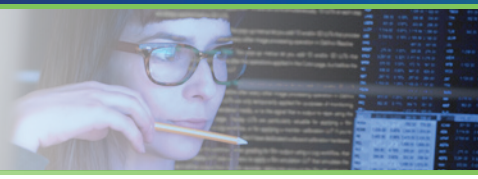
CMMC Readiness Assessment

The expertise you need to prepare for CMMC compliance.



- Get ready for CMMC 2.0 compliance quickly with the leader in DoD standards
- Assure your government customers that their information is safe with you
- Keep from losing vital defense contracts
- Establish and maintain a CUI-specific risk management and compliance program

Organizations that store, process, or transmit DoD federal contract information (FCI) or controlled unclassified information (CUI) are required to comply with the Cybersecurity Maturity Model Certification (CMMC), the new DoD standard for handling FCI and CUI in non-government systems. Only organizations that have achieved the DoD-specified CMMC level designated in defense contracts will be considered for the contract award.

If you are among the 300,000 or more organizations who are seeking CMMC compliance, Telos® Corporation can help. We're the leading experts in managing risk and ensuring security compliance for federal IT systems and information with more than three decades of experience in the DoD sector.

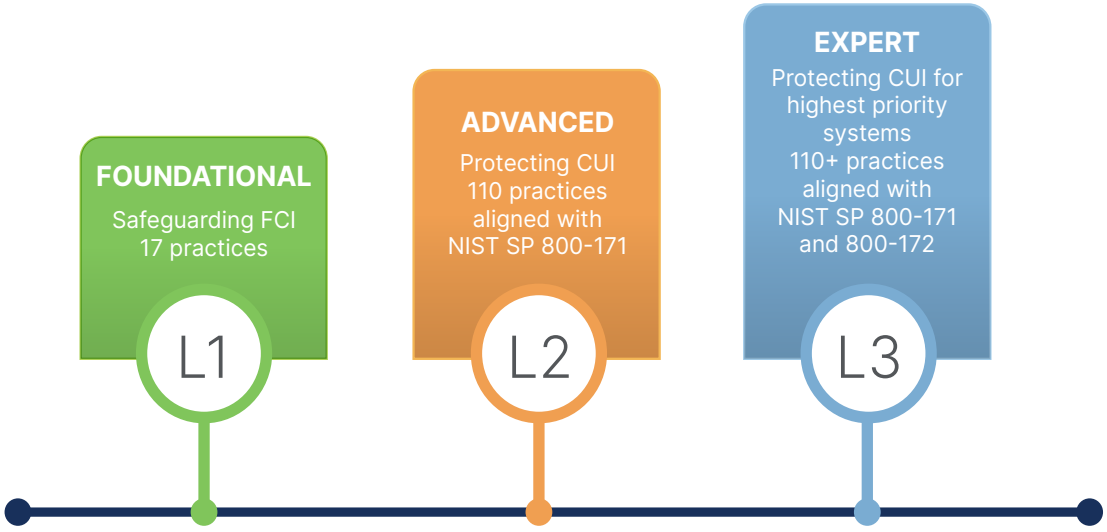
Telos has The Cyber AB registered practitioners on staff to provide consulting services to government contractors and other companies in preparation for their CMMC asssess-ments. We'll help you identify the federal information you hold that might qualify as CUI, show you what you need to do to follow and enforce the requirements and practices speci-fied in the CMMC model, and help you prepare for a CMMC assessment by a certified third-party assessor.

Take the first step toward CMMC with Telos.

The first step is being able to show that you're putting a compliance plan in place. Then you need to demonstrate that you're staying compliant over the long term. There's a lot involved — but no matter where you are on your CMMC journey, Telos can help you create and maintain a program that safeguards the federal information in your care.

Three CMMC levels and up to 110 or more practices. Are you ready?

CMMC has combined multiple security standards and best practices into three distinct maturity levels that range from foundational (17 requirements) to expert (100+ requirements). We'll help you take control of the challenge by helping you identify your required CMMC level and then guiding you to meet the applicable requirements and practices.



Telos offers the experience and capabilities you need for CMMC compliance. Using our proven methodologies and CMMC Registered Practitioner (RP) security personnel, Telos can provide the level of support necessary to exceed your requirements, resulting in exceptional results. Our professionals will:

Scope the situation. First, Telos will help you identify any federal information in your custody that falls into one of the National Archive's 20 index groupings of CUI. Then we'll assess the people, processes, and technologies in your organization that store, process, or transmit CUI or provide security and administration to the CUI in your care.

Identify the CMMC level and security controls you need. Each CMMC level has an assigned set of requirements that must be fully implemented in order to achieve the corresponding level. Telos will identify the controls you need to comply with, supplemented by best-practice configuration requirements for the hardware, software, and networks involved. We'll document the security safeguards you have in place, mapping each mechanism for securing and protecting the CUI to the relevant security controls.

Review and define your security architecture. We'll evaluate the current architecture of your CUI-related systems and recommend any modifications needed to meet the requirements of CMMC.

Assess your compliance with security controls. We start by assessing your current state of compliance with the identified security controls. We then plan and conduct a self-assessment, which will include compliance and vulnerability testing of technical controls and evaluation of security policies, procedures, and administrative controls through interviews, reviews, and inspections.

Address anything that needs remediation. After identifying any vulnerabilities or areas of non-compliance, we'll identify strategies and solutions that will assist in achieving the required level of compliance and maturity and work with the organization to customize the strategies to the organization's unique needs.

Plan for continuous compliance. Organizations will be required to either complete an annual self assessment or a triennial 3rd party assessment. We will assist you in creating a continuous monitoring strategy that will support continuous compliance in the years to come.

About Telos Corporation

Telos Corporation delivers solutions that empower and protect the world's most security-conscious enterprises. Whether we're investigating vulnerabilities, testing your security against external and internal threats, or engineering a hardened IT environment, Telos delivers the capabilities you need for information security and assurance. Our Xacta® suite of enterprise cyber risk management and compliance automation solutions helps our customers meet the complex challenges of managing IT risk with continuous compliance monitoring, security assessment, and ongoing authorization.

For almost three decades, we've provided information security services that protect leaders in financial services, healthcare, technology and other industries, including members of the Fortune 500. We also serve government agencies and contractors who need to ensure that their systems meet federal cyber security standards. Our customers return to us year after year for the in-depth assessment they know they need to stay vigilant in the face of increasing and ongoing threats.

Our cleared and credentialed security experts offer the skills, capabilities, and background to assist you with meeting the terms of CMMC.

Contact us for more information.

Call: 800-708-3567

Email: info@telos.com