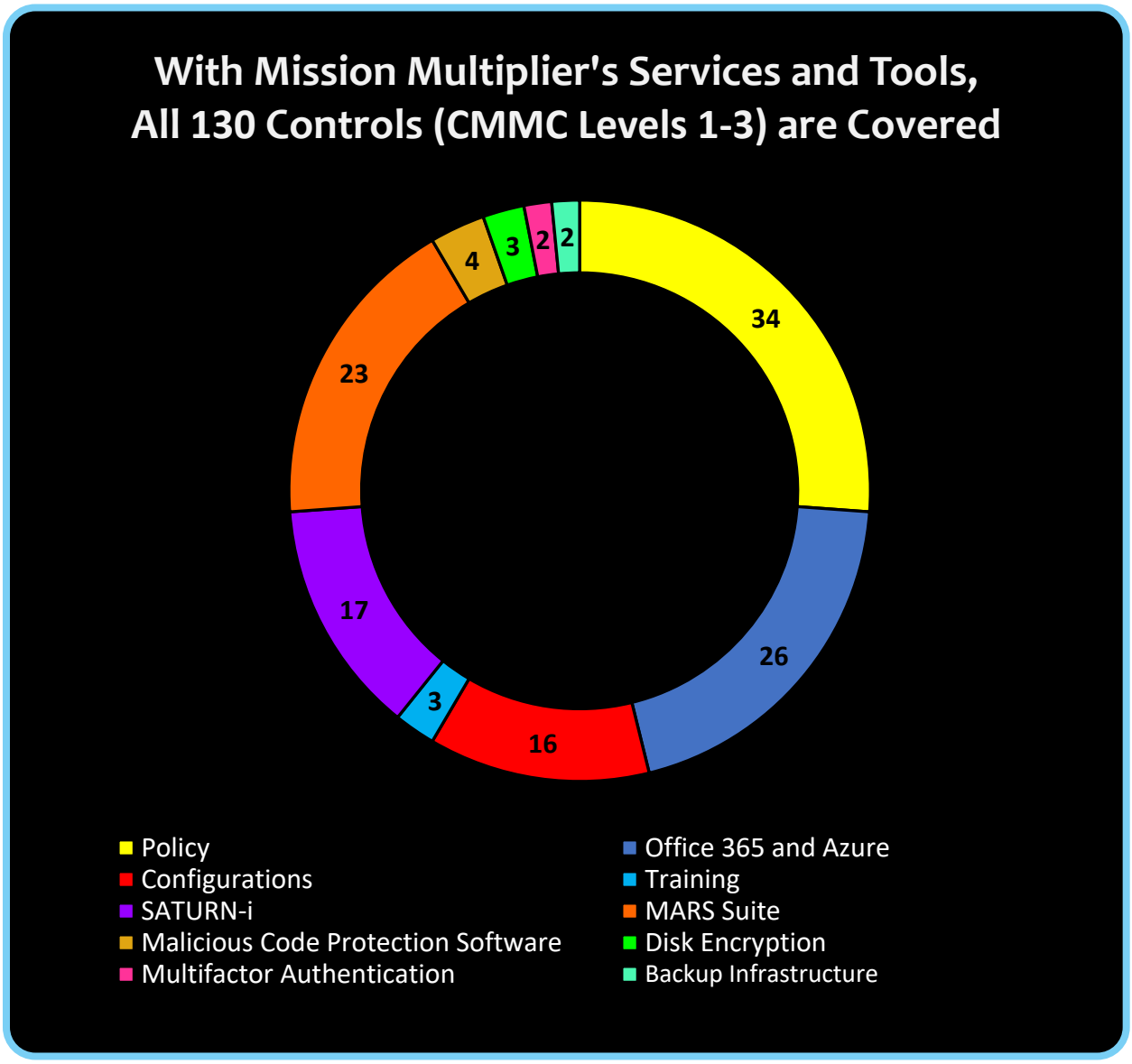
mission multiplier

CMMC Compliance by the Numbers

Introduction



The Cybersecurity Maturity Model Certification (CMMC) is the new certification standard that contractors doing business with the Department of Defense (DoD) will have to adhere to in order to win work in the future. Currently, contractors are required to achieve, by the` time of award, a CMMC certification at the level specified in the contract solicitation. In the future, this requirement may change such that contractors may need to have CMMC certification even to bid on

CMMC IS THE NEWEST EVOLUTION OF DFARS/ NIST COMPLIANCE.

potential opportunities. Simply put, contractors who do not achieve compliance with this government-mandated, third-party assessment-enforced program will not be able to do work with the DoD in the future. As stated in Version 1.02 of the CMMC standard, "a maturity model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline". In this context, CMMC requires organizations to implement processes and practices in the form of 17 *domains* (also sometimes referred to as *control families*). These domains span cybersecurity practices and processes that contractors must incorporate into their organization from Access Control (AC) to Awareness and Training (AT) to System and Information Integrity (SI). These domains are primarily drawn from the control families of NIST SP 800-171 Rev. 2, a cybersecurity framework that is widely known within the Defense Industrial Base (DIB) because of DFARS Clause 252.204-7012. CMMC is the newest evolution of the DFARs/ NIST compliance program of which DoD contractors may already be familiar.

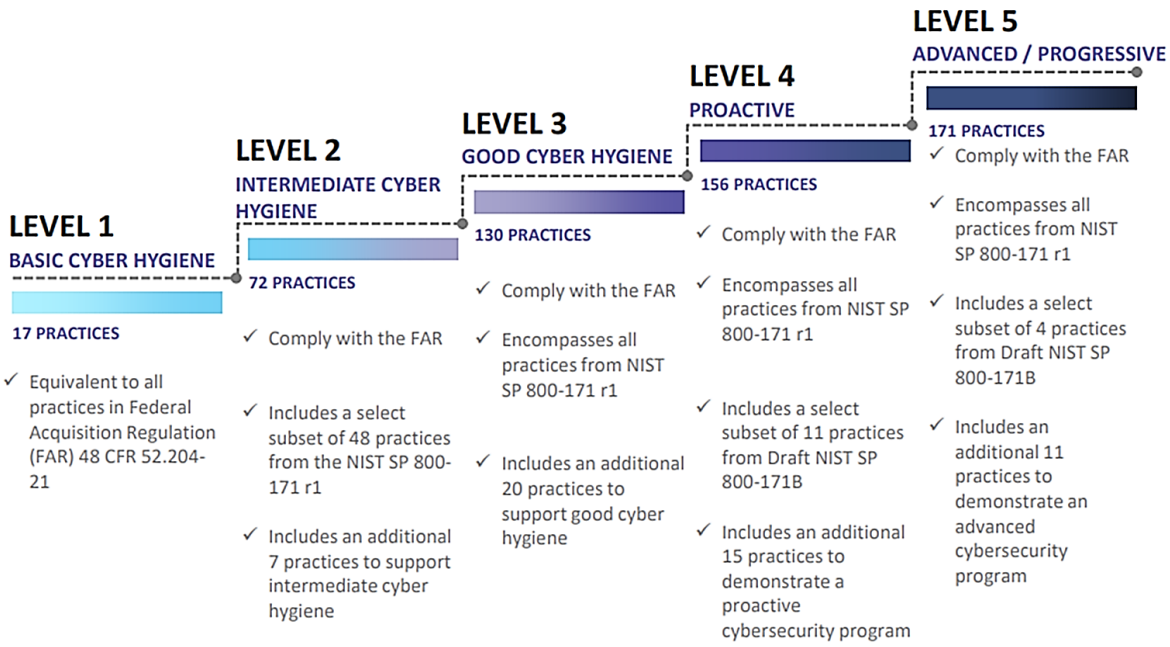
By now, most contractors are well acquainted with DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, which required contractors to "implement NIST SP 800-171 Rev. 2, as soon as practical, but not later than December 31, 2017". In accordance with DFARS 252.250-7012, contractors could demonstrate adherence to DFARS 252.204-7012 and application of NIST SP 800-171 Rev. 2 by way of self-attestation (by signing the contract) and having a System Security Plan (SSP) and Plan of Action and Milestones (POA&M). While program offices reserve the right to scrutinize a specific contractor's approach to providing adequate security to protect CUI (e.g. MDA), there was no formal program in place to broadly audit all DoD contractors.

The allowance of self-attestation has led to a situation where contractors are ignoring DFARs requirements, falsely attesting that they have implemented the requirements, or are indefinitely "POA&M-ing" requirements by establishing unrealistic deadlines to complete unimplemented controls or shifting deadlines once they have been unsuccessfully passed. In fact, according to a survey from the National Defense Industrial Association (NDIA) of small and medium-sized defense contractors, less than 60 percent of respondents had "even read the new DFARS requirement documentation" and 45 percent of respondents "had not read the NIST publication [NIST SP 800-171 Rev. 2]."[1]

Less than 60 percent of respondents "have not even read the new DFARS requirement documentation" and 45 percent of respondents "had not read the NIST publication [NIST SP 800-171 Rev. 2]."

This is a dangerous situation to non-compliant organizations, as DFARS 252.204-7012 is like any other DFARs requirement, and non-adherence brings with it all the consequences associated with DFARs violations, e.g., termination of contract for cause, fines, negative past performance, etc.

Because of these realities, among others, the DoD is giving the DFARs requirement "teeth" by way of the **Cybersecurity Maturity Model Certification (CMMC)**. The CMMC standard is envisioned to "Be a unified cybersecurity standard for DoD acquisitions to reduce exfiltration of Controlled Unclassified Information (CUI) from the Defense Industrial Base (DIB)." The CMMC effort builds upon the existing DFARS 252.204-7012 regulation by adding a verification component with respect to cybersecurity requirements, i.e. assessments by private independent CMMC Third-Party Assessor Organizations (C3PAOs).



Similar to Capability Maturity Model Integration (CMMI), contractors will have to obtain a particular CMMC "Maturity Level" for a specific contract. These requirements will be present in Request for Proposal (RFP) sections L & M, and will be a "go/no-go" decision. These Maturity Levels will span Level 1 through

Level 5, with Level 1 contracts being for simple work (e.g., pencil manufacturing or landscaping) while Level 5 contracts will more than likely only apply to work usually performed by major defense contractors (e.g., Boeing, Lockheed Martin, etc.). The majority of contractors are predicted to need Level 3 certification or lower. This will entail applying the 110 practices from NIST SP 800-171 Rev. 2, implementing an additional 20 practices, managing institutional processes, and of course, a third-party assessment. This white paper was designed to address all 130 practices outlined in Levels 1-3 of the CMMC standard in detail.

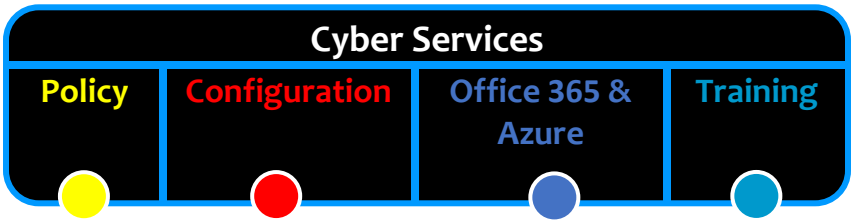
In December of 2020, the DoD announced that they would be introducing the first 15 contracts to serve as "pathfinders" for the new model. The DoD is planning to have full implementation (i.e., all solicitations will contain CMMC language) by 2025. While this may indicate a slow rollout of the full CMMC program, it nonetheless indicates that contractors will soon require a certain level of CMMC certification in order to do work. In the meantime, the DFARs clause is still in effect. Until that changes, contractors are still required to implement NIST SP 800-171 Rev. 2 to make a proposal on *any* DoD work. This was further solidified by the September-November 2020 interim rule change that required contractors to once again self-attest their level of compliance with the DFARs clause and included a requirement for contractors to provide the DoD with a self-determined quantitative score.

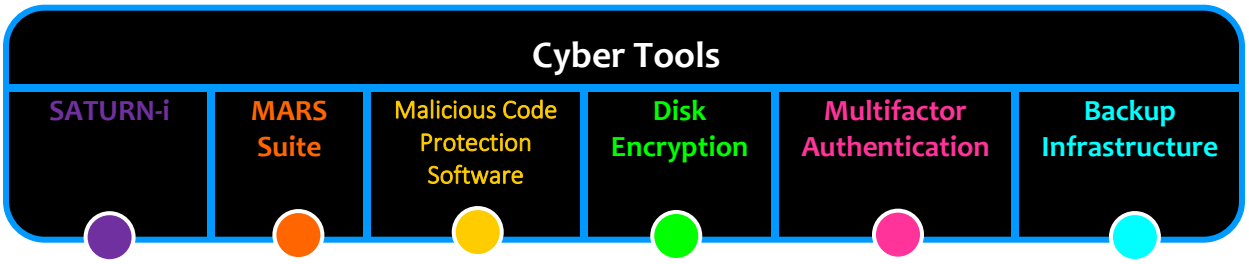
According to official guidance provided by the DoD entitled *An Approach to Implementing NIST SP 800-171*, the DoD states:

> **Most requirements in NIST SP 800-171 are about policy, process, and configuring IT securely, but some may require security-related software or hardware.**

Implementing these controls can be a challenge for small- to medium-sized companies. However, organizations that consider using Mission Multiplier for outside assistance can rest assured that all of these controls can be addressed as part of a coordinated, streamlined implementation process. Simply put, Mission Multiplier is your organization's turn-key solution for complete adherence to the NIST SP 800-171 Rev. 2 controls, the additional 20 controls required by CMMC for Level 3, the management of requisite processes, and support for assessment preparation.

Within the scope of CMMC compliance, Mission Multiplier categorizes our cybersecurity solutions into two broad categories: Cyber Services and Cyber Tools.



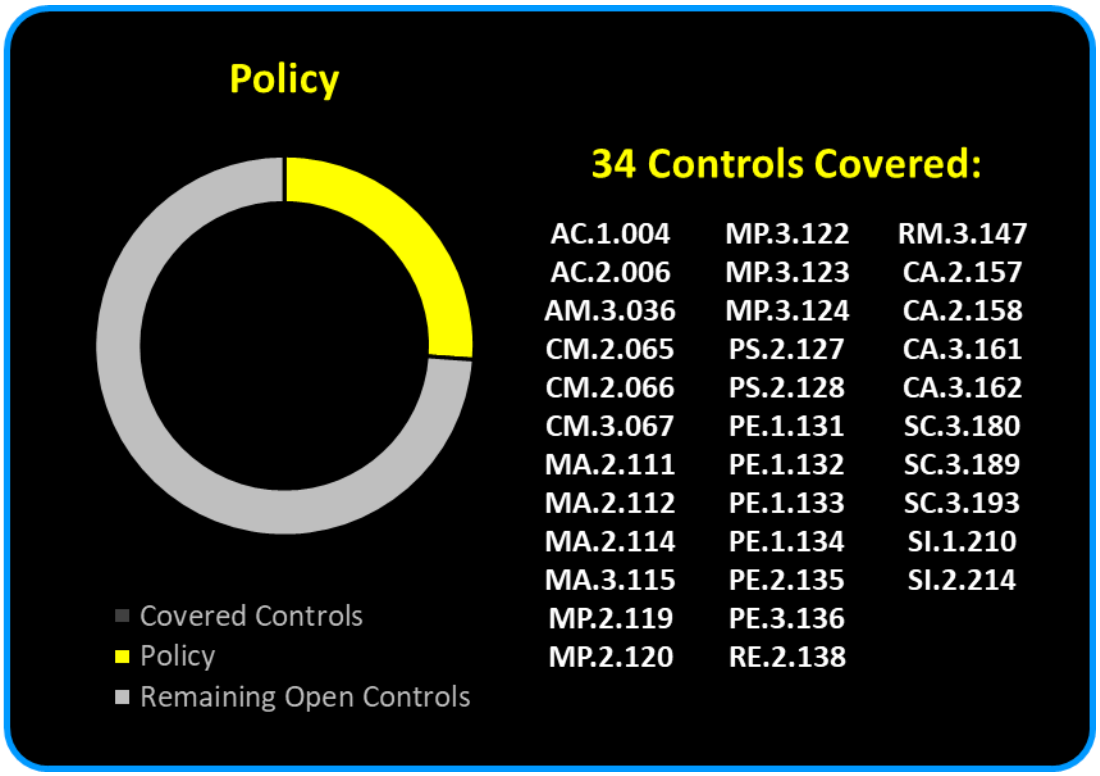


Mission Multiplier's Cyber Services offerings entail many of the services usually associated with an in-house Information System Security Officer (ISSO) for a fraction of the cost of hiring a full-time employee. These duties primarily include policy development, implementing a secure directory service and information system infrastructure like that found in Microsoft Azure and Office 365, hardening system and hardware configurations, and training users on secure practices. Mission Multiplier's services also leverage our eclectic suite of cyber tools comprised of both proprietary solutions designed specifically with CMMC compliance in mind, and industry-recognized off the shelf products that we have thoroughly reviewed and tested for the purpose of compliance. This combination of services and tools allows Mission Multiplier to assist your organization with meeting ***all*** of the one hundred and ten (110) controls required by NIST SP 800-171 Rev. 2, meeting the additional 20 CMMC controls, managing the requisite processes, and successfully preparing for a CMMC assessment for levels 1-3.

Cyber Services

Policy

A key component of DFARs and CMMC compliance is the creation of security policies. DoD guidance states that: “Typically, most requirements entail determining what the company policy should be (e.g., what should be the interval between required password changes) and then configuring the IT system to implement the policy.” In addition, CMMC Levels 2 through 5 require that “a policy exists that cover all activities.” For CMMC, policies must be established for all domains/control families, e.g., policies must be established for Awareness and Training (AT), Media Protection (MP), etc.



Mission Multiplier provides more than just templatized, one-size-fits-all policies. Our policy writers will sit down with key stakeholders within your organization to ensure that each policy is customized to your unique information system architecture and company culture. Mission Multiplier ensures that policies are crafted alongside your organization at each stage of development.

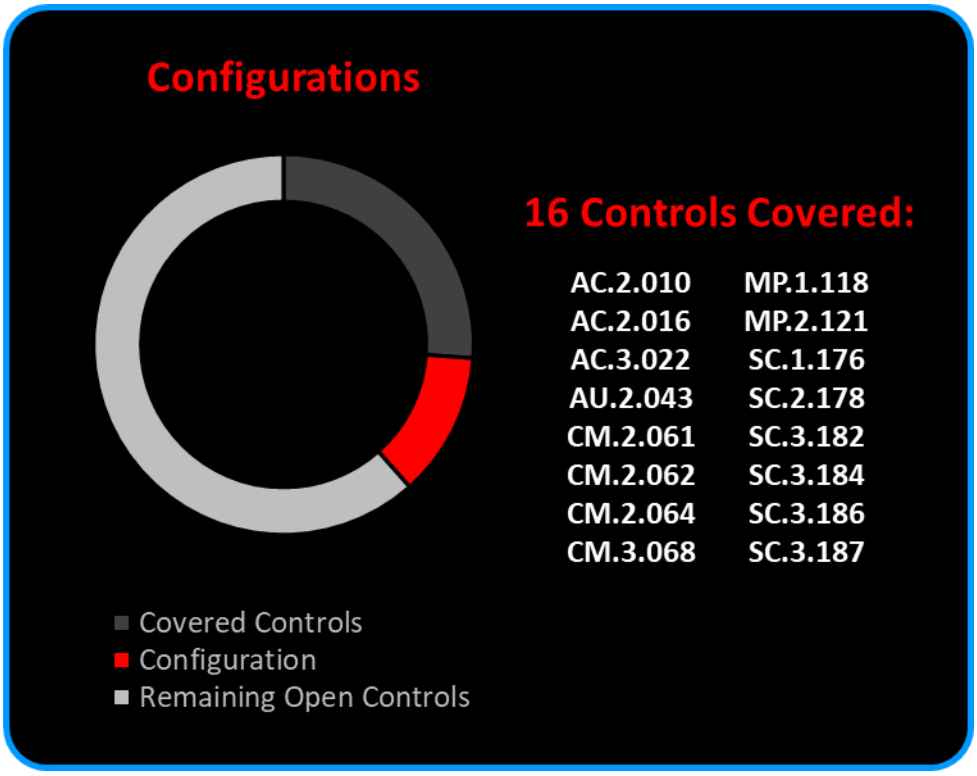
For example, one policy requirement might necessitate a hybrid technical and operational solution (such as installing a vulnerability scanning mechanism and codifying the policies required for the mechanism's

operation). Mission Multiplier will craft the applicable policy in a way that your organization can reasonably adapt to the change and give sufficient time for the policy to proliferate throughout the organization.

Additionally, it is no longer sufficient to simply have a written policy in place. While Level 2 requirements require organizations to "establish and document practices and policies to guide the implementation of their CMMC efforts," CMMC Level 3 requires organizations to "establish, maintain, and resource a plan demonstrating the management activities for practice implementation". In other words, while having written policies is crucial, companies now need specific plans regarding how they plan to execute these policies. Plans may need to include information such as mission, goals, project plans, resourcing, required training, involvement of key stakeholders, and more. Mission Multiplier can assist your organization with navigating the waters between policy requirements and planning requirements.

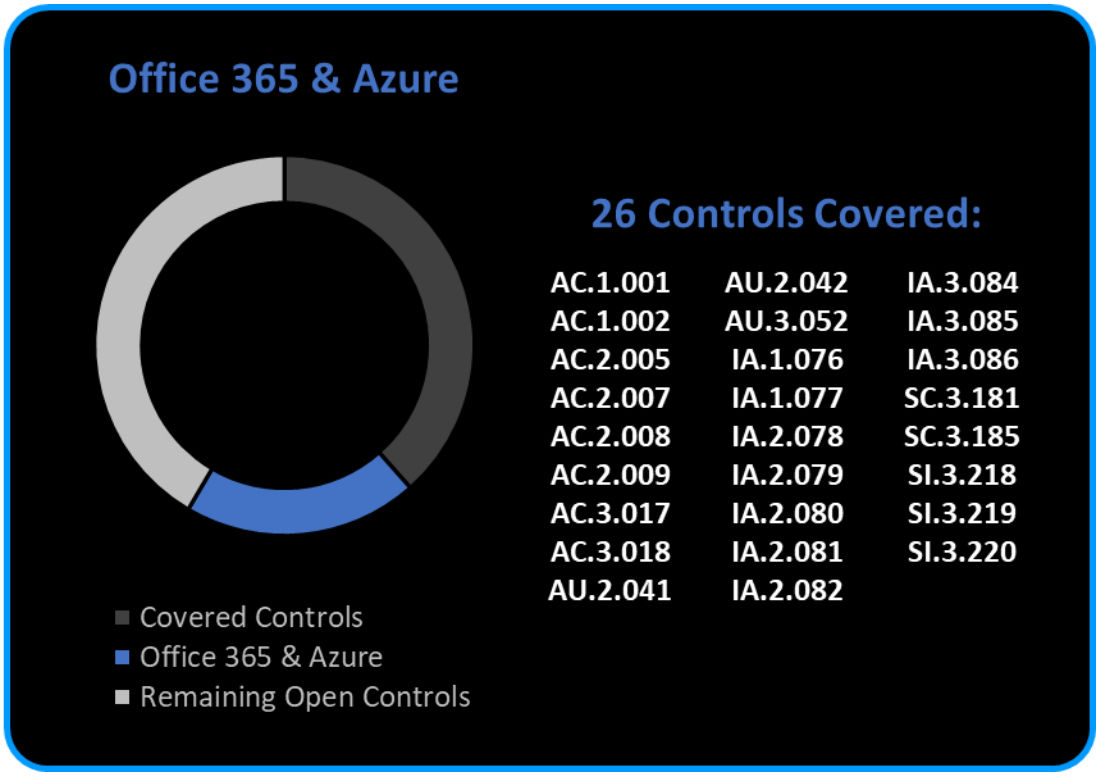
Configurations

One common misconception about DFARs and CMMC compliance is that it requires the purchase of copious amount of additional hardware and software. On the contrary, many organizations already have most of the infrastructure needed for the compliance process. However, while this infrastructure may already be in place, devices and software may need to be configured and fine-tuned in order to better adhere to cybersecurity best practices as required by CMMC. Such modifications can include closing network ports, removing unnecessary services, configuring firewalls, and establishing inactivity conditions. Additionally, the CMMC standard puts emphasis on establishing configuration baselines and performing configuration and change management within the Configuration Management (CM) domain/control family. Mission Multiplier can help configure and harden your organizational information systems to provide the level of security and compliance you need.



Office 365 & Azure

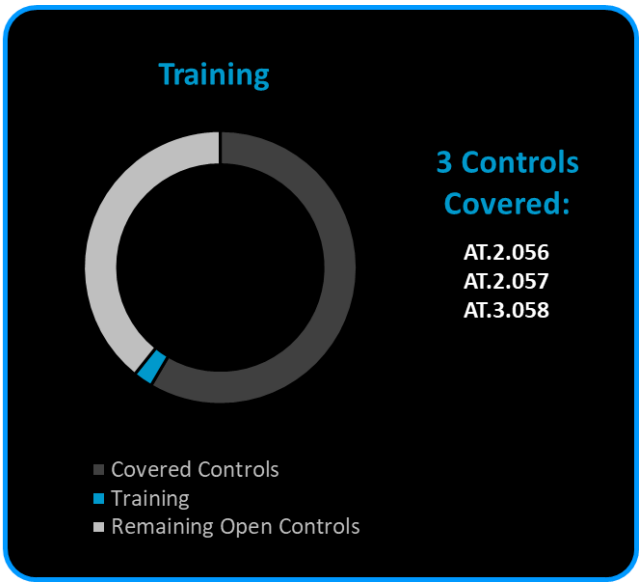
Controlling the flow of information, as well as controlling how information is created, processed, stored, and accessed, is a vital part of cybersecurity and CMMC compliance. Equally important is the need to ensure that user roles are arranged in such a way that only authorized personnel are given access to particular information. This is often accomplished by way of Office 365 (O365) and Azure.



Mission Multiplier is experienced in applying these products in the ways that will best benefit your organization in terms of both security and compliance. While other technical solutions do exist for managing this set of requirements, Mission Multiplier recommends this suite of resources based on our industry experience and near-ubiquity with DoD contractors.

Training

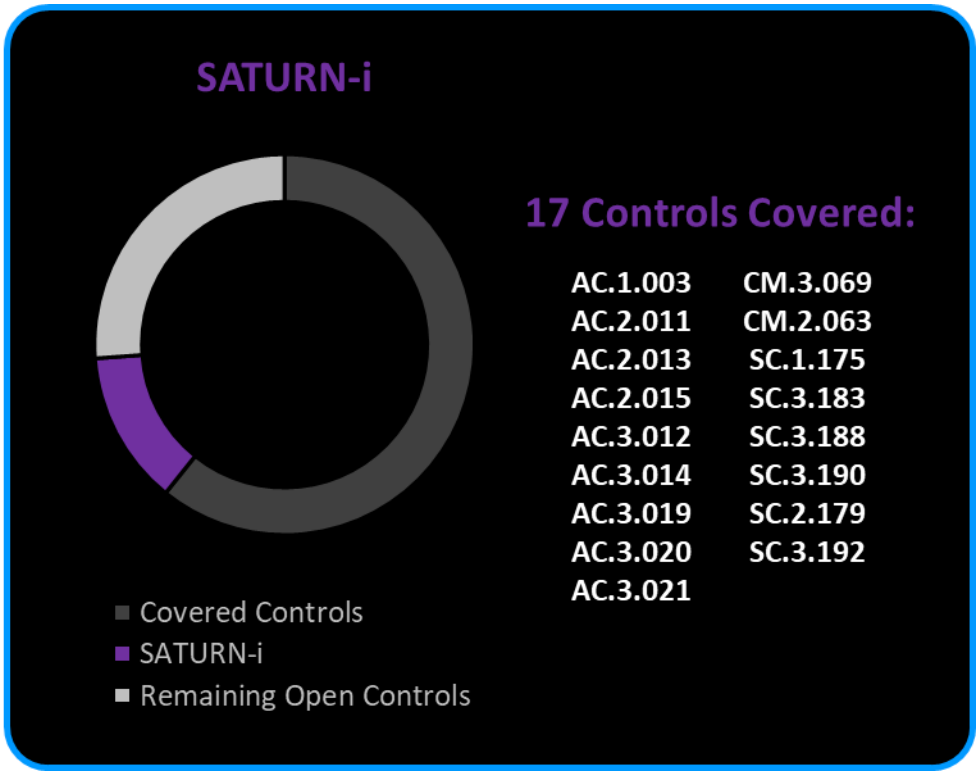
The CMMC standard requires that employees are trained on security awareness topics like insider threat. It also requires that individuals charged with specific security-related tasks are trained to perform their duties. Mission Multiplier can conduct training sessions to ensure that your employees are familiar with policies and knowledgeable in general cybersecurity practices, professional/job-oriented tasks as they pertain to cybersecurity, and have access to on-demand customized training as required.



Cyber Tools

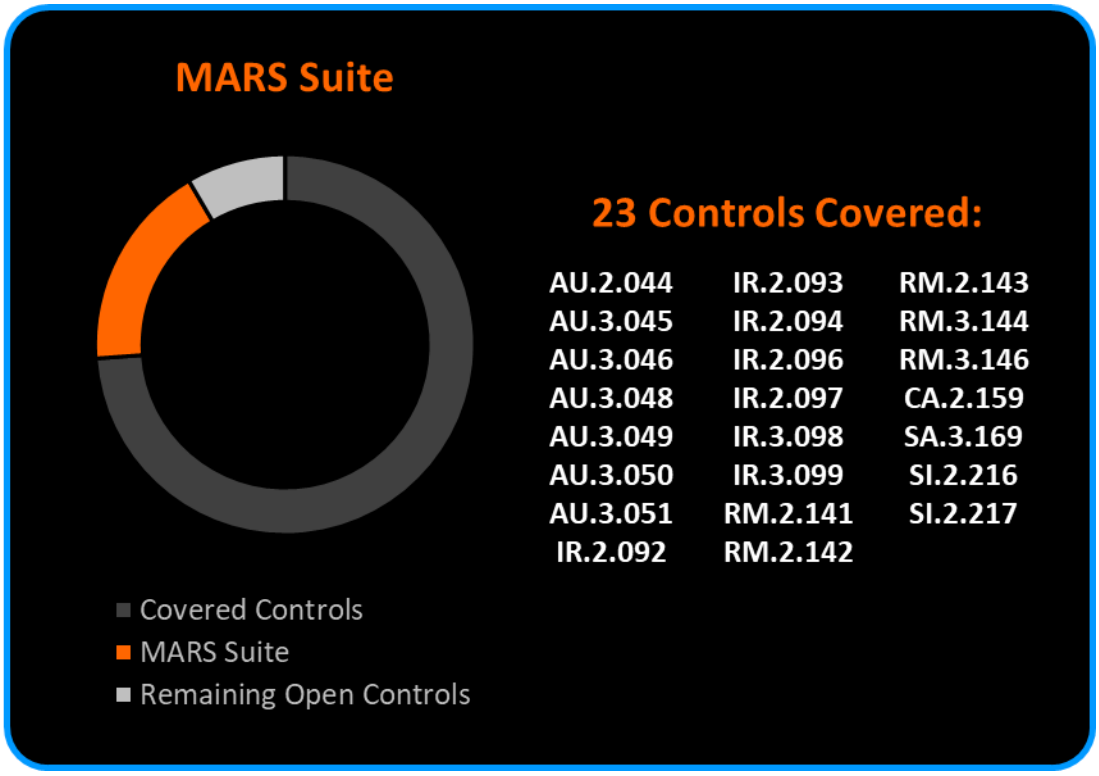
SATURN-i

Even those unfamiliar with the finer points of cybersecurity may be familiar with elements such as firewalls and web content filtering. What may not be as well known is the fact that such security countermeasures often represent a considerable expense for organizations. Mission Multiplier's SATURN-i can fulfill these functions and more at a reasonable cost and better value. Beyond firewall and web content filtering functionalities, the SATURN-i can also provide services such as intrusion prevention, application control, VPN, and other features that align with the requirements of NIST SP 800-171 Rev. 2 and the CMMC standard. Additionally, the CMMC standard requires that organizations, "Employ spam protection mechanisms at information system access entry and exits points." The SATURN-i can cover those requirements as well, meaning you can cover at least 17 of the tool-related CMMC controls with just one tool.



MARS Suite

Routine vulnerability scanning is a requirement of both DFARs and CMMC. Vulnerability scanning is used so that organizations can ensure that potential vulnerabilities within organizational systems are identified and addressed as quickly as possible. Vulnerabilities include weak passwords, outdated operating systems, and unpatched systems. These vulnerabilities are discovered via the use of a vulnerability scanner, which is a device or application that identifies organizational assets for vulnerabilities while creating a prioritized list of asset vulnerabilities based on level of severity. Obviously, acquiring such a scanner, implementing it on a network, managing it, and responding to the vulnerabilities it uncovers can be a daunting task. MARS Suite is Mission Multiplier's preferred choice for providing this scanning capability, and we can provide the necessary services to help you install and use MARS Suite in a way that satisfies the bulk of the remaining tool-related CMMC controls.



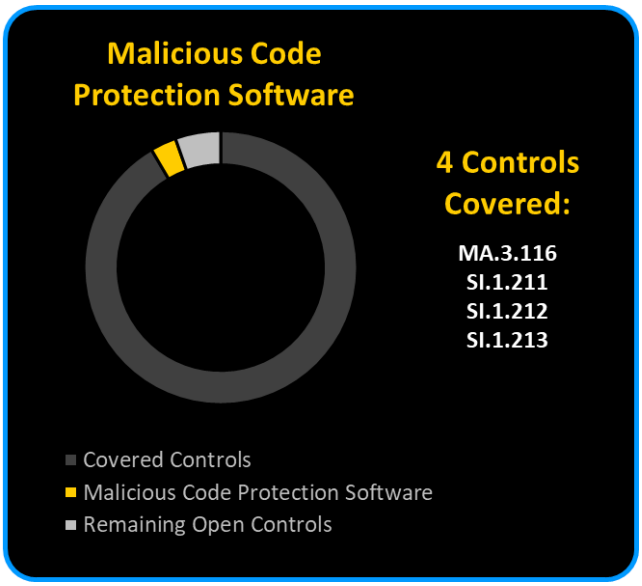
Beyond being a vulnerability scanner, the MARS Suite solution uses automated tools/technologies and data analytics to aggregate and normalize disparate data feeds to provide the continuous monitoring of IT systems, networks, and/or programs. It captures near real-time security information to effectively and efficiently manage risk, and enables the prioritization of resources, more informed decision-making, and

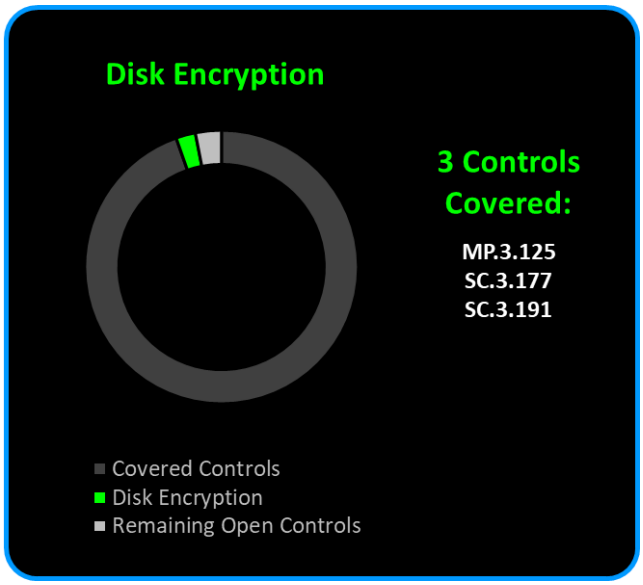
reduced cost. MARS Suite correlates cyber threat and vulnerability data to asset criticality, mission risks, and other operational data to achieve an Enterprise-wide Common Operating Picture – for Holistic Situational Awareness and to quickly identify and manage risk in an ever-changing network environment.

With this depth of situational awareness, organizations can use the MARS Suite to fulfill 23 or more of the CMMC requirements for Levels 1-3. For instance, within the domain of Incident Response (IR), organizations are required to analyze, correlate, and triage events to determine if a cyber incident (e.g. data breach) has occurred, as well as find the root cause of an event. With the information gathered and presented by MARS Suite, organizations can maintain ongoing awareness and support the incident response process.

Malicious Code Protection Software

The use of malicious code protection software, better known colloquially as anti-virus or anti-malware software, is a natural component of any cybersecurity program. This is especially true for DFARs and CMMC compliance. Mission Multiplier can leverage industry partnerships to bring tested and proven malicious code protection software to your organization and ensure that is the most appropriate choice for both CMMC compliance and your unique infrastructure.



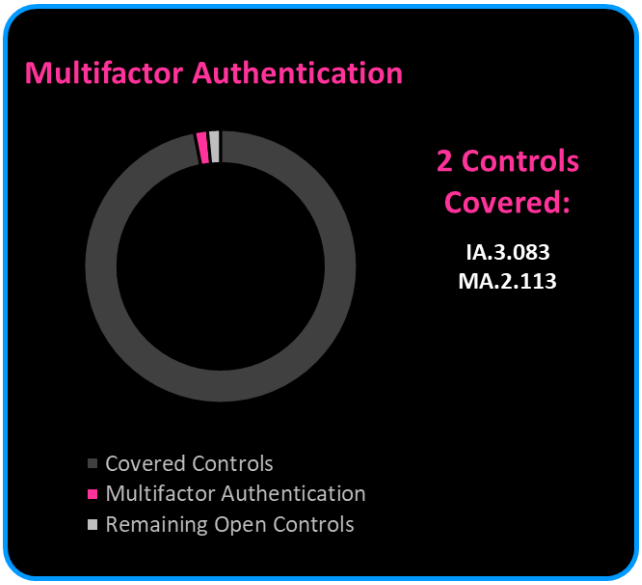


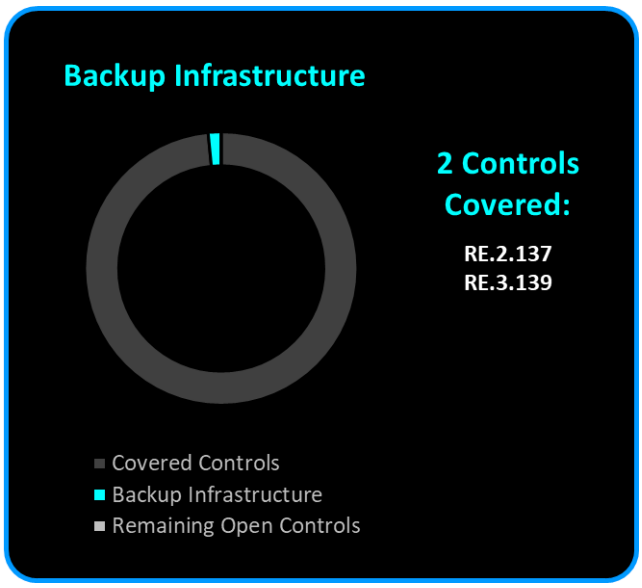
Disk Encryption

The protection of data at rest is a mainstay of cybersecurity, and the way to accomplish this while being CMMC compliant is to use FIPS-validated cryptography. Mission Multiplier can assist your organization by configuring existing encryption modules within your infrastructure (e.g. Bitlocker or FileVault), or assist in the procurement and implementation of other encryption mechanisms deemed necessary.

Multifactor Authentication

The DoD has made it abundantly clear that multifactor authentication is an unavoidable safeguard needed for DFARs compliance. Fortunately, NIST SP 800-171 Rev. 2 allows for a "variety of multifactor solutions" such as "hard tokens (e.g., smartcards, key fobs, or dongles) or a soft token solution." Mission Multiplier can make recommendations based on your unique infrastructure to provide the most appropriate form of multifactor authentication. Mission Multiplier can install a form of multifactor authentication on information systems, as well as assist with all stages of implementation, including user training, troubleshooting, and account association.





Backup Infrastructure

One key difference between the CMMC standard and the original DFARs requirements is that CMMC introduced the new Recovery (RE) domain. Within this domain, organizations are primarily required to manage and protect backups of critical data and systems. Backing-up information is a fundamental safeguard against data loss (e.g. from natural disasters), data corruption, sabotage, and ransomware attacks. Depending on their existing infrastructure, organizations may require additional hardware to facilitate the routine creation and support of backups. Mission Multiplier can make recommendations on the most appropriate solution for a given organization and can assist with the implementation and maintenance of new backup infrastructure.

Conclusion

The implementation of the one hundred and thirty (130) processes and practices found in the CMMC standard for levels 1-3, as required by the Office of the Under Secretary of Defense for Acquisition and Sustainment, encompasses many tasks that utilize many different strategies. With the help of Mission Multiplier, your organization can have access to a full turn-key solution to meet all of the requirements set forth by the CMMC standard. Whether it is a policy-driven requirement or a technical application that is needed, Mission Multiplier can leverage our exceptional roster of products and services to meet the needs of your organization.

About Mission Multiplier

Mission Multiplier is a HUBZone-certified small business headquartered in Huntsville, Alabama that specializes in full spectrum cybersecurity solutions – with a focus on cyber services for government and commercial markets, as well as the development of innovative cyber tools and technologies. Beyond Mission Multiplier bringing innovation to our products and services, we were founded on a truly innovative business value proposition. For every hour a Mission Multiplier employee works, we direct a portion of the company profit to a local charity of the employee's choice. In this way, each employee knows that not only are they getting to develop and deliver innovative cybersecurity services, but that they are directly giving back to the local community. Building on this principle, our goal is to multiply the successes that our clients achieve against their respective missions, while simultaneously enabling the missions of our employees – with the end result of securing and enriching the communities we serve.

Mission Multiplier
1300 Meridian St N Suite 101
Huntsville, AL 35801
www.missionmultiplier.com

ISO 9001 2015 CERTIFIED

HUBZone Historically Underutilized Business Zone CERTIFIED

BBB ACCREDITED BUSINESS
BBB Rating: A+