well you do on your final audit will depend on how well you have postured your organization. There is a lot of time and effort that goes into this step and CSS provides a turn-key approach that will be covered in the next few pages of this document.

Schedule a C3PAO compliance audit ASAP

There are over 300,000 defense contractors all looking to become CMMC compliant, and as you can imagine C3PAO schedules are filling up fast! The good news is that CSS has partnered with several C3PAO companies that will prioritize our customers... and since they have our Dashboard the process will take less time.

Pass your audit & maintain your CMMC compliance

The hard work is done right? Now we can hang the CMMC certification on the wall and go back to normal... wrong! CMMC is a maturity model certification that requires the proper security culture to maintain compliance. This is where you need a team like CSS to monitor your network and evolving requirements to maintain compliance.

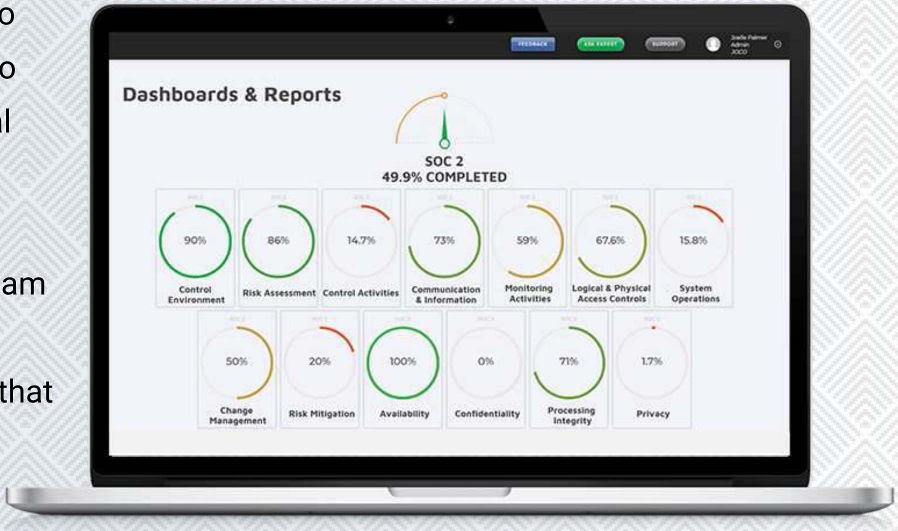
So that was a lot...
I don't even know where to begin.

When looking at meeting all of the requirements of CMMC many people become overwhelmed, and many don't even know where to begin. Just the thought of developing all new policies and procedures, purchasing the right security equipment, or developing training programs that emphasize the change in culture of how your organization must now protect data can cause major headaches. That's not even factoring in the need to bring in multiple vendors and piecemeal a solution that hopefully integrates and adapts to your business in the first place.

Other companies are assisting with CMMC...
What makes CSS different?

We love when we get this question, and I promise we're not trying to sound arrogant when we say "It's because we do it all." The main differentiator for CSS is that are not just a Managed Security Service Provider or a consulting company. We don't come in and tell you what equipment YOU should buy, what risks YOU should remediate, or what Policies and Procedures YOU should write. We handle all of those headaches for you, and everything that we do is custom to YOUR company!

We aren't a company that just says let go and hit the "I Believe" button either. We keep you up to date throughout the entire process. We offer our all inclusive CMMC Dashboard that shows your executive team exactly where we are in the process, and tie it to your percentage of compliance. No more cookie cutter solutions that only address a portion of the required controls, no more paying ridiculous prices and still having work on your plate to reach compliance, and most importantly no more surprises of hidden fees or additional costs. We offer full transparency in our process and we are there for you to obtain compliance, and maintain it as well. Our team takes pride in knowing we can offer a high quality, true turn-key experience at a price that is affordable for companies of any size!



Dashboards & Reports

SOC 2
49.9% COMPLETED

90%	86%	14.7%	73%	59%	67.6%	15.8%
Control Environment	Risk Assessment	Control Activities	Communication & Information	Monitoring Activities	Logical & Physical Access Controls	System Operations
50%	20%	100%	0%	71%	1.7%	
Change Management	Risk Mitigation	Availability	Confidentiality	Processing Integrity	Privacy	

We're here to help!

We believe that CMMC should be an easy adaptation, not one that stresses you out. After all, if you are not a Cybersecurity or IT firm you probably didn't go into business infatuated with adapting to evolving requirements that you aren't familiar with. We have perfected our CMMC implementation and onboarding processes to the point we can help you reach compliance in less than 90 days of signing up for our services. Yes, you read that right... we can have your organization 100% compliant in less than 90 days, waiting for a C3PAO to show up and complete your audit.

Our solution is a turn-key, white glove service that brings all of the required security solutions to the fight, backed by our 24/7 monitoring and help desk at our Secure Operations Center (SOC). We have developed over 60 compliant Policies and Procedures that ensure your organization and your team meet compliance. Here are some services we provide to ensure your compliance, but don't worry we break each one down in our **CMMC Compliance - 30 Things Included** document on our website:

24/7 Monitoring
Vulnerability Scan
Remote Workforce
Forward/Reverse Proxy
Multi-Factor Authentication
Compliance Assessment
Data Destruction
Data Encryption
Policies & Procedures
SIEM
Firewall as a Service
Web Security
Reporting Platform
CMMC Compliance Dashboard
Patching
Incident Response
Anti-Malware
Secure Storage
Security Training
Virtual Private Network
After Action Reports
Disaster Recovery
Anti-Virus
24/7 Help Desk
Secure Chat
Phishing Campaigns
Risk Assessment
Email Security
Microsoft Office Suite
Secure Backup
Exposure Assessment

Summary

No matter how long we try to push off CMMC implementation, it is real, and it is a requirement for all future DoD contracts. At CSS we believe that cybersecurity and compliance do not have to be expensive or complicated. We also believe that just because some vendors have higher costs, it doesn't mean that their solution is higher quality.

This is a new market for defense contractors, and there are a lot of companies who market that they can get your organization to achieve CMMC compliance. We never claim to be the only vendor that provides A-Z services needed for CMMC compliance, but we do stand by our word to offer full transparency on the products and services we provide guarantee you meet the requirements for **ALL 17 control areas** and pass your C3PAO audit.

During our CMMC Demo we provide pricing along with all services that are included. We recommend for you to shop around, using the list of services to get a good apples to apples comparison of what we provide. At the end of the day we want you to be confident in the investment you are making to obtain and retain compliance. This is a major culture change for your organization, we want you to make the best decision for you!

How Compliant Are You?

Email us today to schedule your **COMPLIMENTARY** Compliance Scan!

cmmc@securedbycss.com

The CSS Way

CMMC Compliance

30 Things Included at One Low Cost

1 Secure Storage

Securing your business takes more than installing alarm systems and video cameras, because the real value for criminals is in the data that your business holds. The amount of data organizations need to protect is growing at a rapid pace, and the environment where data lives is constantly evolving. It is vital for an organization to ensure their data is stored securely. Our secure storage solution is more than just a place to keep files, it is security enforced, Security Operations Center (SOC) monitored, and Disaster Recovery supported. Our team will perform automated synchronization through scheduled or continuous backups, that fit your needs. We offer scalable secure storage options in 1 TB increments to support small or large enterprise customers.

2 Vulnerability Scan

It is difficult to know what you need to do before you determine where you are today. This scan will enable you to plan the path forward and receive an accurate quote for services needed rather than just guessing. Our vulnerability scan illuminates the unknown. Security requires leaving no stone left unturned and this scan enables the detection of devices, services, and vulnerabilities that were previously operating without the knowledge of the operators. This scan is required to effectively secure a network and comply with regulations. That’s why we developed our solution to provide continuous monitoring rather than performing quarterly checkups.

3 Risk Assessment

The worst type of risks are the ones that have yet to be assessed. That’s why we work with you to understand the current state of your security posture and evaluate it against the compliance requirements mandated in your industry. Our Risk Assessment detects unencrypted data holding Personally Identifiable Information (PII) that could potentially be breached. It then checks the vulnerabilities within the system holding the data to determine potential exposure. To help your team understand the financial impact of risks identified we provide a cost associated with a potential data breach. Our report identifies the financial impact per exposed file and calculates the total cost liability you could potentially face if a breach were to occur, based on historical breaches in your industry.

4 Compliance Assessment

Dealing with compliance services isn’t sexy, that’s why we simplify the compliance process to make it more attractive. We’re here to help your business meet industry compliance regulations so that you can get back to the running the business you love. Everything starts with our compliance assessment where we determine applicable laws and regulations that your organization must comply with and the associated controls. We then compare the technical controls to the detected policies and procedures within your organization and report the compliance status for each control, line by line. This is a much needed assessment to understand the adjustments that need to be made for your organization to meet industry compliance.

5 Policies and Procedures

It is easy to become overwhelmed when it comes to developing Policies and Procedures that satisfy IT and cybersecurity regulations within your industry. After all, if you are not in the business of IT or cybersecurity many of the requirements can look like they are written in a foreign language. Don’t worry, we are here to help! We use the data from your Compliance Assessment and industry requirements to generate appropriate Policies and Procedures that address the controls dictated within your industry. We develop the clear, consistent Policies and Procedures needed to reinforce your organization’s security and compliance programs. We continue to monitor industry requirements and update your Policies and Procedures as they change, allowing you to focus on your business.

The CSS Way
CMMC Compliance
30 Things Included at One Low Cost

6

24x7 Helpdesk

We believe that your team shouldn't have to wait when it comes to getting the IT support you deserve. That's why we offer our 24x7 Helpdesk to our Complete Compliance solution subscribers. Our experienced team not only responds to customer reported issues, but we often fix issues before your team even notices. As your security provider we monitor your network 24/7 and proactively look to close tickets often times before they occur. Our proactive approach to security enables us to excel beyond our competitors' standard I.T. and remote managed solutions that include reactive and minimally proactive helpdesk. Our 24/7 Help Desk services are essential components of efficient business operations and processing of end-user service requests.

7

Secure Vault

Our Secure Vault enables remote and office workers to collaborate easily while still maintaining regulatory compliance. Unlike other cloud providers, we also understand that sometimes corporate policy disallows sensitive information to be stored on 3rd party servers. So we enable you to run the Secure Vault on your own internal infrastructure to enable compliance with both regulations and internal policies. Regardless if personnel access from a desktop in the office, a laptop in the field, or a mobile device on the go, the same secure real-time editing and sharing capabilities are possible. Our Secure Vault can be used for document storage, sharing, and real time collaboration as well as calendar integration, appointment scheduling, task management, and much more.

8

Email Security

In some cases organizations want to bring their own email solution without dealing with a migration. Though we can make the migration simple, we also provide a means for applying the same security and compliance to your existing email solution. Our Email Filtering service ensures that everyone has the ability to operate with security and compliance in a way that doesn't slow down operations. Our Email Security and Filtering services are tailored to meet your corporate policies. We protect your users and business from threats like malware and spam, as well as advanced threats like targeted spear phishing and ransomware. We ensure every email is quickly filtered and sanitized before it is delivered to your inbox server to protect you from potential threats.

9

SIEM

Intrusion prevention systems alone aren't enough when you need to prevent sophisticated malware, which is why a SIEM is so important. Our SIEM continuously monitors and acts upon real-time security information from virtually any source. This is required to comply with most cybersecurity regulations. Our SIEM ensures that every aspect is factored in by automating a preventative or notifying of a proactive action based upon millions of incoming data points every day. Additionally, our SIEM solution is able to aggregate data from across your entire network, and analyze this data together to limit false-positives that your organization is receiving. Without a SIEM the millions of data points would have to be checked manually every day without missing a detail, which isn't possible, secure, or compliant.

10

Exposure Assessment

Life is good, until the day your data or the data of your customers is exposed. The sad part is that most companies do not test for exposure until the incident response team show up to figure out what has been exposed and from where. Our Exposure Assessment monitors external communications to your company's infrastructure and compares the detected communications and attempted attacks with the vulnerabilities detected in our Vulnerability Scan. This enlightens business owners and Cybersecurity Analysts with details relating to current or previous exposure of internal vulnerabilities. For example, if your Exposure Assessment reveals that Country X is consistently attempting to launch attacks on a specific server then that would tell us that they may have previously had access to it.

The CSS Way

CMMC Compliance

30 Things Included at One Low Cost

11

Security Training

Your company can spend its entire IT and cybersecurity budget on cutting edge technology to protect your network, just to be breached due to an untrained staff member. You are only as strong as your weakest link, so let's make sure your staff are properly prepared to withstand cyber threats. Security Training handles the human aspect of insecurity in an organization. We ensure that each employee is educated and prepared to avoid scams and attacks and properly report and handle incidents. Since email is the most attacked surface we include custom email phishing campaigns each quarter for our customers. This is used to gauge your staff's adherence to policy and provide a realistic opportunity for employees to train. Annual training is required for compliance and CSS provides it.

12

Disaster Recovery

No business ever wants to deal with a disaster. However, if a disaster were to occur you will be happy that you had our Disaster Recovery service. Our Disaster Recovery service provides a means of restoral of files and even services on protected servers. Backup is often confused with Disaster Recovery but the difference is that backup only offers file restoral whereas our Disaster Recovery provides complete service restoral in our cloud in as little as 4 hours, even if a complete loss of server hardware occurs. File restoral would not protect a complete loss of server hardware and would take weeks to get back to operational status again. This is while all internal services are offline, which could prevent all operations for your employees, whether a natural disaster or a ransomware attack.

13

Secure Backup

We recognize the need to keep files safe on your desktop computers that your employees use and not just on the server. Sometimes employees accidentally save a file on their computer rather than the proper shared server storage location. This can cause a loss of data if the computer fails. Our Secure Backup service provides desktops with a means of file protection from natural disaster and ransomware. This does not restore services or entire servers like the Disaster Recovery service but will ensure that the most important types of files are not lost in an incident. We understand how important time is when it comes to business, so we are here to ensure you don't get stuck creating the same document twice.

14

Anti-Malware

Malware stands for "malicious software," and like it's name, it poses a big threat both to your computer's operating system as well as the data stored inside. Malware is typically disguised as harmless files, software, and links. When downloaded and opened, they wreak havoc on the system by slowing performance, corrupting data, and even holding sensitive information hostage until a payout is received. Anti-Malware from CSS will always ensure that the latest attack prevention methods are in place on all endpoints, while managing all vendors required to provide the security. This acts as the last layer of defense for the data that is being protected. In the event that a more sophisticated attack manages to bypass other security measures, an organization needs the best possible protection on every device.

15

Firewall as a Service

Implementing and handling security controls for your business is complicated, costly, and time consuming for your staff. Our approach is to remove the headaches, offer highly competitive pricing, and save your organization time. Problem solved. Our Firewall as a Service provides the first layer of defense against all attacks. Every second of every day we fend off a barrage of attacks at this layer to prevent the opportunity for aggressors to interact with internal services and data. We handle the licensing, management, and security of our proprietary CTC box where the firewall resides. We don't recommend a company to assemble their own vendor alphabet soup but rather allow us to handle all needed aspects of first line of defense and security.

The CSS Way

CMMC Compliance

30 Things Included at One Low Cost

16

Patching

Many customers have asked us what Patching is. No we're not talking about fixing up your favorite jacket or pair of jeans. However, a software patch can be applied to a program or operating system to repair an exposed flaw, just like that favorite jacket you've been refusing to give away. Patching can target a myriad of issues like a addressing a bug, improving your operating system, or fixing a specific security vulnerability. Patching is a standard and well known requirement that many IT companies offer for an additional fee. We don't charge anything extra to provide this necessity since it's required by all industry regulatory compliance. Patching is included with each of our business package solutions.

17

Web Security

Internet is a great tool to get work done, it is also a massive distraction or even a vulnerability in certain cases. Our Web Security service can be used to limit use of certain websites or block them entirely on the corporate network. Web Security adds a layer of defense to an organization's data by preventing employees from clicking known malicious links. No matter if the employee is performing google searches or getting malicious scam emails, our Web Security helps prevent attacker success by disallowing access to those sites. Furthermore, any company on our business packages can implement policies to prevent access to any requested types of websites such as pornography, gambling, and even media streaming such as YouTube and Netflix.

18

Remote Workforce

Most businesses didn't have a care in the world for Remote Workforce tools, and then came COVID-19. We understand that many businesses had to adjust to trusting and relying on Remote Workforce tools, we include it in all of our business packages. This provides the most secure means of accessing office computers from anywhere in the world, without exposing vulnerable systems to the internet. Typical solutions for working remotely include Remote Desktop Protocol (RDP) but that is a major security risk and most often insecure. There are freely available tools on the internet to breach RDP which is why many attackers use it to gain access to networks. Our Remote Workforce solution allows employees to work securely from anywhere as if they were sitting at their desk.

19

Microsoft Office Suite

It was reported in 2017 that 83% of enterprises use Microsoft Office, and the numbers have continued to grow. Pretty much everyone is familiar with Microsoft Office products, which is why we provide the tools that you are used to using the most. Microsoft Office Suite allows us to provide a license to each endpoint protected by our business packages. There's no need to pay for expensive individual licenses or increased costs for Office 365 for your office employees to have the Microsoft Office applications, we'll provide that for you. This fits the rest of our business model and approach in reducing the number of vendors, invoices, and licenses that your business has to keep up with.

20

Forward/Reverse Proxy

Forward Proxy requires our CTC box and offers your organization increased security when office employees browse the web. Our Forward Proxy service monitors all web traffic in and out from office computers and stops any malicious behavior. Furthermore, it disallows internet access from unknown devices. This prevents data exfiltration from internally placed devices that aren't known.

Reverse Proxy enables secure and compliant access to internal services on your local network. If you host a web server that you need external employees to have access to, this service monitors and secures all external web traffic which prevents any data from being transferred outside of your organization without security.

The CSS Way

CMMC Compliance

30 Things Included at One Low Cost

21

Virtual Private Network

A Virtual Private Network is one of the smartest ways to protect your online privacy, all while maintaining data security. Our Virtual Private Network solution enables company owned devices to access internal network services from remote locations. Anywhere that a company owned device has internet access, it can securely behave as if it is directly connected to the corporate network behind all layers of defense. It also simplifies and secures access to corporate data without the added step of remotely controlling a corporate device using Remote Workforce. A trustworthy Virtual Private Network will secure and encrypt your internet, keeping your data safe from malicious eyes.

22

Data Destruction

What do you do with your old hard drives? Do you know the proper way to ensure all sensitive data is removed? These are tough questions for most companies, many do not want to deal with potentially leaving sensitive data on their retired equipment. Data Destruction is required for compliant disposal of assets that once held data. Simply deleting files or reinstalling over previous systems does not meet regulatory compliant needs for data destruction. We ensure that your data storage assets are properly wiped using standards that meet or exceed your regulatory compliance needs. Many organizations are unaware that throwing away or selling old devices without data destruction is defined as a data breach without proper encryption and data destruction.

23

Data Encryption

We all store sensitive data, but how many organizations are positive that their data is properly encrypted and secure? We ensure that your data remains secure and reduce the change of interception by those unauthorized to view it. Our Data Encryption service provides necessary device level data protection for regulatory compliance. This prevents a data breach report from being required when a device is stolen or lost. Many organizations have faced fines and hefty loss of reputation and profits due to loss or theft of devices with sensitive information. Our Complete Compliance service ensures that an organization meets all necessary regulatory compliance controls for encrypting data.

24

Incident Response

Nobody can predict a breach before it occurs, and the truth is no matter how much money you spend on security a breach can still happen. If a breach were to occur you will want to make sure you have an experienced team ready to take action. We will quickly determine the source, cause and extent of a security breach. Incident Response provides a team of experts in response to cyber incidents as required by regulatory compliance. Our business security packaged solutions provide the necessary Incident Response team and procedures to enable organizations to comply with regulations without vendor management.

25

Reporting Platform

Our Reporting Platform is provided along with our business package solutions and enables organization decision makers to see details about what we do every day to help make cost saving decisions. An example of how this helps decision makers is by historically tracking and reporting troublesome devices that cause employees headaches and loss of productivity. When armed with this information, a business owner or office manager can prioritize replacement of the most troublesome equipment which increases productivity of the workforce. Furthermore, it can allow the business owner to grade our level of engagement on issues and our ability to meet our contractual Service Level Agreements.

The CSS Way

CMMC Compliance

30 Things Included at One Low Cost

26

Identity Management Platform

It is important to ensure that the process of signing in to your systems is a secure one. This is why we encourage customers to sign up for Identity Management Platform services that ensure your users are who they say they are. Identity Management Platform provides Authentication Authorization and Accounting to protect data and systems as required by regulatory compliance. This has the added benefit of Single Sign On for many applications which simplifies workflow and employee training. Added security is built-in with two factor authentication prior to access authorization for protected data.

27

After Actions Reports

It is important to be able to analyze the management or response to an incident, exercise or event. Often times this is done by identifying strengths to be maintained and built upon, as well as identifying potential areas of improvement. Our After Actions Report is a tool used to prove compliance with regulation controls. Each possible incident is greeted with an investigation and categorized, executed, and notified appropriately while being tracked using our After Actions Reports. This historic reference of events allows for quicker audits by regulators in every industry.

28

Phishing Campaigns

We all have received some type of phishing emails, some look so genuine that it is difficult to identify. We create a mock malicious email campaign and target company employees to test who clicks, reports, or ignores these types of emails. Those who click get training on how to identify malicious emails. Those who ignore get training on how to properly report malicious email activity. The statistics help guide our annual Security Training for your company.

29

Secure Chat

A safe and secure business is a smart business. Every business from small startups to large enterprises should understand the importance of their security. In today’s day and age almost everyone has a smart phone, and a lot of professionals use their phones to discuss business. Have you ever considered the security aspect of what may be sent via an non-secure text message between your employees? Although many companies have a VPN-type login to access a corporate email account in a secure manner, there is rarely a system or policy in place for secure text messaging. Our Secure Chat solution provides employees in the office or working remote with a web application and phone app to chat in a secure and compliant manner.

30

Compliance Dashboard

While compliance is something that we should all take seriously, nobody jumps for joy to implement and track the progress. With our Compliance Dashboard you can not only understand where you are today, you can easily identify your non-compliance areas and develop a plan to mitigate those risks. Our Compliance Dashboard provides executive reporting, project management, and engineering task management to keep your compliance up-to-date easily while staying on budget. Executives can quickly understand short falls and compliance budget. Project managers can quickly address compliance issues and assign engineers.