THE TRIPLE PLAY
DFARS, CMMC & ITAR

AN E-BOOK

FROM MANAGED SERVICES PROVIDER

SIMPLE HELIX

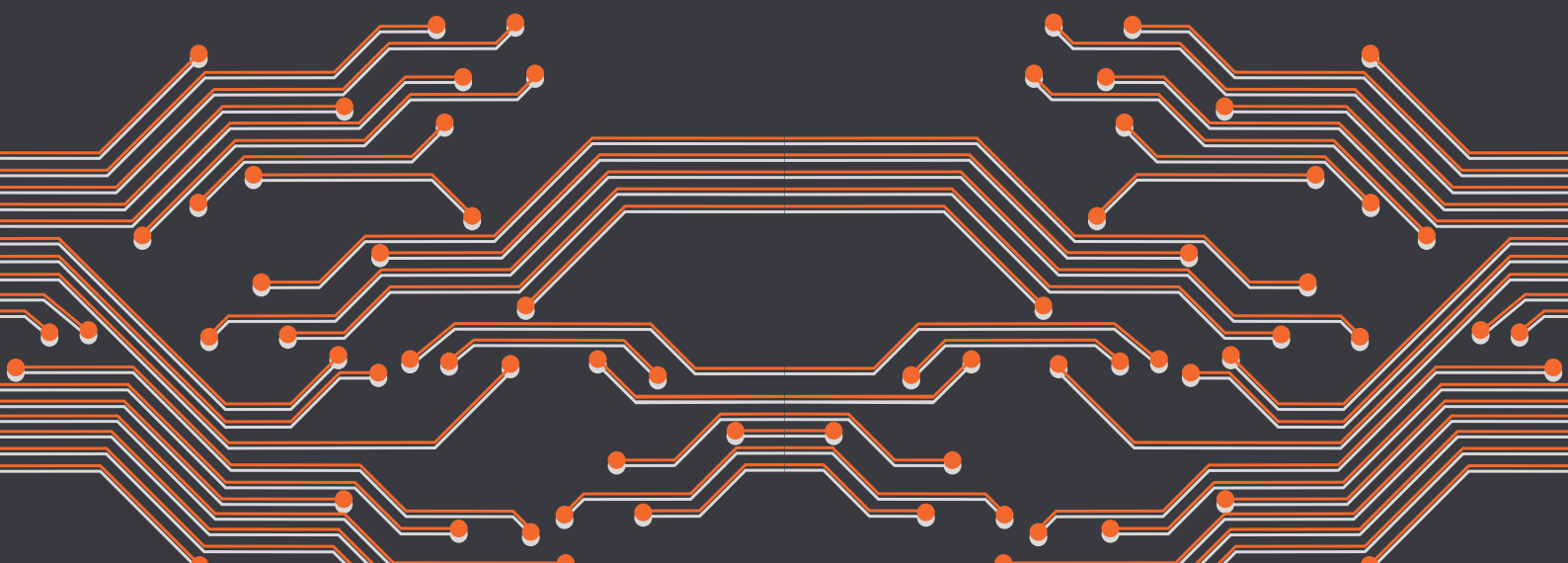
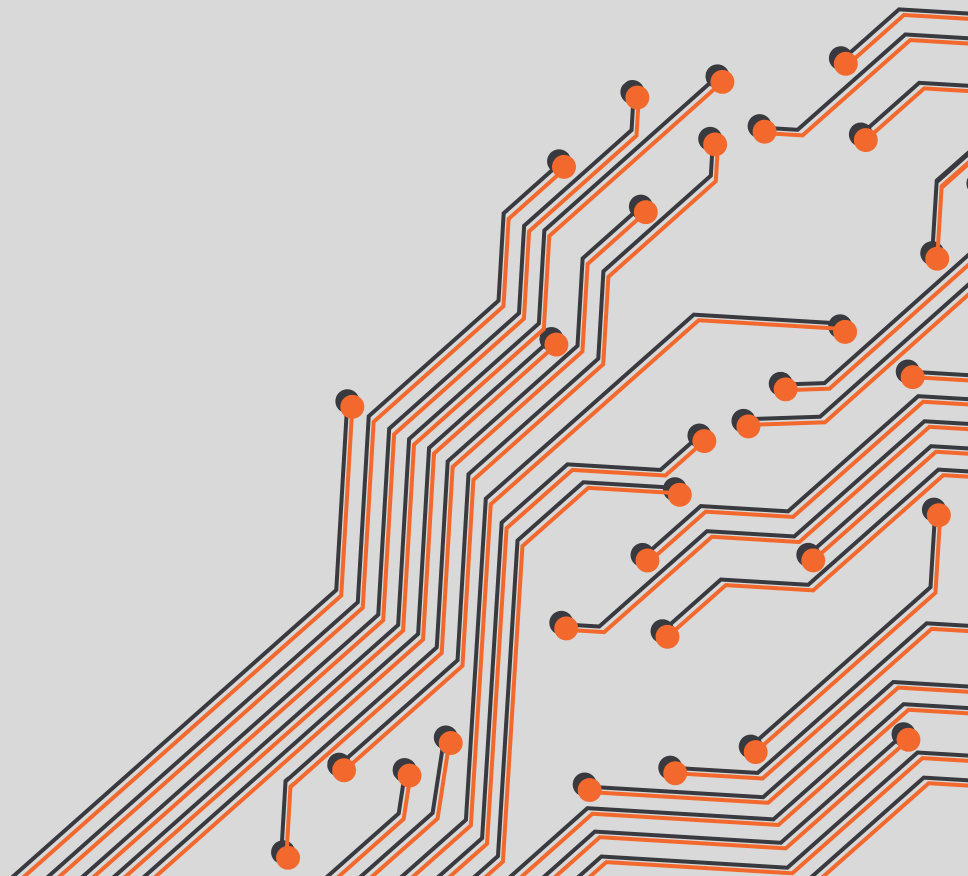


TABLE OF CONTENTS



DFARS

WHY IS THIS HAPPENING?

The DoD has released a new interim rule on September 29, 2020 for grading your NIST 800-171 self attestation assessment. This has been put in place to bridge the gap between NIST 800-171 and CMMC Level 3 deployment.

WHAT IS THE DFARS INTERIM RULE CHANGE?

The new control adds two critical clauses.

1. 252.204–7019 is a solicitation clause that advises contractors, "**They must have a current (not older than three years) assessment on record in a government database.**" This clause is required in all DoD solicitations except for commercially available off-the-shelf items(COTS).
2. The second clause 252.204–7020 designates **the methodology that contractors need to use when conducting Basic Assessments.**

DFARS 252.204-7020 is required in all solicitations and contracts, except for those solely to acquire COTS items. The contractor must acquire an assessment at one of three levels:

1. **Basic** - Self-assessment submitted to the DoD. Required for all new contract actions, including option exercises.
2. **Medium** - Conducted by the DoD (our expectation is that it will be virtual but we have not confirmed).
3. **High** - In person, Onsite Assessment conducted by the DoD

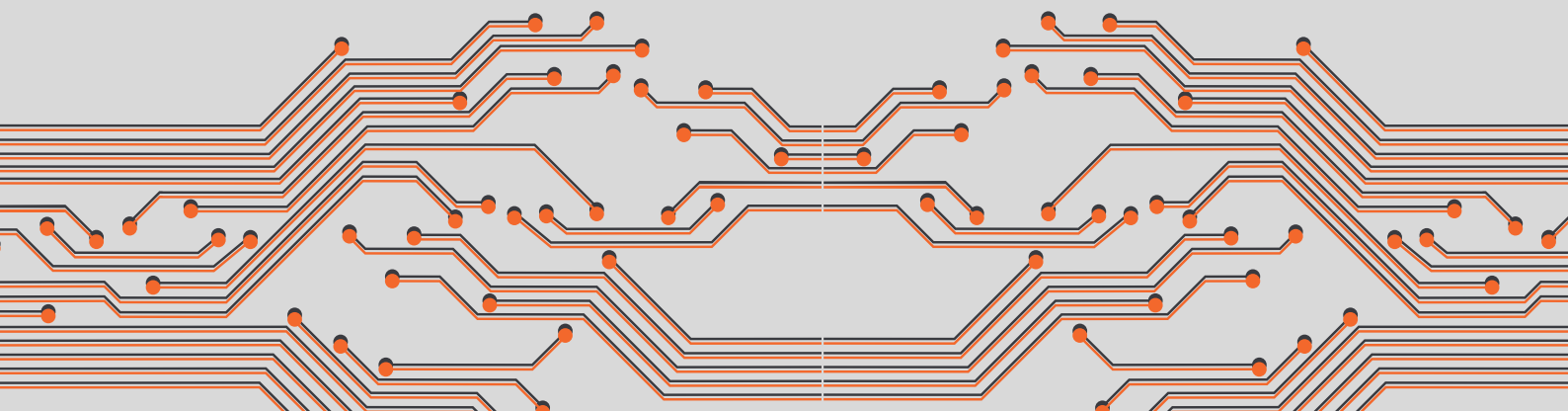
WHEN WILL CONTRACTORS HAVE TO ADHERE TO THIS NEW RULE?

By November 30, 2020, all DoD Contractors will have to have their self-assessments submitted to the Supplier Performance Risk System (SPRS) at https://www.sprs.csd.disa.mil/.

DFARS INTERIM RULE HIGHLIGHT REQUIREMENTS

The table below shows the first 5 security requirements from the DFARS Interim Rule the are assigned a -5 point value. Also featured on the table are Simple Helix's recommended solutions for meeting each requirement. You can find the entire table of requirements at the link provided here.

Security Requirement		Value	Simple Helix Solution
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)	5	Password Implementation, Key Card Access, Firewall, Multi-Factor Authentication with DUO
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	5	Active Directory, O365, and Multi-factor Authentication with DUO
3.1.12	Monitor and control remote access sessions. • Comment: Do not subtract points if remote access not permitted	5	VPN, Multi-Factor Authentication with DUO, Monitor & Review Log Files with LogRhythm
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. • Comment: Do not subtract points if remote access not permitted	5	VPN, PreVeil, O365
3.1.16	Authorize wireless access prior to allowing such connections • Comment: Do not subtract points if wireless access not permitted	5	Active Directory, Firewall, Routing Policies, IP Routing



CMMC

WHY IS THIS HAPPENING?

As the threat of data theft rises daily, so does the need to protect our nation's sensitive information. The Defense Industrial Base or DIB and DoD serve as major targets for cyber adversaries. These adversaries are most interested in gaining insight regarding our war machines and defense technologies. To prevent them from gaining this insight, our nation must seek to strengthen it's cyber security hygiene. Because of this CMMC was created. The new compliance standard ensures those companies that develop our greatest technologies can also keep them safe from those who would use them against us.

WHAT IS CMMC?

The Cybersecurity Maturity Model Certification or CMMC is a new standard of cybersecurity compliance developed by the Department of Defense (DoD). The compliance standard is an evolution of the DFARS 252.204-7012 & NIST 800-171 standards and is meant to protect the nation's most sensitive data from our adversaries. **All government contractors will have to become CMMC Compliant by 2026 in order to continue business with the U.S. Government.**

WHEN WILL CONTRACTORS HAVE TO BE CERTIFIED?

The CMMC roll-out will be a phased approach over a 5-year period starting with the release of 10 RFIs and RFPs in 2020. The number of new contracts requiring CMMC certification will grow in subsequent years until all contracts require CMMC Compliance in 2026. Contractors will have to meet CMMC Compliance in order to be awarded these contracts. Deciding when to start on the journey to compliance will depend on the release of the contractor's preferred RFI/RFP as well as what their business circumstances dictate. Contractors will be able to bid on opportunities prior to becoming CMMC compliant. However, they will not be awarded the contract unless they meet the compliance requirement.

CMMC

HOW IS CMMC SET UP?

The CMMC Standard is comprised of 5 levels. Each level is cumulative and features more practices (or requirements) than the level before it. Implementation and maintenance costs rise with each level as well. Level number 3 will be the most popular level pursued by DoD Contractors. Which level you pursue depends on what types of contracts your company bids on. For guidance on which level to choose, you will need to consult a CMMC Expert.

There are four types of CMMC Experts that you will encounter on your journey to compliance.

1. GAP Assessors
2. Implementors
3. Certified Third Party Assessment Organizations (C3PAOs)
4. Ongoing Support Providers

To obtain contact information for these types of individuals/companies, please feel free to contact Simple Helix at 256-704-1041.

THE TABLES BELOW SHOW THE PRACTICE OF EACH LEVEL AND OUR RECOMMENDED TOOLS. SIMPLE HELIX PROVIDES SOLUTIONS FOR THE PRACTICES BELOW AUGMENTED THROUGH MANAGED SERVICES.

LEVEL 1: BASIC CYBER HYGIENE

LEVEL	PRACTICE	SOLUTION	PRACTICES COVERED*
1	Spam Filtering	Office 365	11/17
	Password Encryption	Multi-factor Authentication by DUO	
	Antivirus	Webroot	

LEVEL 2: INTERMEDIATE CYBER HYGIENE

LEVEL	PRACTICE	SOLUTION	PRACTICES COVERED*
2	All previous practices	See previous tools/services	46/72
	Offsite, offline backups	Veeam Cloud-based Backups	

*The # of Practices Covered are based on how many practices Simple Helix can meet within the level associated.

LEVEL 3: GOOD CYBER HYGIENE

LEVEL	PRACTICE	SOLUTION	PRACTICES COVERED*
3	All previous practices	See previous tools/services	87/130
	DNS Filtering	Webroot or Palo Alto Firewalls	
	Encrypted Email & File Sharing	Office 365, Office 365 GCC High, or PreVeil	
	Retroactive monitoring of Log Files	LogRhythm SIEM Solution	
		SOC Monitoring Services	

LEVEL 4: PROACTIVE

LEVEL	PRACTICE	SOLUTION	PRACTICES COVERED*
4	All previous practices	See previous tools/services	100/156
	Proactive monitoring of Log Files	LogRhythm SIEM Solution	
		SOC Monitoring Services	

LEVEL 5: ADVANCED/PROGRESSIVE

LEVEL	PRACTICE	SOLUTION	PRACTICES COVERED*
5	All previous practices	See previous tools/services	107/171
	24/7, real-time monitoring of Log Files	LogRhythm SIEM Solution	
		SOC Monitoring Services	

*The # of Practices Covered are based on how many practices Simple Helix can meet within the level associated.

ITAR

WHY IS THIS HAPPENING?

The International Traffic in Arms Regulation (ITAR) was put in place by the Government to ensure materials being sent outside the United States are secure.

WHAT IS ITAR?

The International Traffic in Arms Regulation (ITAR) is an export control for the United States Munitions List(USML), which contains articles, services, and related technology. Discussions with several Simple Helix Prime Contractors revealed that among the three compliances on the horizon, Nist 800-171 Revision, CMMC Level 3, and ITAR. ITAR is their most considerable concern.

On March 23, 2020, the U.S. Department of State issued a final ruling explaining the accepted use of end-to-end encryption to secure sensitive data and enable cloud adoption. The ITAR Data Protection carve-out was the result of that ruling. The carve-out establishes that defense companies can now share unclassified ITAR technical data without requiring an export license.

The stipulation states that properly secured data must have end-to-end encryption and must use decryption keys that are not shared with any third parties. According to the Federal Register: "properly secured (by end-to-end encryption) electronic transmission or storage of unclassified technical data via foreign communications infrastructure does not constitute an export, reexport, retransfer, or temporary import."

WHEN WILL CONTRACTORS HAVE TO BE ITAR COMPLIANT?

Contractors that export materials outside of the United States must be ITAR Compliant now. The standard has already taken effect.

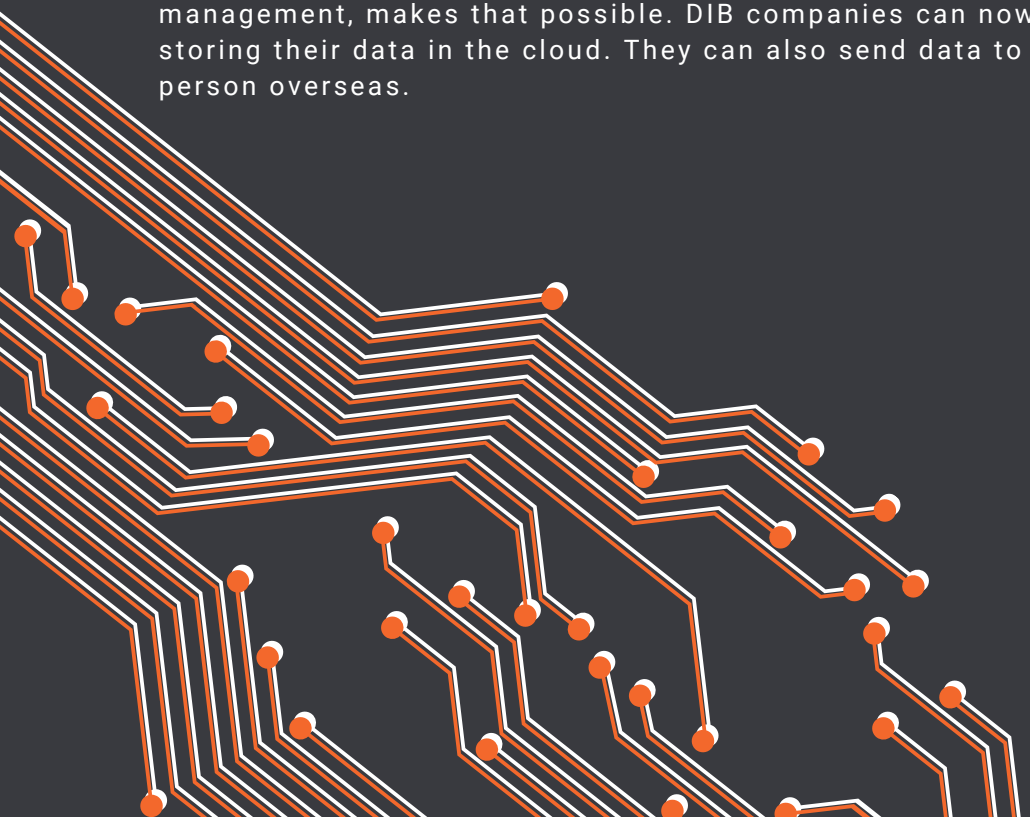
ITAR is the only one that spells out precisely what penalties will transpire on the unfortunate contractor that does not follow the rules. Violation of this control can result in civil fines. These fines range up to $500,000. Criminal penalties can range up to $1M. Imprisonment for up to 10 years and or being barred from conducting any export business in the future.

ITAR CARVE-OUT REQUIREMENT HIGHLIGHTS

Before this ruling, ITAR technical data had to reside on cloud platforms that were expensive and difficult to use. The servers had to be located exclusively in US-based data centers. Those data centers could only employ U.S. personnel. The new carve-out frees technical data from many of the restrictions the old rules imposed. The ruling clarifies that end-to-end encrypted technical data may be stored on any cloud service. As long as it does not store data in a country hostile to the U.S. or the Russian Federation. Additionally, the data can be accessed by U.S. or authorized persons outside the U.S. The specifications for the exchange are:

Security Requirement	Simple Helix Solution
Data must be unclassified	PreVeil
Data must be secure with end-to-encryption that meets FIPS 140-2 compliant algorithms	
Cloud services providers can't access the decryption keys	
Data is not intentionally sent to a person in or stored in restricted countries	
Data is not sent from a restricted country	

The new carve-out provides DIB companies with the flexibility to use cloud computing in ways denied in the past. End-to-end encryption, with proper key management, makes that possible. DIB companies can now easily take advantage of storing their data in the cloud. They can also send data to a U.S. or authorized person overseas.



THE TRIPLE PLAY DIFFERENCE

As a convenience to our customers, Simple Helix is now offering what we like to call "The Triple Play." This service is centered around the compliance standards mentioned above. A**fter our partners assess your compliance needs in regards to DFARS, CMMC, and ITAR, our team of IT experts will implement the tools and services that will help you pass your audit for all three standards.**

INCLUDED IN THIS PACKAGE

DFARS

- Initial Assessment
- POA&M
- SSP Creation
- Implementation of SSP
- Managed IT Services
- Ongoing Support

CMMC L3

- Initial Assessment
- POA&M
- SSP Creation
- Implementation of SSP
- Managed IT Services
- Ongoing Support

ITAR

- Initial Assessment
- POA&M
- SSP Creation
- Implementation of SSP
- Managed IT Services
- Ongoing Support

FOR A FREE CONSULTATION, CONTACT US:

(256) 704-1041
SALES@SIMPLEHELIX.COM

OR VISIT US AT SIMPLEHELIX.COM

DUNS: 009815946 | CAGE: 7FNU2 | NAICS: 518210 (PRIMARY), 517311, 541513, 541519, 541690

SIMPLE HELIX

CITATIONS

1 Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-Do41) by Defense Acquistion Regulations System https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of (last accessed October 26, 2020)

2 *NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1* by Unknown Author https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%206.24.2020.pdf (last accessed October 26, 2020)

3 *Cybersecurity Maturity Model Certification (CMMC) Version 1.02* by Unknown Author https://wplstage.simplehelix.host/wp-content/uploads/2020/07/CMMC_ModelMain_V1.02_20200318.pdf (last accessed July 23, 2020)

4 *International Traffic in Arms Regulations: Creation of Definition of Activities That Are Not Exports, Reexports, Retransfers, or Temporary Imports; Creation of Definition of Access Information; Revisions to Definitions of Export, Reexport, Retransfer, Temporary Import, and Release* by the State Department https://www.federalregister.gov/documents/2019/12/26/2019-27438/international-traffic-in-arms-regulations-creation-of-definition-of-activities-that-are-not-exports (last accessed October 26, 2020)