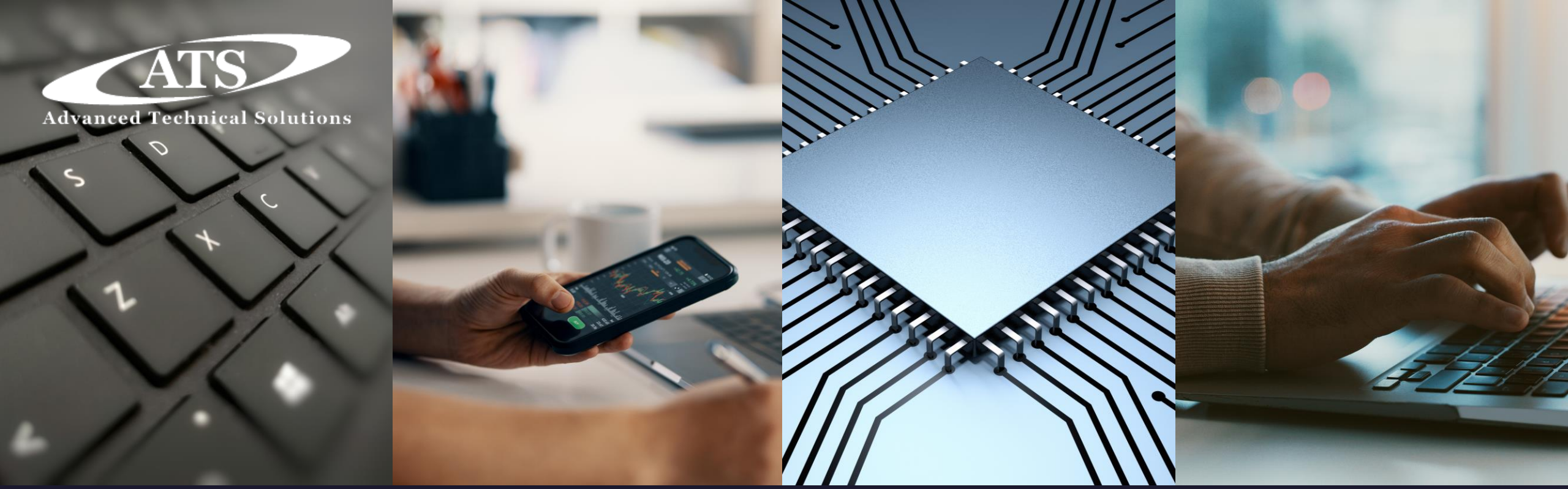
ATS

Advanced Technical Solutions

NIST 800-171 & CMMC 2.0

Guidance from an RPO



About ATS

Advanced Technical Solutions (ATS) is a leading Information Technology (IT) and Information Systems (IS) service provider serving small, medium, and large organizations across New York State for more than 18 years.

We build strong, long-term relationships with our clients and offer budget-conscience service plans. We can fully manage or co-manage your IT/IS needs and offer cybersecurity assessments, cloud solutions, consulting, and top-notch customer service while always following our philosophy: Take pride in our work, be sensitive to client needs, and be flexible in our approach.

ATS
Advanced Technical Solutions

Agenda

- Introduction to CMMC
- CMMC 2.0
- Risks
- Cost and Funding Opportunities
- Audience Questions and Answers

ATS
Advanced Technical Solutions

Introduction to CMMC

- ❑ What is CMMC?
- ❑ Who is subject to CMMC?
- ❑ Journey to CMMC 2.0
- ❑ CMMC 2.0 Maturity Levels

WHAT IS CMMC?

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

- The **Cybersecurity Maturity Model Certification (CMMC)** is a major Department of Defense (DoD) program built to protect the defense industrial base (DIB) from increasingly frequent and complex cyber attacks. It particularly aims to enhance the protection of controlled unclassified information (CUI) and federal contract information (FCI) shared within the DIB.

- CMMC builds on existing trust-based regulations (DFARS 252.204-7012) by adding a verification component for cybersecurity requirements.

- DoD's Office of the Under Secretary of Defense for Acquisition & Sustainment developed the CMMC Framework, working with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDC), and industry. The Framework combines various cybersecurity standards and best practices, intended to:

  - Safeguard sensitive information to enable and protect the warfighter
  - Dynamically enhance DIB cybersecurity to meet evolving threats
  - Ensure accountability while minimizing barriers to compliance with DoD requirements
  - Contribute towards instilling a collaborative culture of cybersecurity and cyber resilience
  - Maintain public trust through high professional and ethical standards

WHO IS SUBJECT TO CMMC?

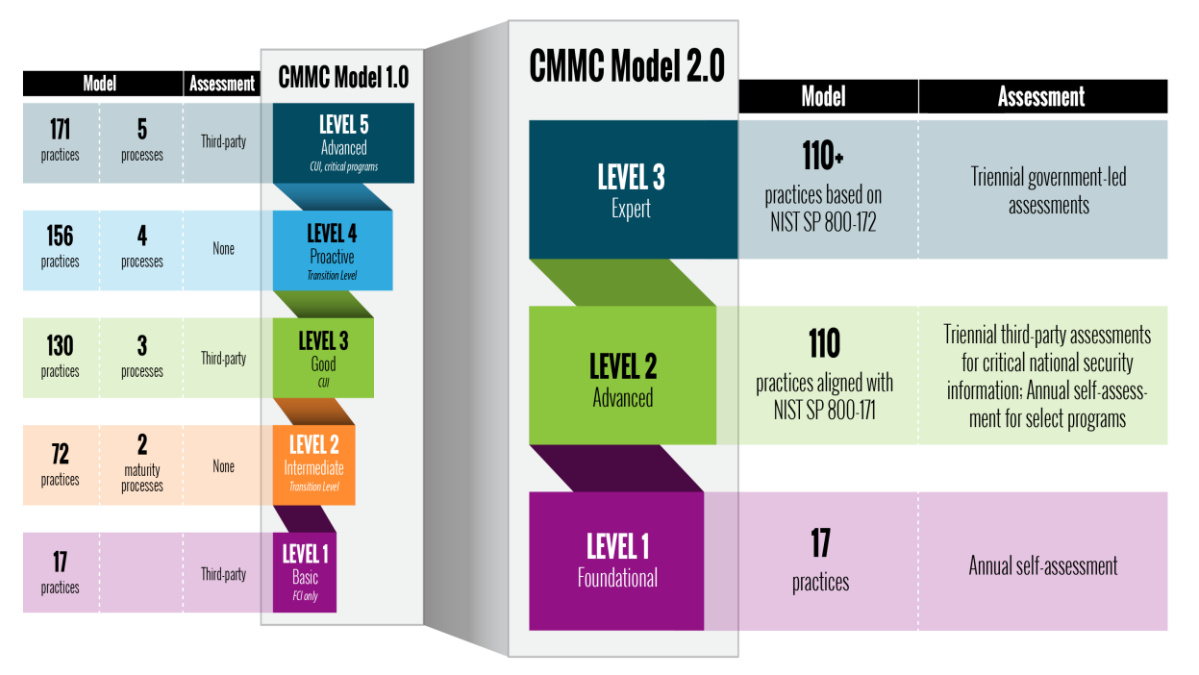
CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

- All DoD prime and sub-contractors planning to bid on future contracts with the CMMC DFARS clause will be required to obtain a CMMC certification prior to contract award. Some prime- and sub-contractors accessing, processing or storing FCI (but not CUI) will minimally require a Level 1 attestation. A DoD contract will specify which level of compliance a contractor needs to meet.

- All DIB members should learn the CMMC's technical requirements not only for certification but for long-term cybersecurity agility. However, DoD recognizes that many DIB members are small businesses that lack the resources of their larger, prime counterparts. As a result, the CMMC Framework incorporates cost-effective and affordable controls for small businesses to implement at the lower CMMC levels.

- Overall, CMMC is designed to provide DoD increased assurance that a DIB company can adequately protect sensitive CUI and FCI, accounting for information flow down to subcontractors in a multi-tier supply chain.

Journey to CMMC 2.0



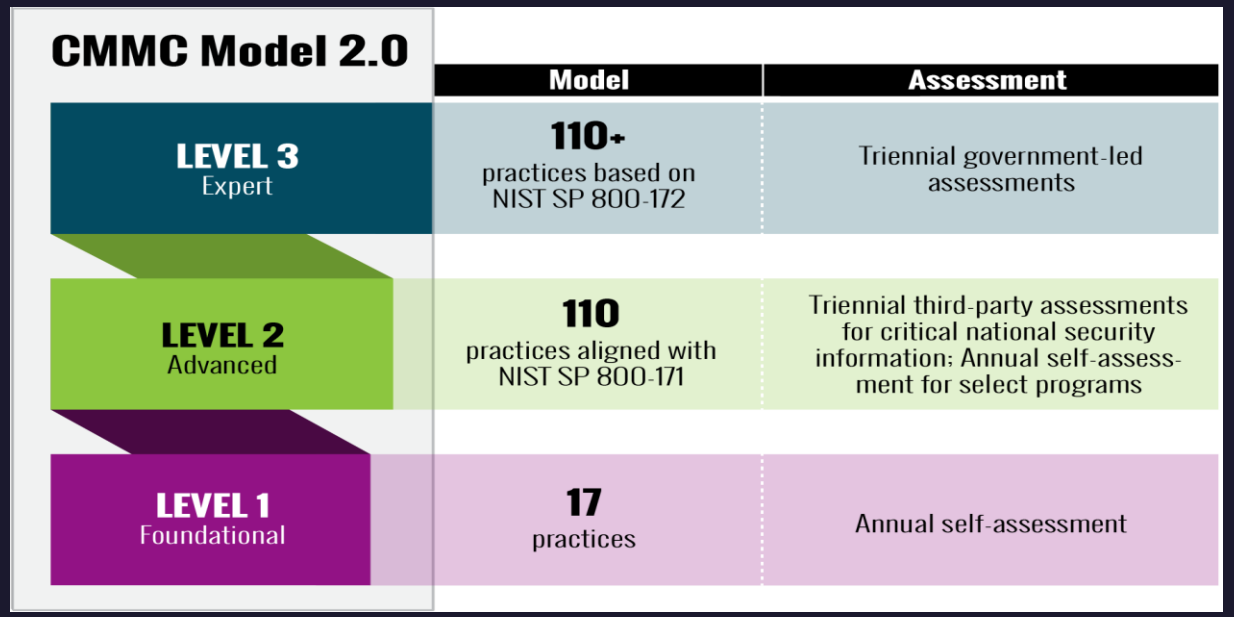
In **September 2020**, the DoD published an interim rule to the DFARS in the Federal Register (DFARS Case 2019-D041), which implemented the DoD's initial vision for the CMMC program ("CMMC 1.0") and outlined the basic features of the framework (tiered model, required assessments, and implementation through contracts). The interim rule became effective on **November 30, 2020**, establishing a five-year phase-in period.

In **March 2021**, the Department initiated an internal review of CMMC's implementation, informed by more than 850 public comments in response to the interim DFARS rule. This comprehensive, programmatic assessment engaged cybersecurity and acquisition leaders within DoD to refine policy and program implementation.

In **November 2021**, the Department announced "CMMC 2.0," an updated program structure and requirements designed to achieve the primary goals of the internal review:

- Safeguard sensitive information to enable and protect the warfighter
- Enforce DIB cybersecurity standards to meet evolving threats
- Ensure accountability while minimizing barriers to compliance with DoD requirements
- Perpetuate a collaborative culture of cybersecurity and cyber resilience
- Maintain public trust through high professional and ethical standards

CMMC 2.0 MATURITY LEVELS



The CMMC Framework requires a systematic approach to certification mapped to three organizational maturity levels: Foundational, Advanced, and Expert.

Level 1 - Foundational

An organization must demonstrate basic cyber hygiene practices, such as ensuring employees change passwords regularly to protect Federal Contract Information (FCI). FCI is "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government."

Level 2 - Advanced

An organization must have an institutionalized management plan to implement good cyber hygiene practices to safeguard CUI, including all the NIST 800-171 r2 security requirements and processes

Level 3 - Expert

An organization must have standardized and optimized processes in place and additional enhanced practices that detect and respond to changing tactics, techniques and procedures (TTPs) of advanced persistent threats (APTs). An APT is as an adversary that possesses sophisticated levels of cyber expertise and significant resources to conduct attacks from multiple vectors. Capabilities include having resources to monitor, scan, and process data forensics.

ATS
Advanced Technical Solutions

CMMC 2.0

- ❑ CMMC Timeline
- ❑ CUI & Current Contract Requirements
- ❑ Crawl-Walk-Run Approach
- ❑ How to get started with CMMC

CMMC Timeline

September 2007 — The Defense Industrial Base (DIB) Cybersecurity Task Force was established.

August 2015 — The DoD issued the DFARS clause 252.204-7012 Safeguarding Covered Defense Information & Cybersecurity Incident Reporting clause

December 2016 — NIST Special Publication 800-171 R1 is released.

December 2017 — Deadline for contractors to implement DFARS clause 252.204-7012.

March 2019 — **CMMC development begins.**

September 2020 — The DoD published an interim rule to the DFARS in the Federal Register (DFARS Case 2019-D041), which implemented the DoD's initial vision for the CMMC program ("CMMC 1.0") and outlined the basic features of the framework.

November 2020 — The interim rule became effective, establishing a five-year phase-in period.

March 2021 — The DoD initiated an internal review of CMMC's implementation, informed by more than 850 public comments in response to the interim DFARS rule. This comprehensive, programmatic assessment engaged cybersecurity and acquisition leaders within DoD to refine policy and program implementation.

November 2021 — The DoD announced "CMMC 2.0", an updated program structure and requirements designed to achieve the primary goals of the internal review.

2021 - 2025 — **Five-Year Phase-in Period**

You'll see a gradual increase of contracts requiring a CMMC certification leading up to 2025 and 2026 will be the deadline.

CUI & Current Contract Requirements

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified.

DFARS 252.204-7012

You should already be familiar with DFARS clause 252.204-7012. It has been in federal contracts for about 5 years now and has the following requirements:

- Applicable when the CUI is involved.
- Requires compliance with NIST 800-171.
- Must report cybersecurity incidents within 72 hours.
- Must cooperate with DoD investigations.

CUI & Current Contract Requirements

NOT JUST FOR THE DEPARTMENT OF DEFENSE (DOD)

FAR 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems:

Another clause already in contracts is FAR clause 52.204-21. All civilian contractors and subcontractors with access to non-public information must comply with the 15 basic controls outlined in the clause:

1. Limit information system access to authorized users
2. Limit information system access to transactions and functions that authorized users are permitted to execute.
3. Verify and control/limit connections to and use of external information systems.
4. Control information posted or processed on publicly accessible information systems.
5. Identify information system users, processes acting on behalf of users, or devices.
6. Authenticate the identities of users.
7. Sanitize or destroy information
8. Limit physical access to authorized individuals.
9. Escort visitors and monitor visitor.
10. Monitor, control, and protect organizational communications.
11. Implement subnetworks, separated from internal networks.
12. Identify, report, and correct information in a timely manner.
13. Provide protection from malicious code.
14. Update malicious code protection mechanisms when new releases are available.
15. Perform periodic scans of the information systems and real-time scans of files from external sources.

FAR clause 52.204-21 is considered a best-practice even if you do not have government contracts.

Crawl-Walk-Run Approach

- DFARS rules follow a "crawl, walk, run" approach, giving the DoD greater assurance in the security posture of its supply chain while the CMMC is phased in.
  - "Crawl": DFARS 252.204-7019 - Basic Self-Assessment
  - "Walk": DFARS 252.204-7020 - Medium/High Assessment
  - "Run": DFARS 252.204-7021 - CMMC Certification

Crawl

CRAWL (IN-EFFECT)

Winter of 2020 CMMC becomes a legal requirement.

- Self-Assessments
- DFARS 252.204-7019
- Must have current NIST 800-171 assessment on record within Supplier Performance Risk Systems (SPRS) to be considered for an award.

Walk

WALK (CLAUSE IN CONTRACTS)

The rollout of CMMC initiated January 2021 and the delivery will escalate each year until done. This requires a contractor to provide the government with access to its facilities, systems, and personnel when it is necessary for DoD to conduct or renew a higher-level assessment.

- Right to be Assessed
- DFARS 252.204-7020
- Must provide access to systems for advanced assessments

Run

RUN (DEADLINE)

CMMC is planned to be a requirement for all doing business with the US Defense Industry by the end of 2025. CMMC is required for all solicitations and contracts, task orders or delivery orders.

- Everyone will be Assessed
- DFARS 252.204-7021
- Must maintain the requisite CMMC Level for the duration of the contract.

How to get started with CMMC

If you're ready to embark on the journey towards CMMC certification but unsure of where to begin, the following steps will help you to get started:

- ❑ Register with Cyber AB: The first and essential step is to register with Cyber AB. By becoming a member, you gain access to valuable resources and support throughout the certification process.
- ❑ Work with an RPO: Once registered, you can collaborate with a Registered Provider Organization (RPO) available through Cyber AB. An RPO will assess your organization's current security posture, identify any gaps in your security program, and guide you towards meeting the CMMC requirements. They offer readiness and gap assessments, implementation guidance, and ongoing support.
- ❑ Conduct Assessments and Track Progress: Cyber AB provides an assessment platform where an RPO can simulate an assessment to evaluate your organization's readiness and track your remediation efforts. This platform enables you, along with your affiliated RPO, to systematically address any identified gaps, ensuring you are on track to meet the CMMC certification requirements.
- ❑ Achieve Certification with a C3PAO: Once you have made significant progress in addressing the gaps and implementing the necessary security controls, it's time to pursue CMMC certification. Collaborate with a CMMC Third-Party Assessment Organization (C3PAO) to conduct the official certification assessment and receive your CMMC certification.

ATS
Advanced Technical Solutions

Risks

- Cost of Noncompliance
- The False Claims Act (FCA)
- Loss of Revenue

Cost of Noncompliance

- CMMC 2.0 is a crucial security standard that DoD contractors must adhere to when bidding on DoD contracts.
- CMMC 2.0 requires independent third-party assessments for prioritized acquisitions involving CUI at Level 2.
- Organizations not complying with CMMC 2.0 may face fines of $10,000 per control under the **False Claims Act**. There are 110 controls in NIST 800-171.
- Compliance is critical to preventing new and emerging cyber threats to the security of critical systems and information, and failure to comply can lead to severe consequences.

The False Claims Act (FCA)

- The FCA provides that any person who knowingly submits, or causes to submit, false claims to the government is liable for three times the government's damages plus a penalty that is linked to inflation.
- In addition to allowing the United States to pursue perpetrators of fraud on its own, the FCA allows private citizens to file suits on behalf of the government (called "qui tam" suits) against those who have defrauded the government.
- Private citizens who successfully bring qui tam actions may receive a portion of the government's recovery. Many Fraud Section investigations and lawsuits arise from such qui tam actions.

Loss of Revenue

- Losing a contract or not being able to bid on new contracts due to not being compliant can result in significant revenue loss.
- Cyber attacks can cripple a business that is not protected:

Malware

Malware is also known as malicious code or malicious software. Malware is a program inserted into a system to compromise the confidentiality, integrity, or availability of data. It is done secretly and can affect your data, applications, or operating system.

Ransomware

Ransomware prevents or limits users from accessing their system via malware. Ransomware asks you to pay a ransom using online payment methods to regain access to your system or data.

Spam & Phishing

Spam includes unwanted, unsolicited, or undesirable messages and emails. Phishing is a form of social engineering, including attempts to get sensitive information. Phishing attempts will appear to be from a trustworthy person or business.

ATS
Advanced Technical Solutions

Cost and Funding Opportunities

- ❑ Consulting, Software and Hardware Costs
- ❑ Government Grants
- ❑ Recovering Cybersecurity Costs

Consulting, Software and Hardware Costs

CONSULTING

- There will be cost involved with working with Cybersecurity Consultants, RPO's, C3PAO's, and Lawyers.

CLOUD SERVICES

- CMMC Cloud services provide a controlled cloud environment for CUI to help reduce scope of the auditable environment.

  Popular vendors: Microsoft Azure, Amazon Web Services (AWS), and Egnyte

- Contractors holding or CUI or subject to ITAR must employ a secure way to send and receive information. Email is a popular way to transmit information and

  Popular vendors: Microsoft GCC High, Preveil Email, and Cerberus SFTP

SOFTWARE AND HARDWARE

- You will need to purchase Cybersecurity software for things like Mutli-Factor-Authentication (MFA), Event Log Monitoring (SIEM), Encrypted Email, and Security Awareness Training.

- You will need to replace outdated software, operating systems, and anything else that is end-of-life and no longer receives security updates.

- Outdated and end-of-life hardware will also need to be replaced.

Government Grants

NEXTCORPS.ORG

- There are organizations out there that help businesses obtain grants and funding for cybersecurity.
- If you're a manufacturer in the Finger lakes Region of New York State, our partner NextCorps might be able to get you access to funding opportunities that can take 10-60% off your costs.

Recovering Cybersecurity Costs

CONTRACTS

- ❑ Companies often spend thousands of dollars on internal/external resources and software in the process of achieving and maintaining compliance. Spreading costs across contracts by raising pricing can help recover some of your Cybersecurity costs.

CYBER LIABILITY INSURANCE

- ❑ Cyber liability insurance is a policy taken out by an organization to cover expenses following a Cybersecurity Incident.
- ❑ Like any insurance policy, it's important to read the fine print to make sure you understand exactly what is covered. Watch out for the following:
  - Many cyber liability insurance policies consider a state-sponsored cyberattack to be an act of war and refuse to pay claims for these attacks.
  - Many insurance companies offer cyber liability insurance as part of generalized business insurance. Chances are that this add-on coverage will not offer you the protection you need if a breach occurs.
  - You will be better off purchasing a stand-alone cyber risk insurance policy rather than relying on add-ons to your existing business policies.
  - Keep an eye out for loopholes that will allow them to wiggle out of paying a claim.

Summary

- Do not assume time is on your side. If you have not started with CMMC yet you are already behind.
- It can take 12 to 18 months to be complaint with the 110 Controls of NIST 800-171.
- Once compliant, you should be following your security policies for 4 to 6 months before you schedule a Certification Assessment with a C3PAO.
- You should start to budget the costs.

CMMC Acronym Cheat Sheet

Acronym	Definition
CMMC	The **Cybersecurity Maturity Model Certification** covers three maturity levels ranging from "Basic Cybersecurity Hygiene" to "Advanced/Progressive." In time, you will need to demonstrate CMMC compliance to do business – as a prime or subcontractor – with the U.S. Department of Defense.
CMMC-AB	The **CMMC Accreditation Body** oversees a community of qualified, trained, and trustworthy assessors who can assess your performance against the controls and best practices outlined in CMMC.
CUI	**Controlled Unclassified Information** is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.
DIB	The **Defense Industrial Base** is the collection of organizations that support the mission of the Department of Defense. DIB includes some of the nation's largest aerospace and defense corporations, as well as thousands of smaller businesses that contribute to the successful execution of DOD missions.
EDR	**Endpoint Detection and Response**, also known as endpoint threat detection and response (ETDR), is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.
FCI	**Federal Contract Information** means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.
FedRAMP	The **Federal Risk and Authorization Management Program** provides a standardized approach to security authorizations for Cloud Service Offerings. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
FIPS	**Federal Information Processing Standards** is a set of standards that describe document processing, encryption algorithms and other information technology processes for use within non-military federal government agencies and by government contractors and vendors who work with these agencies.
POAM	As part of any NIST 800-171/CMMC assessment, you should create **Plans of Action & Milestones** to map out next steps for remediation.
SIEM	A **Security Incident & Event Management system** combines Security Event Management (SEM), which analyzes event and log data in real-time to provide event correlation, threat monitoring, and incident response, with Security Information Management (SIM), which gathers and analyzes log data and generates a report.
SPRS	**Supply Performance Risk System** is DOD's single, authorized application to retrieve information about a supplier's performance. This web-enabled enterprise application gathers, processes, and displays data about supplier performance – including compliance with NIST 800-171.
SSP	A **System Security Plan** is a "living" document that articulates an organization's security policies and posture.

CMMC Acronym Cheat Sheet

Acronym	Definition
OSC	**Organization Seeking Certification** within the DIB seeking CMMC certification for Maturity Levels 1-3.
RPO	**Registered Provider Organizations** that provide advice, consulting, and recommendations to OSCs but do not conduct certified assessments. CMMC-AB authorizes RPOs to represent the organization as familiar with the basic constructs of the CMMC standard. They have agreed to the CMMC-AB Code of Professional Conduct.
RP	**Registered Practitioners** are authorized by CMMC-AB to provide non-certified advisory services, informed by basic training on the CMMC standard. RPs do not conduct certified CMMC assessments. RP's must be associated with an RPO.
C3PAO	**CMMC Third-Party Assessor Organizations** are authorized by the CMMC-AB to manage the Organizations Seeking Certification (OSCs) assessment process. Defense contractors and subcontractors may only obtain certification through a C3PAO.
GCC High	Microsoft maintains several clouds, including Microsoft Office 365 (Commercial) and **Office 365 GCC (Government Community)**. Additionally, Microsoft created a cloud specifically for DOD, with authorization for impact Level 3 in Azure Government.
MFA	**Multi-factor Authentication** is a security feature offered by many websites, applications and devices that dramatically improves account security. Sometimes MFA is also referred to as Two-Factor Authentication or 2FA. Technically, MFA could refer to a system where there are more than two forms of authentication.
NIST 800-171	The **National Institute of Standards and Technology** promotes and maintains measurement standards and guidelines to help protect federal agencies' information and IT systems. NIST 800-171, Protecting Controlled Unclassified Information In Nonfederal Information Systems and Organizations, was first published in June 2015 but has since been updated in response to evolving cyberthreats. It offers guidelines on how to securely access, transmit, and store CUI in nonfederal information systems and organizations.
FAR	The **Federal Acquisition Regulation** is the primary regulation for use by all executive agencies to acquire supplies and services with appropriated funds. FAR is jointly issued by The Department of Defense (DoD), the U.S. General Services Administration (GSA), and the National Aeronautics and Space Administration (NASA).
DFARS	**Defense Federal Acquisition Regulation Supplement** (DFARS) is a set of cybersecurity regulations administered by the Department of Defense (DoD) for external contractors and suppliers. The DFARS implements and supplements the FAR and provides detailed information about applying the regulation for DoD contractors, minimum requirements, and options to meet compliance standards.
ATS	**Advanced Technical Solutions (ATS)** is a leading Information Technology (IT) and Information Systems (IS) service provider headquartered in Rochester, NY, serving small, medium, and large organizations across New York State for more than 18 years. ATS is a Registered Provider Organization (RPO) with the CMMC Accreditation Body (CMMC AB).

ATS
Advanced Technical Solutions

THE CYBER AB
CMMC CERTIFICATION

Thank You

Advanced Technical Solutions (ATS)

- Registered Practitioner Organization (RPO)
- sales@atscgc.com
- 585.475.0605
- atsconsultingcorp.com

Dan Garrett

- Owner of ATS
- dgarrett@atscgc.com
- 585.738.1062

Topher Robinson

- Sr. Network Engineer / Registered Practitioner (RP)
- trobinson@atscgc.com
- 585.475.0605 x106

Richard Nardone

- Sr. Network Engineer / Registered Practitioner (RP)
- rnardone@atscgc.com
- 585.475.0605 x115

Downloads

CMMC Presentation - PDF

https://www.atsconsultingcorp.com/files/CMMC_Compliance_Presentation-Photonics-NY.pdf

CMMC Acronym Cheat Sheet – PDF

https://www.atsconsultingcorp.com/files/CMMC-Acronym-Cheat-Sheet.pdf