InterSec
Ignite . Inspire. Innovate

CONTROLLED UNCLASSIFIED INFORMATION

WHITE PAPER

Federal agencies and their external service providers routinely generate, use, store, and share information that, while not meeting the standards for classified national security information nevertheless requires safeguarding and dissemination controls.

This whitepaper will discuss Controlled Unclassified Information (CUI) and how to protect it best. We will be covering:

1. US Government's document handling restrictions and control mechanism to safeguard protected unclassified information.

2. Guidance on identifying, using, storing, and sharing CUI.

WHAT IS CUI?

Controlled Unclassified Information (CUI) is a marking and control mechanism for all unclassified information or other data that meets standards for usage, safeguarding, and dissemination controls according to and consistent with applicable laws, regulations, and government-wide policies.

Types of data that fall under CUI includes, but is not limited to:

- Anything labeled "For Official Use Only" (FOUO)
- Anything labeled "Sensitive But Unclassified" (SBU)
- All information contained in the Department of Defense technical documents and related materials
- Anything referred to as "Limited Official Use"
- Anything defined as "Sensitive Information" by the Computer Security Act of 1987
- Any proprietary business information (PROPIN)

Important points:

- CUI refers to unclassified information that must be protected from public disclosure.
- CUI is not classification and should not be referred to as "classified as CUI." A better way to phrase it is "designated as CUI."

WHY IS THE CUI PROGRAM NECESSARY?

Before the CUI Program, there were over 100 different ways of characterizing unclassified information. Different rules for each Federal Agency created conflict on when and how to share information, making it difficult to collaborate and ensure the information was protected.

Established in Executive Order 13556, the CUI Program standardizes how the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies.

Important points:

- The CUI Program makes no changes to the Freedom of Information Act (FOIA) process.
- Standardized CUI markings help ensure that CUI is adequately protected by all agencies and facilitate timely information sharing to authorized recipients.
- Even the release of unclassified information can be damaging. Unclassified information can be pieced together to provide an adversary with a better understanding of classified information.
- The CUI Program helps mitigate and reduce threats of compromise or loss of information.

IDENTIFYING CUI

Only information requiring protection based on law, Federal regulation, or government-wide policy can qualify as CUI.
Like classified information, CUI is marked with bold banners, i.e., Controlled or CUI, and may also include limited dissemination controls making it clear how the information should be shared or distributed as directed by the responsible agency.

In this whitepaper, we will cover the two types of CUI: CUI Basic and CUI Specified, and the specific protections required for each.

EXAMPLES: LIMITED DISSEMINATION CONTROLS	
No foreign dissemination	NOFORN
Fedaral Employees Only	FED ONLY
Fedaral Employees and Contractors Only	FEDCON
No dissemination to Contractors	NOCON
Dissemination List Controlled	DL ONLY
Authorized for release to certain nationals only	REL TO [■USA, LIST■]
Display Only	DISPLAY ONLY

CUI LIFECYCLE

CUI follows a lifecycle similar to all protected information. While the designation of certain types of information requiring safeguarding and dissemination may be new, the process should be very familiar to DIB partners.

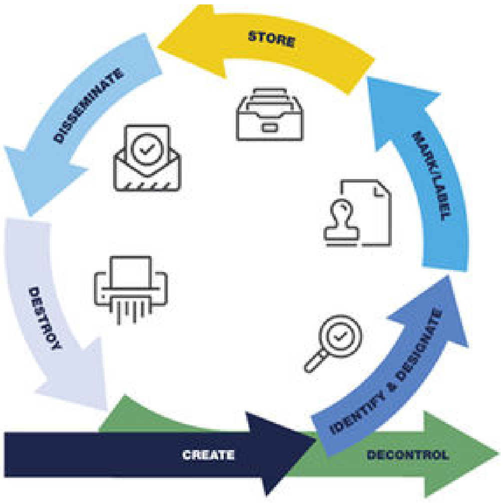
Create: CUI is created when recorded on paper or entered into an information system.

Identify & Designate: Realize that the information is generated for or on behalf of an agency within the Executive Branch under a contract and determine if the information falls into one of the more than one hundred categories of CUI in the National and DOD CUI Registries. It is also important to realize what is not CUI.

Mark/Label: At a minimum, CUI markings for unclassified DOD documents will include the acronym "CUI" or "CONTROLLED" in the banner of the document. It is a best practice to include markings in both the banner and footer of the document, and it is imperative to reference the CUI Marking Guide to ensure correct markings.

Store: CUI can be stored in NIST 800-171 compliant information systems or controlled physical environments.

Disseminate: Only authorized holders may disseminate in accordance with distribution statements, dissemination controls, and applicable laws.



CUI Lifecycle.

Image Source: DOD CUI Program

Destroy: Hard and soft copies of CUI should be appropriately destroyed, meaning they are rendered unreadable, indecipherable, and irrecoverable. Review clearing, purging, and destruction in NIST SP 800-88: Guidelines for Media Sanitization.

Decontrol: All holders must promptly decontrol CUI once the CUI owner has properly determined the information no longer requires safeguarding or dissemination controls, unless doing so conflicts with the related law, regulation, or government-wide policy in accordance with DoDI 5230.09.

WHO CAN VIEW CUI?

Access to CUI can be granted to individuals performing "any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes [as] within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement) on the need to know basis".

	U.S. Citizen	U.S. Person	Foreign National
Definition	Has citizenship in the United States through birth or naturalization.	A legal resident of the United States. Includes: U.S. Permanent Resident, U.S. Asylee/ Refugee	is not a legal citizen/ permanent resident of the United States; also referred to as a non - U.S. Person or Foreign Person
Verification	U.S. Birth Certificate Naturalization Certificate	Permanent Resident "green card"	Any type of employment visa
Access Rights	Can hold a national Security clearance Can view any type of CUI Can view CUI marked NOFORN with a valid need to know Can view international Traffic in Arms Regulations (ITAR) data	Cannot view classified information Cannot view CUI marked NOFORN Can view CUI not marked NOFORN Can view ITAR (International Traffic in Arms Regulations) data	Cannot view classified information Cannot view any type of CUI Cannot view ITAR data Can view non Defense and non-Federal data

Types of CUI

There are two types of CUI: CUI Basic and CUI Specified.

CUI BASIC

CUI Basic is the type of CUI that a law, regulation, or government-wide policy says must be protected, but doesn't provide any further instruction for its protection. CUI Basic contains basic handling and dissemination controls.

- CUI Basic has the same handling and sharing guidance across the entire Executive Branch and can be marked as either CUI or Controlled.
- The Federal Information Systems Modernization Act (FISMA) requires that CUI Basic be protected at the FISMA Moderate level.
- Examples of CUI Basic Categories

Agriculture	Comptroller General	Terrorist Screening
Ammonium Nitrate	Geodetic Product Information	Informant
Water Assessments	Asylee	Privilege
Emergency Management	Visas	Victim
Bank Secrecy and Budget	Information Systems Vulnerabilities	Death Records

CUI SPECIFIED

CUI Specified is the type of CUI where the authorizing law, regulation, or policy puts more restrictive controls on the specific handling, marking, or sharing requirements to ensure adequate protection.

- Individual directors of Federal Agencies define guidance.
- Each Federal Agency has its additional handling and storing requirement(s) and may apply limited dissemination controls to the CUI content.
- Each Federal Agency has its own rules for CUI Specified.
- Export-controlled (ITAR and EAR-controlled information) are types of CUI Specified.

Important points:

- Since CUI Specified can call for different controls and protection than CUI Basic, it is mandatory to label the specific protection of the content in the banner (SP-)
- Examples of CUI Specified Categories

Sensitive Security Information	Safeguards Information	DNA
Student Records	NATO Restricted	Criminal History Records
Sensitive Security Information	Safeguards Information	Financial Records
Personnel	NATO Unclassified	Export Control
Source Selection	Federal Grand Jury	Protected Critical Infrastructure Information
Nuclear	Witness Protection	Controlled Technical Information

OTHER CATEGORIES

Covered Defense Information (CDI) is unclassified Department of Defense information that might typically be labeled CUI in other government agencies. CDI can also include Controlled Technical Information (CTI).

COVERED DEFENSE INFORMATION (CDI)

CDI is unclassified information provided by or on behalf of the Department of Defense in connection with the performance of the contract, or unclassified information which is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

CONTROLLED TECHNICAL INFORMATION (CTI)

CTI is technical information with military or space applications that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Identifying CDI and CTI starts with Dissemination Statements, also known as Distribution Statements, that cover the content underneath.

The Distribution Statement is commonly found on the front page or top of the document, making it clear how the information should be shared or distributed. The underlying data itself may also be marked with bold banners at the top or bottom of each page or the beginning of a paragraph to alert the reader.

Depending on the sensitivity of the information, additional markings may also be in the body of the document.

EXAMPLES: DoD DISTRIBUTION STATEMENTS	
Distribution A: Public Release	Public Released
Distribution B: U.S. Govt Only	Export Control Warning Label
Distribution C: U.S. Govt & Contractors	Atomic Energy
Distribution D: DoD & US DoD Contractors	NOFORN
Distribution E: DoD only	RESTRICTED
Distribution F: Further dissemination only as directed by controlling office	Government Contractors Only
A Foreign Government Agreement Statement	FOUO

CUI MARKING GUIDANCE

CUI markings alert holders that the information must be protected. A cover sheet may also be used to identify CUI, alerting observers that CUI is present from a distance and serving as a shield to protect CUI from inadvertent disclosure. In the CUI program, there is a standard way to apply markings, as well as alternative methods to satisfy marking or identification requirements. Listed below are three components of marking CUI and an example of a CUI coversheet.

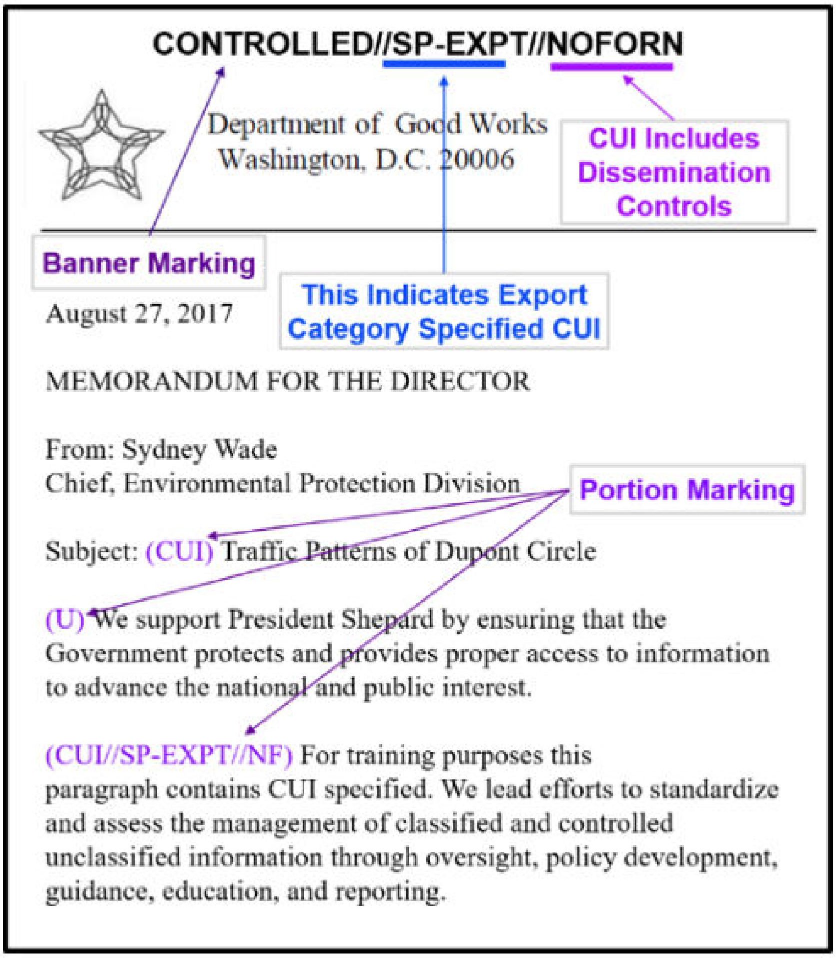
Designation Indicator

- A mandatory component for all CUI markings that identifies who originated the CUI.

Banner Markings

- For CUI Basic, it is mandatory to include the CUI Control banner marking “CUI” or “CONTROLLED”.
- For CUI Specified, the category marking must appear in the banner and must be preceded by “SP-”.
- Use the same banner marking on every page – the top banner must apply to the entire document.
- If possible, apply markings to the bottom of the document.
- If feasible, make the text black, bold, capital, and centered.

Example:



CONTROLLED//SP-EXPT//NOFORN

Department of Good Works
Washington, D.C. 20006

August 27, 2017

MEMORANDUM FOR THE DIRECTOR

From: Sydney Wade
Chief, Environmental Protection Division

Subject: (CUI) Traffic Patterns of Dupont Circle

(U) We support President Shepard by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

(CUI//SP-EXPT//NF) For training purposes this paragraph contains CUI specified. We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

CUI Includes Dissemination Controls
Banner Marking
This Indicates Export Category Specified CUI
Portion Marking

Portion Markings

- Check Agency requirements to determine whether portion markings are required.
- Place abbreviations, in parentheses, at the beginning of the portion to which they apply, and throughout the document.
- It may include up to three elements:
  - CUI Control Marking ("CUI")
  - CUI Category or Subcategory Markings (mandatory for CUI Specified)
  - Limited Dissemination Control Markings
- When a portion doesn't contain "CUI", put "(U)" to indicate that it contains unclassified information.

PROTECTION BARRIERS

CUI must always be secured using controlled environments, both physically and electronically, that ensure access to CUI is only by authorized users with a lawful government purpose.

PHYSICAL BARRIERS

The CUI Program requires that inside a controlled environment there is at least one physical barrier to prevent unauthorized access to CUI such as the following:

- Sealed envelopes
- Locked doors, overhead bins, drawers, file cabinets
- Area equipped with electronic locks

CUI safeguards must also prevent unauthorized individuals from observing or overhearing discussions containing CUI. Public areas such as break rooms, lobbies, or public transportation, are not acceptable for the storage, discussion, or review of CUI.

ELECTRONIC BARRIERS

The CUI program requires that some barrier or compartmentalization exists to prevent unauthorized users from accessing electronic CUI, such as the following:

- Dedicated network drives or SharePoint sites
- Protected file folders
- Intranet sites

Information stored on electronic systems and networks must be compartmentalized and protected according to the lawful government purpose for accessing that information. All projects should establish procedures to ensure that only authorized individuals have access to CUI, and its access is removed when it is no longer required.

ACCESS AND INFORMATION SYSTEMS CONTROLS

CDI or CUI data may only be processed (i.e., transmitted, accessed, or stored) on company-approved devices including company workstations, GFE, approved subcontractor workstations, or MDM or MAM-enrolled devices.

- To handle CUI, you must use Office 365 GCC High environment (aka "O365 Defense").
- If your client has CUI Specified or Certain Dissemination Controls that require certification at the FIPS High level, contact InterSec, Inc. for further guidance.

Access to CUI while on company business foreign travel must be permitted by your client and your contract and is subject to company device restrictions. Access to CUI while on personal foreign travel is not permitted.

	Permitted Systems and Devices by Information Type						
	Company Windows Workstation	Company MacOS Workstation	Government Furnished Equipment	Approved Company Subcontractor Workstations	MDM or MAM -enrolled Devices	Office 365 GCC High (aka O365 Defense)	Office 365 Commercial
Covered Defense Information (CDI)	X		X	X	X	X	
Controlled Unclassified Information (CUI)- Specified	X		X	X	X	X	
Controlled Unclassified Information (CUI) - Basic (Projects subject to DFARS)	X		X	X	X	X	
Controlled Unclassified Information (CUI) - Basic (Projects NOT subject to DFARS)	X	X	X	X	X	X	X

ACCESSING, SHARING, AND STORING CUI/CDI

CDI or CUI data may only be processed (i.e., transmitted, accessed, or stored) on approved devices including workstations, Government Furnished Equipment (GFE), approved subcontractor workstations, MDM or MAM-enrolled personnel devices; more specifically:

- Office 365 Commercial is limited to information that is suitable for public release and CUI Basic for non-DFARs projects and is built to the FIPS Moderate specifications. For guidance on FIPS requirements, reference NIST 800-171.
- Office 365 GCC High (aka O365 Defence) must be used for CDI, CUI Specified, and CUI Basic for DFARS projects.

DISPOSING CUI

Regardless of the type (i.e., physical or electronic), CUI must be destroyed until the information is rendered unreadable, indecipherable, and unrecoverable.

PHYSICAL DESTRUCTION

- Procedures for the physical destruction of CUI are different from those for unclassified information.
- For physical media, such as a document, use an approved cross-cut shredder or a secured destruction bin.
- Ensure that the shredder or destruction bin is marked "Approved for the destruction of Controlled Unclassified Information".
- Never use trash cans or recycling bins to dispose of CUI.

ELECTRONIC DESTRUCTION

- Follow proper roll-off procedures when leaving your project.
- Seek necessary technical guidance for electronic destruction of CUI, contact InterSec, Inc. for support on clearing, purging, and destroying.
- Projects can also reference guidance found in NIST SP 800-88 to ensure that their methods align with the standards of the CUI Program.

CUI is a complex topic and many companies struggle to determine if they have CUI in their environment to choose the appropriate level of CMMC compliance.

CUI scoping plays a significant part in the cost of CMMC compliance, whether you want only certain programs to be in scope for CMMC compliance or the entire company.

We offer a rapid and field test CUI scoping to help you determine the CMMC level compliance.

☎ Schedule a 30 min complimentary CUI Scoping call

How can an RPO like InterSec help in CMMC Compliance?

Achieving compliance with the Cybersecurity Maturity Model Certification (CMMC) can be challenging for DIB Contractors. However, by working with a Registered Provider Organization (RPO), contractors can gain access to the guidance, expertise, and resources necessary to successfully navigate the requirements and best practices for each maturity level.

RPOs can assist with the assessment process, provide training and resources, and offer feedback and recommendations for improvement. Partnering with an RPO can significantly increase a DIB Contractor's chances of quickly achieving and maintaining CMMC compliance.

InterSec, a Cyber-AB RPO, has years of experience helping Federal Contractors navigate complex compliance requirements. As a Cybersecurity organization, we provide end-to-end CMMC Compliance consulting.

We provide a compliance-accelerated platform and rapid CUI scoping to begin your CMMC compliance journey. We have expertise in technical remediation and provide audits for your company.

We are a dedicated team of professionals to help your company meet your CMMC needs through cost-effective solutions. Our bespoke solutions and services save your company valuable time, resources, and money in achieving CMMC compliance.

As a Cyber-AB authorized CMMC RPO, Intersec offers Consulting, Gap Assessment, Remediation, and Managed Security Services to ramp up and accelerate your CMMC Compliance Journey.

☎ **Schedule a 30 min complimentary CMMC Consultation**

✉ **Send an email for requesting free CMMC Consultation**

Case Study 1 : Unleashing cybersecurity success

How InterSec helps a manufacturing company meet CMMC requirements with ease.

Introduction	A Virginia-based manufacturing company was facing challenges in meeting the Cybersecurity Maturity Model Certification (CMMC) Level 2 requirements set forth by the Department of Defense. The company had limited IT resources and was hesitant about using cloud services.
Problem	The company was struggling to meet the CMMC requirements due to its limited IT resources, lack of dedicated IT staff, and use of outdated technology. Additionally, the company was cautious about using cloud services to store sensitive information.
Solution	InterSec was referred to the company to help them achieve CMMC compliance. InterSec engaged the company's executive management, educated the company's staff, and defined roles and responsibilities for information security. InterSec then utilized its NIST 800-171/CMMC field-tested readiness methodology to ensure a successful CMMC compliance milestone.
Methodology	• Controlled Unclassified Information (CUI) scoping • Gap analysis • A current state analysis of the client's organization security • Development of a remediation plan • Policies and procedures development • Technical remediation services, including asset management, multi-factor authentication, vulnerability scanning, email encryption, drive encryption, and virtual private network
Results	InterSec was able to quickly remediate and improve the company's security posture, resulting in an SPRS score of 110. The client subsequently requested our Managed Security Service Provider (MSSP) services to maintain CMMC compliance.
Conclusion	InterSec's well-defined methodology, streamlined project execution, and expertise made the project a success, helping the company achieve the CMMC requirements and secure its systems. The company can now continue serving the defense industry while minimizing potential security risks.

Case Study 2 : Accelerating CMMC compliance

A Virginia-based acquisition support contractor's success story with InterSec

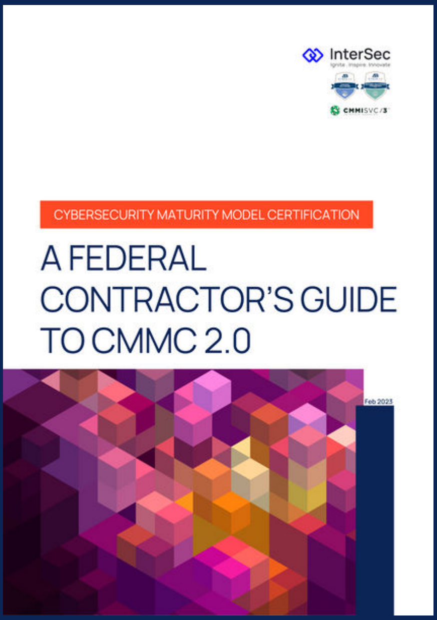
Introduction	A Virginia-based Acquisition Support contractor with 200+ employees was facing challenges in meeting the Cybersecurity Maturity Model Certification (CMMC) Level 2 requirements set forth by the Department of Defense. With two office locations and a recent acquisition of a small manufacturing company, the contractor needed to comply with a defense contract and improve the SPRS score to 110.
Problem	The contractor faced the complex task of integrating the acquired company employees into its existing systems, and employees were not on the parent company's Active Directory which made it harder to enforce CMMC policies and procedures.
Solution	InterSec came to the rescue with its innovative approach to CMMC compliance, leveraging its CMMC accelerators and field-tested NIST 800-171/CMMC methodology to assess the current state and develop a remediation plan. The plan was executed by creating policies, and procedures, supplement documents, and providing technical remediation services.
Methodology	InterSec brought a rigorous CMMI Services Level 3 mature service delivery process and ISO 9001 quality management to CMMC services, conducted an assessment, developed a remediation plan, implemented policies/procedures, provided technical remediation services, integrated the acquired company, prepared documentation, and executed the project using their NIST 800-171/CMMC field-tested readiness methodology, resulting in a successful outcome for the customer.
Results	The contractor's SPRS score improved to 110, the acquisition was seamlessly integrated into the parent company's systems, and all required documentation was uploaded into the SPRS system ahead of the deadline, meeting the customer's CMMC compliance requirements.
Conclusion	InterSec's innovative approach and experienced team helped the contractor achieve CMMC compliance and secure their systems, ensuring their ability to serve the defense industry while minimizing security risks. The well-defined methodology and field-tested approach to execution made the project a resounding success.

FREE CMMC GUIDE

The Cybersecurity Maturity Model Certification (CMMC) is a program implemented by the U.S. Department of Defense (DoD) to ensure that organizations handling controlled unclassified information (CUI) have appropriate cybersecurity controls in place to protect sensitive information from unauthorized access, use, or disclosure. If your organization handles CUI for the DoD, it is important to understand which CMMC level you need and begin the journey toward certification.

CMMC 2.0 introduces a tiered system of levels, ranging from Level 1 (Basic Cybersecurity Hygiene) to Level 3 (Advanced/Progressive).

We have developed a CMMC guide that covers important topics to provide a comprehensive understanding of CMMC 2.0 and the importance of achieving compliance.



CYBERSECURITY MATURITY MODEL CERTIFICATION

A FEDERAL CONTRACTOR'S GUIDE TO CMMC 2.0

LIST OF TOPICS FOR CMMC GUIDE

1. CMMC 2.0 Framework
2. Key Changes to CMMC 2.0
3. Why is CMMC compliance important?
4. Whom does CMMC apply to?
5. How long does it take to get CMMC certified?
6. When will CMMC requirements start appearing in solicitations?
7. What does the journey to CMMC certification look like?
8. What are the challenges faced by small businesses to comply with CMMC?
9. What is the difference between Basic, Medium, and High assessments
10. How much does CMMC Compliance Cost?

and much more...

CLICK HERE TO READ AND DOWNLOAD THE FREE CMMC GUIDE

FOR MORE INFORMATION

DOD CUI Program Website: https://www.dodcui.mil/

DOD CUI Registry: https://www.dodcui.mil/Home/DoD-CUI-Registry/

DOD Mandatory Controlled Unclassified Information Training (for DOD and Industry): https://securityawareness.usalearning.gov/cui/index.html

CMMC COMPLIANCE CONSULTING FOR DOD CONTRACTORS

WHY DO DIBS CHOOSE INTERSEC AS A CMMC COMPLIANCE PARTNER?

- ✓ InterSec brings a rigorous CMMI Services Level 3 mature service delivery process and ISO 9001 quality management to the CMMC services.
- ✓ InterSec is a CMMC-AB RPO with many seasoned RPs and assessors.
- ✓ A prime contractor on the Virginia GENEDGE CMMC services BPA, so you can count on us as a vetted CMMC compliance service provider.
- ✓ A dedicated team of security professionals is available to you throughout the CMMC compliance process.
- ✓ Strategic partnerships and alliances with product vendors to provide turnkey and cost-effective solutions to meet CMMC compliance.
- ✓ Multiple services and price models that can be easily customized to meet your organization's unique needs.

OUR APPROACH TO CMMC COMPLIANCE

At InterSec, we take CMMC compliance seriously, and we have developed an approach that ensures our clients are fully prepared for compliance. Our approach involves assessment, remediation, and ongoing monitoring to ensure guaranteed compliance:

ASSESS CMMC GAP ASSESSMENT	DEFEND REMEDIATION	SECURE ONGOING MONITORING
• SCOPING TO EVALUATE APPLICABLE CMMC LEVEL • IDENTIFY CUIS, FCIS • ESTABLISHING EXISTING CYBERSECURITY MATURITY • ASSESS COMPLIANCE • SPRS EVALUATION • POA&MS WITH ACTIONABLE REMEDIATION GUIDANCE	• DOCUMENTATION AND TECHNICAL REMEDIATION • ESTABLISHING EXISTING CYBERSECURITY MATURITY • ASSESS COMPLIANCE • SPRS SCORE • POA&M • SYSTEM SECURITY PLAN • ACTIONABLE REMEDIATION REPORT	• PERIODIC POLICIES AND PROCEDURES REVIEWS AND UPDATES • INCIDENT RESPONSE TABLE TOP EXERCISE • ANNUAL PHISHING EXERCISES • SECURITY AWARENESS TRAINING • PERIODIC VULNERABILITY SCAN • SPRS SCORE UPDATES

Rapid CUI scoping to right-size your CMMC compliance efforts

Discounted CMMC Level 2 Gap Assessment

Expertise in CMMC Technical Remediation

CMMC audit-ready artifacts for quick turnaround

CMMC Pre-audit to baseline the existing cybersecurity readiness

MSSP services for ongoing CMMC compliance

Hundreds of DFARS assessments and readiness experience

170+
NIST 800-171 SSP, POA&M, AND SPRS

200+
LEVEL 1 ADVISORY AND CONSULTING

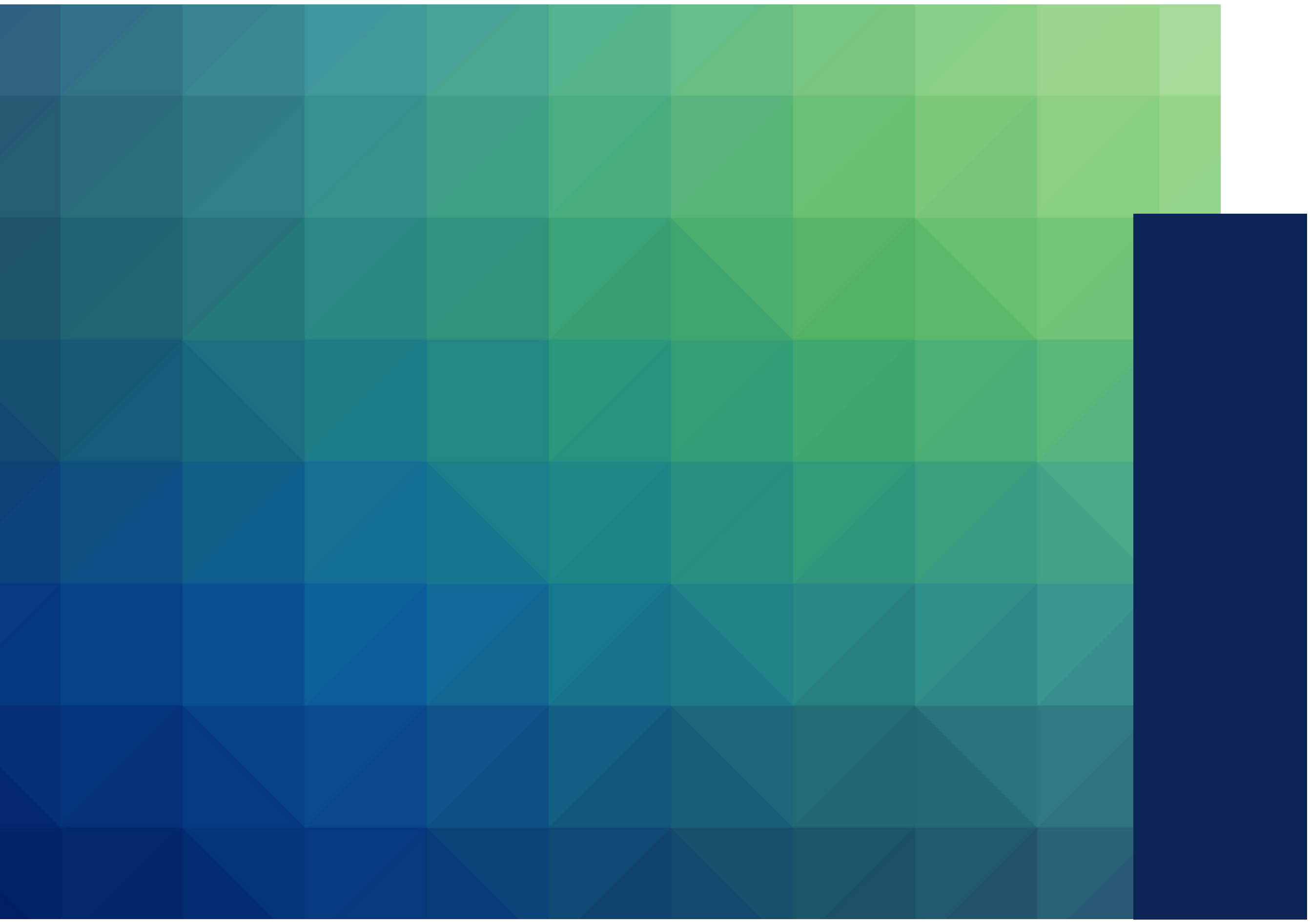
50+
LEVEL 2 ADVISORY, CONSULTING, AND MSSP

OUR CLIENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES, USA · UNITED STATES COURTS · Maryland INSURANCE ADMINISTRATION · FannieMae · ARRIKAI LLC "Experience Matters"

HRSA Health Resources & Services Administration · navitas Innovation • Delivery Excellence · WAVERLEY LABS · verizon · USDA United States Department of Agriculture Natural Resources Conservation Service

sprowt



InterSec
Ignite . Inspire. Innovate

Ready to start your CMMC Journey?

Please contact us at complianceservices@intersecinc.com
Call us at (833) 228-4858 (toll-free)

Website: www.intersecinc.com
NAICS Codes: 541511, 541512, 541519
GSA Multiple Award Schedule Contract: 47QTCA19D00EG
54151S – Information Technology (IT) Professional Services,
54151HACS – Highly Adaptive Cybersecurity Services (HACS), and OLM – Order Level Materials.