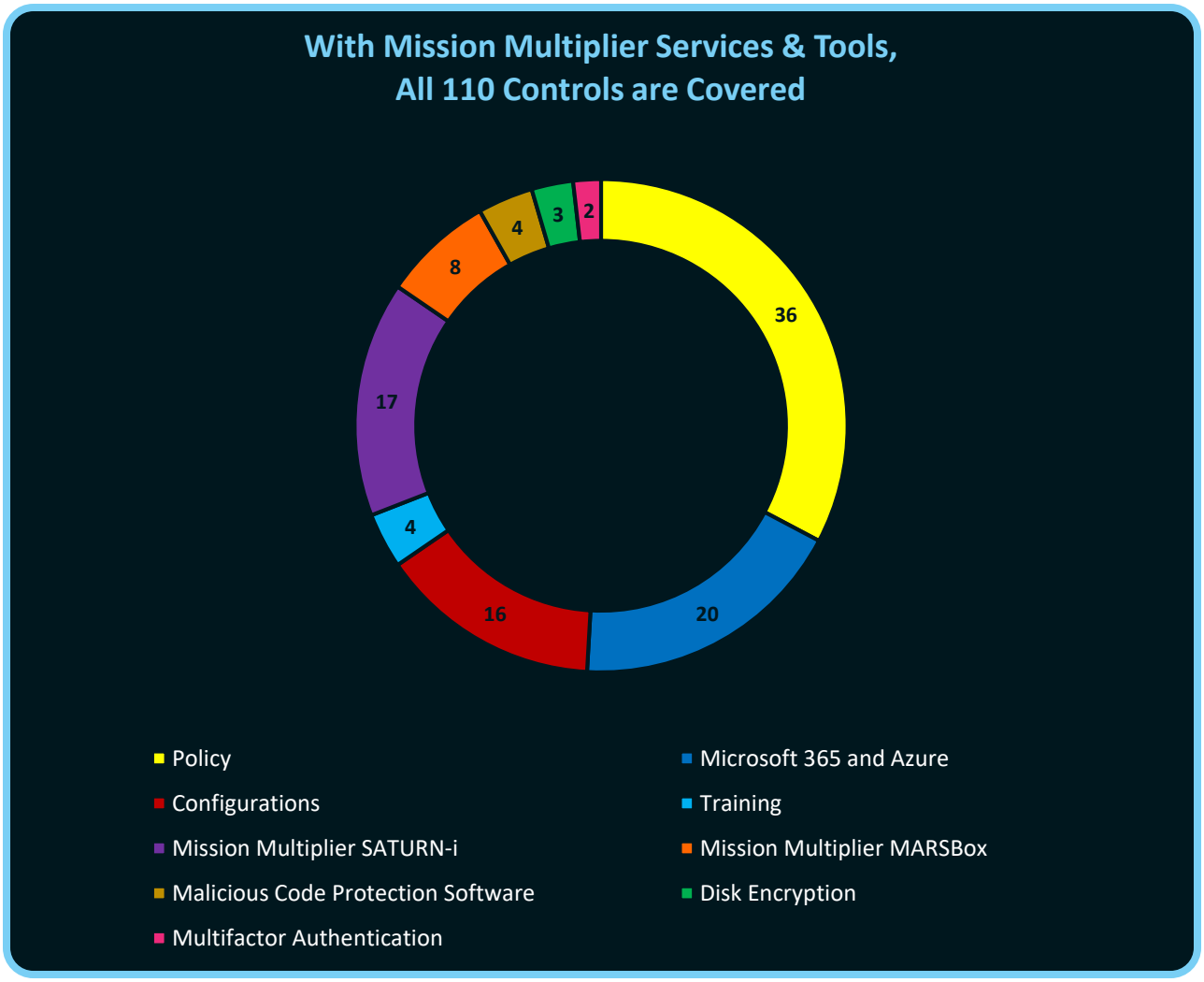
mission multiplier

DFARS Compliance by the Numbers

Introduction



By now, most contractors doing business with the Department of Defense (DoD) have heard of DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, which requires contractors to "implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017." Many contractors are aware that a System Security Plan (SSP) and a Plan of Actions and Milestones (POA&M) are the artifacts required to demonstrate implementation of NIST SP 800-171. Some may even know that NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, contains one hundred and ten (110) individual security controls that need to be addressed, the creation of a Plan of Action and Milestones (POA&M) and System Security Plan (SSP) being only two of those controls (control designations 3.12.2 and 3.12.4, respectively). So that leaves the question:

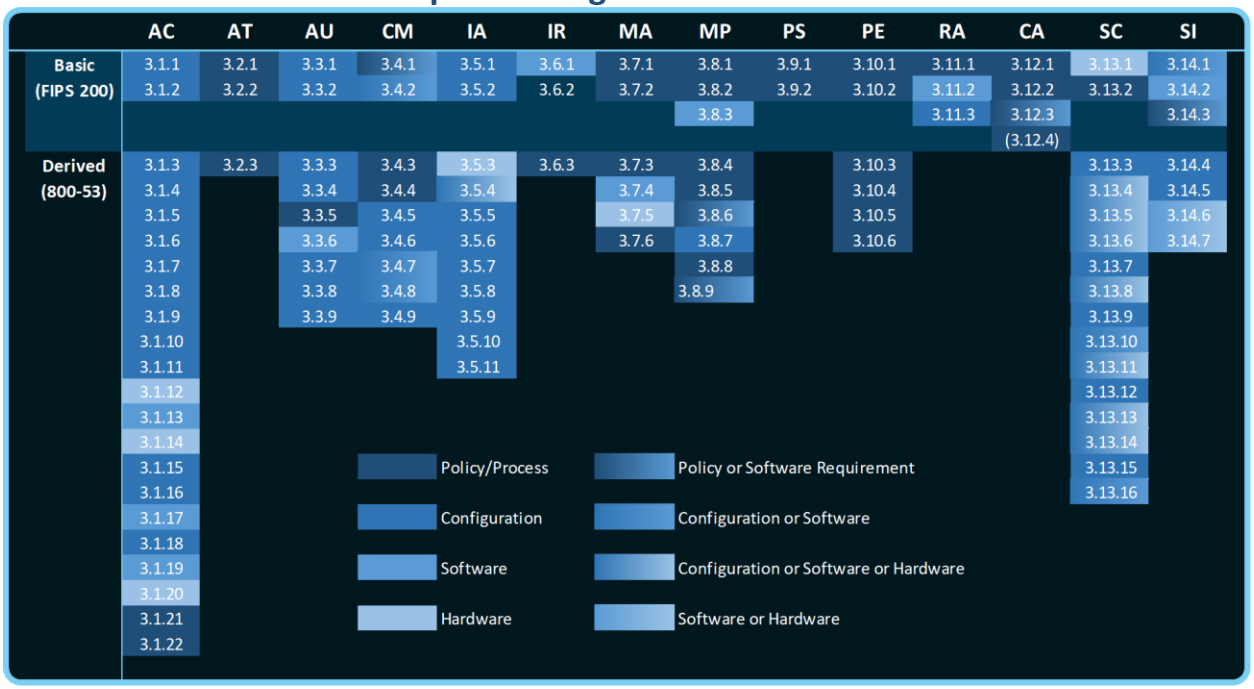
Beyond the creation of an SSP and POA&M, how does an organization go about implementing the remaining one hundred and eight (108) controls?

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. For companies new to the requirements, a reasonable approach would be to:**
>
> **1. Examine each of the requirements to determine**
>
> **— Policy or process requirements**
>
> **— Policy/process requirements that require an implementation in IT (typically by either configuring the IT in a certain way or through use of specific software)**
>
> **— IT configuration requirements**
>
> **— Any additional software or hardware required Note that the complexity of the company IT system may determine whether additional software or tools are required.**
>
> **2. Determine which of requirements can readily be accomplished by in-house IT personnel and which require additional research**
>
> **3. Develop plans of action to implement the requirements**

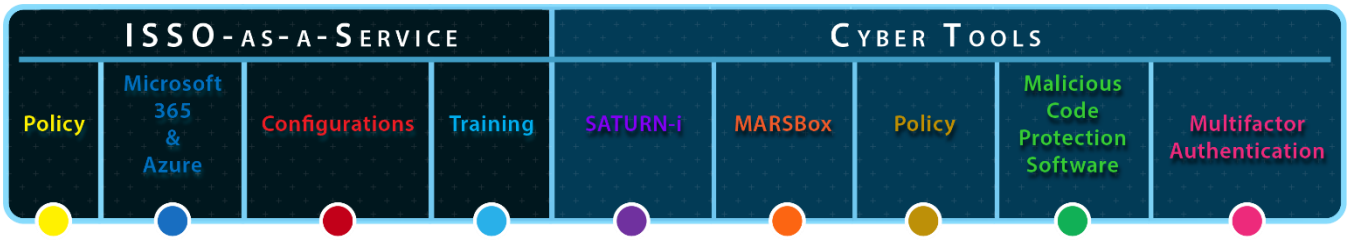
Furthermore, the DoD provides a reference chart breaking down the controls into their various categories of policy/process, configuration, software, hardware, or some combination thereof:

Implementing NIST SP 800-171



Even with guidance like this, implementing these controls can still 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 single, coordinated, streamlined implementation process. Simply put, Mission Multiplier is your organization's turn-key solution for complete adherence to the NIST SP 800-171 controls.

Within the scope of DFARs compliance, Mission Multiplier categorizes our cybersecurity solutions into two broad categories: ISSO-as-a-Service and Cyber Tools .



ISSO-as-a-Service entails many of the services usually associated with an in-house Information System Security Officer (ISSO) for the fraction of the cost of hiring a full-time employee. These duties primarily include policy writing, 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. Our ISSO-as-a-Service leverages Mission Multiplier's eclectic suite of cyber tools comprised of both proprietary solutions designed specifically with DFARs compliance in mind and industry-recognized off the shelf products that we have thoroughly reviewed and tested for the purpose of compliance.

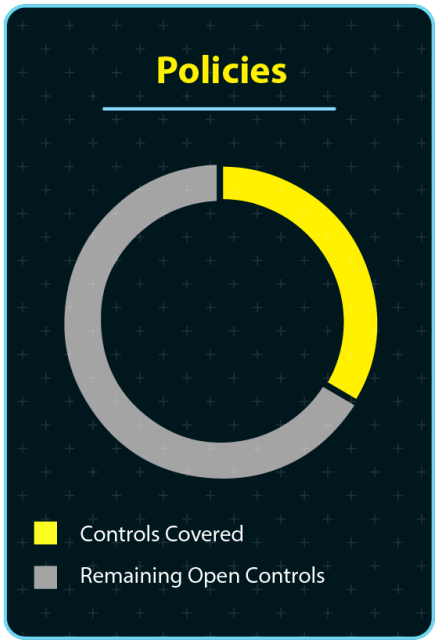
The combination of services and tools allows Mission Multiplier to assist your organization with meeting ***all*** of the one hundred and ten (110) controls required by NIST SP 800-171.

ISSO-as-a-Service

Policy

A key component of DFARs 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.”

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.



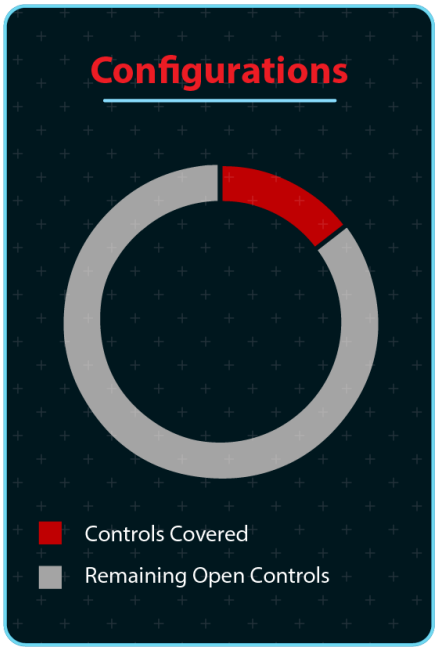
For example, one policy requirement might necessitate a hybrid technical and operational solution (such as installing a vulnerability scanning mechanism and codifying the policies required for the mechanism's operation). Mission Multiplier will craft the applicable policy in a way that your organization can reasonably adapt to the change and give sufficient time for the policy to proliferate throughout the organization.

Policy
36 Controls Covered

3.1.21
3.1.22
3.3.5
3.4.3
3.4.4
3.4.5
3.6.1
3.6.2
3.7.1
3.7.2
3.7.3
3.7.6
3.8.1
3.8.2
3.8.4
3.8.5
3.8.8
3.8.9
3.9.1
3.9.2
3.10.1
3.10.2
3.10.3
3.10.4
3.10.5
3.10.6
3.11.1
3.11.3
3.12.1
3.12.2
3.12.3
3.12.4
3.13.2
3.13.14
3.14.1
3.14.3

Configurations

One common misconception about DFARs compliance is that it requires the purchase of copious amount of additional hardware and software. On the contrary, many organizations already have the necessary 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 DFARs. Such modifications can include closing network ports, removing unnecessary services, configuring firewalls, and establishing inactivity conditions. With Mission Multiplier, your organizational information systems can be configured and hardened to be more secure and compliant.

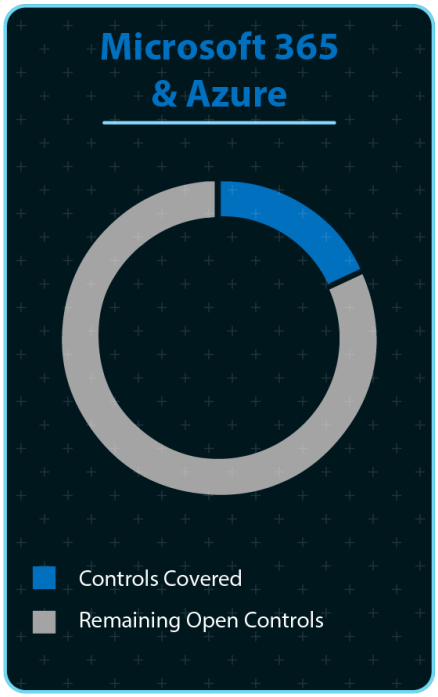


Configurations
16 Controls Covered

3.1.3
3.1.10
3.1.19
3.3.7
3.4.1
3.4.2
3.4.6
3.4.7
3.8.7
3.13.4
3.13.5
3.13.7
3.13.9
3.13.10
3.13.12
3.8.3

Microsoft 365 and 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 DFARs 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 can be accomplished by way of Microsoft 365 and Azure. Mission Multiplier is experienced in applying these products in a way that best benefits 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 contractors working for the DoD.



Microsoft 365 & Azure 20 Controlls Covered

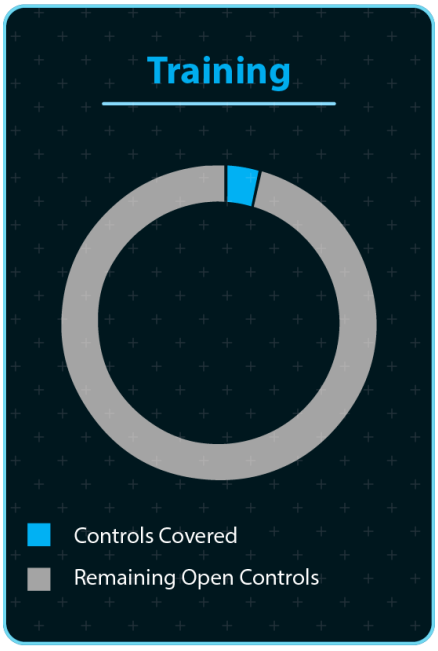
3.1.1
3.1.2
3.1.4
3.1.5
3.1.6
3.1.7
3.1.8
3.1.9
3.5.1
3.5.2
3.5.4
3.5.5
3.5.6
3.5.7
3.5.8
3.5.9
3.5.10
3.5.11
3.13.3
3.13.8

Training

Once policies are created, accepted, and applied to organizational users, training must be conducted in order to ensure that the policies are fully understood and followed by users. This process is realized through training. 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 on-demand customized training as required.

Training 4 Controls Covered

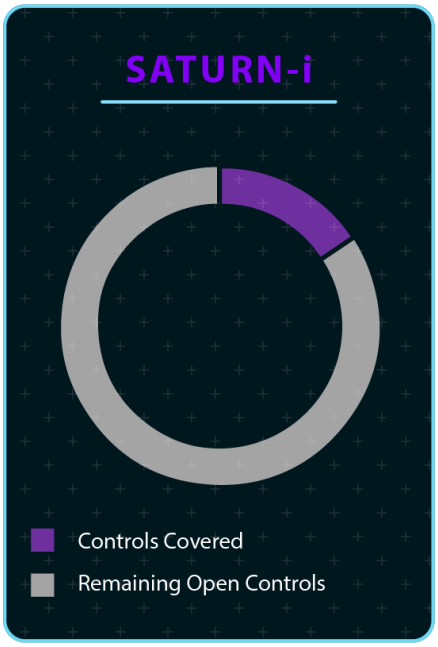
3.2.1
3.2.2
3.2.3
3.6.3



Cyber Tools

Mission Multiplier 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 meet these requirements and more at a reasonable cost and better value. Beyond that, 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.



SATURN-i 17 Controls Covered

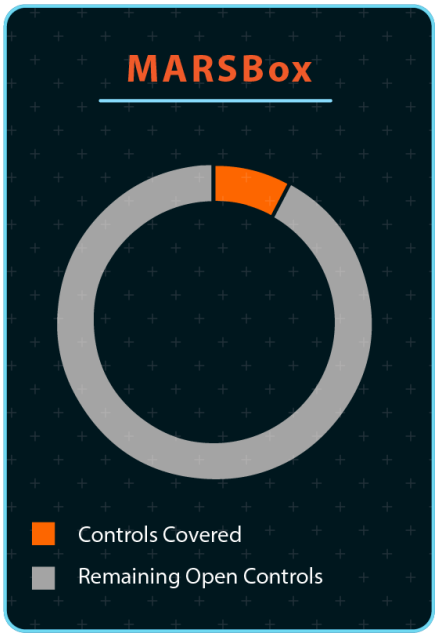
- 3.1.11
- 3.1.12
- 3.1.13
- 3.1.14
- 3.1.15
- 3.1.16
- 3.1.17
- 3.1.18
- 3.1.20
- 3.4.8
- 3.4.9
- 3.13.1
- 3.13.6
- 3.13.13
- 3.13.15
- 3.14.6
- 3.14.7

Mission Multiplier MARS Box

Proper log management and vulnerability scanning are also vital parts of DFARs compliance. These two requirements are covered by a proprietary solution we call the Mission Multiplier MARS Box. This simple, compact hardware solution can be easily integrated into any organizational network infrastructure to ensure technical activity logs (e.g. user logins, system updates, etc.) are recorded and maintained and to perform routine vulnerability scanning, ensuring that you are aware of any emerging vulnerabilities that require patching or other mitigation efforts.

MARSBox 8 Controls Covered

3.3.1
3.3.2
3.3.3
3.3.4
3.3.6
3.3.8
3.3.9
3.11.2

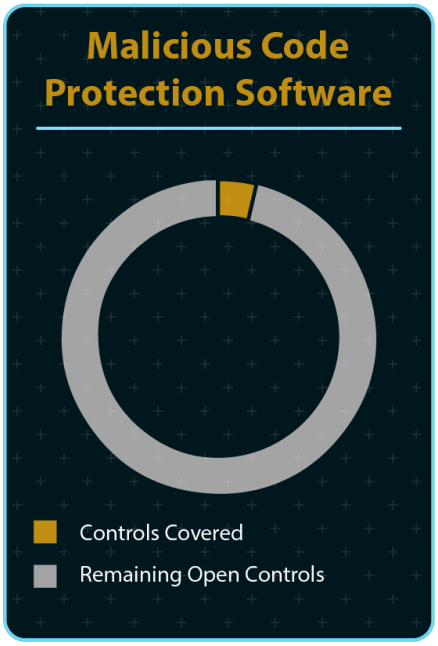


Malicious Code Protection Software

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 compliance. Mission Multiplier can leverage industry partnerships to bring tested and proven malicious code protection software to your organization that is most appropriate for both DFARs compliance and your unique infrastructure.

Malicious Code Protection Software Covered

3.7.4
3.14.2
3.14.4
3.14.5

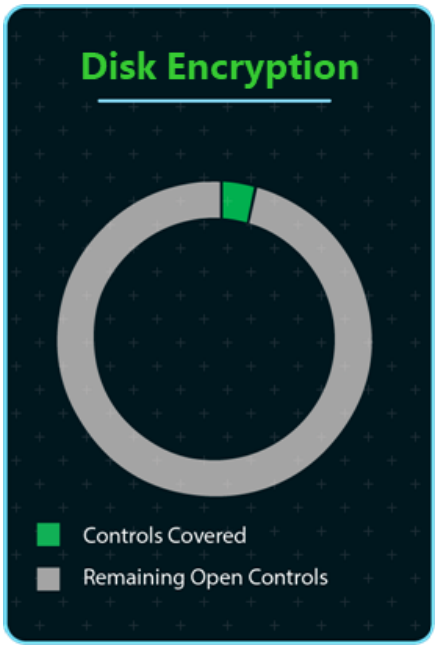


Disk Encryption

The protection of data at rest is a mainstay of cybersecurity, and DFARs should be accomplished via 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.

Disk Encryption
3 Controls Covered

3.8.6
3.13.11
3.13.16

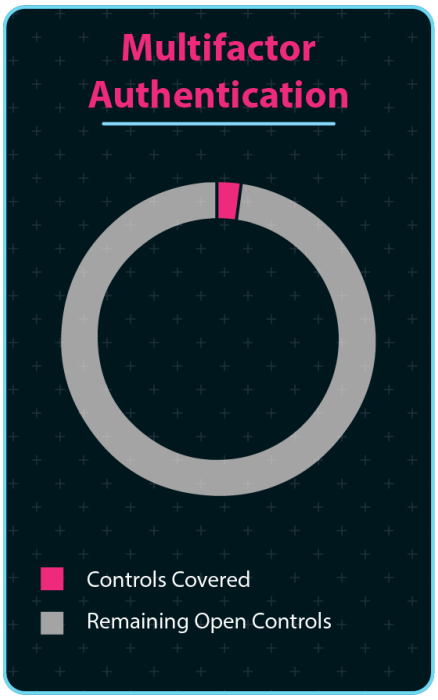


Multifactor Authentication

The DoD has made it abundantly clear that multifactor authentication is an unavoidable safeguard needed for DFARs compliance. Fortunately, NIST SP 800-171 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.

Multifactor Authentication
2 Controls Covered

3.5.3
3.7.5



Conclusion

The implementation of the one hundred and ten (110) controls found in NIST SP 800-171 as required by DFARs 252.204-7012 encompasses many tasks utilizing many different strategies. With Mission Multiplier,

your organization can have access to a full turn-key solution to meet all controls. 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 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+