How to Comply with DFARS 252.204-7012 & NIST SP 800-171 Rev. 2

In the Interest of National Security

CROSS TIMBERS
Procurement Technical Assistance Center
Webinar Guidelines

All attendees are muted.

Use Chat box for questions.

Presentation available in Hand Out box or at http://www.uta.edu/crosstimbers/pages/Webinars/index.php

- This procurement technical assistance center is funded in part through a cooperative agreement with the Defense Logistics Agency.
The Procurement Technical Assistance Program was established to expand the number of business capable of participating in government contracts. The program is administered by DLA's Office of Small Business in cooperation with states, local governments and nonprofit organizations.

https://www.dla.mil/SmallBusiness/PTAP/ink to DLA’s PTAP program
Alerts

Effective **Dec 31, 2017**, all DoD contractors must comply with the requirements of the DFARS 252.204-7012.

Effective **November 30, 2020**, DoD implemented a phased rollout of CMMC- The Interim Rule. The interim rule established two new provisions and clauses to further address NIST SP 800–171 requirements.

- DFARS provision 252.204-7019 “Notice of NIST SP 800–171 DoD Assessment Requirements” will be inserted into solicitations
- DFARS clause 252.204–7020 “NIST SP 800–171 DoD Assessment Requirements” will be used in solicitations and awards.
Effective January 13, 2021, the DoD created the Trusted Capital Digital Marketplace (TCDM) - designed to promote innovation and ensure access to trusted sources of capital for emerging technologies and critical capabilities required for national security.

In November 2021, the Department announced “CMMC 2.0,” an updated CMMC program structure designed to achieve the primary goals to:

• Safeguard sensitive information to enable and protect the warfighter

• Dynamically enhance 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
Alerts

The oversight of CMMC 2.0 is now the DoD’s Office of the Chief Information Officer (DOD CIO), and not the CMMC Accreditation body (CMMC-AB)
Agenda

1. DFAR 252.204-7012 Compliance Steps
2. CMMC
   2.1 Cybersecurity Maturation Model Certification (CMMC)
   2.2 NIST SP 800-171: Control Families
   2.3 The Interim Rule
It’s the Law

Effective Dec 31, 2017 all DoD contractors must comply with the requirements of the DFARS 252.204-7012 and NIST 800-171. The Department of Justice will prosecute false claims.

The new DFARS provision 252.204-7019 advises contractors who are required to implement the NIST SP 800-171 standards have a current (not older than three years) NIST SP 800-171 DoD Assessment on record to be considered for the award. This results must be posted to the Supplier Risk Management System (SPRS, https://www.sprs.csd.disa.mil/) - DoD's authoritative source for supplier and product performance information.

The new DFARS clause 252.204-7020 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. The clause also requires the contractor to ensure that applicable subcontractors also have the results of a current Assessment posted in SPRS prior to awarding a subcontract or other contractual instruments.
It’s the Law

To comply with NIST SP 800-171, and the Interim Rule, a company must:

1) implement 110 security requirements on their covered contractor information systems; or

2) document in a “system security plan” and “plans of action” those requirements that are not yet implemented and when the requirements will be implemented.

3) complete a Basic Assessment and upload the resulting score (SPRS)- DoD's authoritative source for supplier and product performance information.

4) The Basic Assessment, valid for three years, is a self-assessment done by the contractor using a specific scoring methodology that tells the Department how many security requirements have not yet been implemented.
It’s the Law

• A company that has fully implemented all 110 NIST SP 800-171 security requirements, would have a score of 110 to report in SPRS for their Basic Assessment.
• A company that has unimplemented requirements will use the scoring methodology to determine their score. It is possible to have a negative score.
• After a contract is awarded, DoD may choose to conduct a Medium or High Assessment of an offer based on the criticality of the program.
• Under both Assessments, DoD assessors will review the contractor's system security plan, or description of how each NIST SP 800-171 requirement is met, and will identify any descriptions that may not properly address the security requirements.
• The contractor provides DoD access to its facilities and personnel, if necessary, and prepares for/participates in the assessment conducted by the DoD.
• Under a High Assessment a contractor will be asked to demonstrate their system security plan.
Types of Unclassified Information

All types of Unclassified Information are covered under DFARS 252.204-7012, NIST 800-171 and CMMC.

Federal Contract Information (FCI): FCI is information provided by or generated for the Government under contract not intended for public release.

https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

Controlled Unclassified Information (CUI): CUI is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

https://www.archives.gov/cui  https://youtu.be/egbAZ1f5r8g

Controlled Technical Information (CTI): CTI means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

Types of Unclassified Information

**Export Controlled Information:** Unclassified information concerning certain items, commodities technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and the munitions list; license applications; and sensitive nuclear technology information.


**Who controls exports?:** There are two government agencies that control exports:
The United States Department of Commerce through its Export Administration Regulations (EAR), Title 15, sections 730-774 of the Code of Federal Regulations. For a list of controlled technologies, see 15 CFR 774, Supplement I.
The United States Department of State (which controls the export of “defense articles and defense services”) under the International Traffic in Arms Regulations (ITAR), 22 CFR 120-130. [http://www.access.gpo.gov/bis/ear/ear_data.html](http://www.access.gpo.gov/bis/ear/ear_data.html) (EAR)
1. DFAR 252.204-7012 Compliance Steps

https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012

1.1 NIST SP 800-171 Self Assessment

1.2 Plan of Action and Milestones (POAMS)

1.3 System Security Plan

1.4 Incident Response Plan and Reporting

1.5 Subcontractor Flow Down Requirements

NOTE: SAVE DOCUMENTS FOR CMMC AUDITORS
1. DFAR 252.204-7012 Compliance

1.1 NIST SP 800-171 Self-Assessment

Address 110 standards (questions) self-assessment located in the NIST Handbook. See link below.

Develop plan and budget to fix the weaknesses. Qualified third-party providers are available. Selection criteria is discussed later.


*This handbook contains the standards with the descriptions.*
1. DFAR 252.204-7012 Compliance Steps

1.2 Plan of Action and Milestones (POAMS) Template

Weaknesses

Responsible Office/ Organization

Resource Estimate (funded/ unfunded/ reallocation)

Scheduled Completion Date

Milestones with Interim Completion Dates

Changes to Milestones

How was the weakness identified?

Status (Ongoing or Complete)
DFARS 252.204–7012
Compliance Steps

1.2 Plan of Action and Milestones (POAMS) Template

<table>
<thead>
<tr>
<th>POAM ID</th>
<th>Creation Date</th>
<th>Weakness Name</th>
<th>Weakness Description</th>
<th>Severity Level (Low, Moderate, High)</th>
<th>Point of Contact</th>
<th>Scheduled Completion Date</th>
<th>Milestones</th>
<th>Changes to Milestones</th>
<th>Source of Weakness</th>
<th>Actual Completion Date</th>
<th>Comments</th>
</tr>
</thead>
</table>

https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012
## 1. DFAR 252.204-7012 Compliance Steps

### 1.3 System Security Plan (SSP) Template

<table>
<thead>
<tr>
<th>Section</th>
<th>Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 Access Control</td>
<td>22</td>
</tr>
<tr>
<td>3.2 Awareness and Training</td>
<td>3</td>
</tr>
<tr>
<td>3.3 Audit and Accountability</td>
<td>9</td>
</tr>
<tr>
<td>3.4 Configuration Management</td>
<td>9</td>
</tr>
<tr>
<td>3.5 Identification and Authentication</td>
<td>11</td>
</tr>
<tr>
<td>3.6 Incident Response</td>
<td>3</td>
</tr>
<tr>
<td>3.7 Maintenance</td>
<td>6</td>
</tr>
<tr>
<td>3.8 Media Protection</td>
<td>9</td>
</tr>
<tr>
<td>3.9 Personnel Security</td>
<td>2</td>
</tr>
<tr>
<td>3.10 Physical Protection</td>
<td>6</td>
</tr>
<tr>
<td>3.11 Risk Assessment</td>
<td>3</td>
</tr>
<tr>
<td>3.12 Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>3.13 System and Communications Protection</td>
<td>16</td>
</tr>
<tr>
<td>3.14 System and Information Integrity</td>
<td>7</td>
</tr>
</tbody>
</table>

1. DFAR 252.204-7012 Compliance Steps

1.4 Incident Response Plan and Reporting

A “Cyber incident” is an action(s) taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

“Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

Submit Incident to DoD DIB portal:

https://dibnet.dod.mil/portal/intranet/
1. DFAR 252.204-7012 Compliance Steps

1.4 Incident Response Plan and Reporting

The incident response plan should include the following elements:

Mission.

Strategies and goals.

Senior management approval.

Organizational approach to incident response.

How the incident response team will communicate with the rest of the organization and with other organizations.

Metrics for measuring the incident response capability and its effectiveness.

Roadmap for maturing the incident response capability.

How the program fits into the overall organization.

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
1. DFAR 252.204-7012 Compliance Steps

1.5 Subcontractor Flow Down Requirements

Subcontracts. The Contractor shall—

(1) Insert the substance of this clause, including this paragraph (c), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items, excluding commercially available off-the-shelf items; and

(2) Prior to awarding to a subcontractor, ensure that the subcontractor has a current (i.e., not older than 3 years) CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.

Selection Criteria for Third Party Providers (TPP’s)

Third Party Providers (TPP’S) MUST meet CURRENT DFARS 252.204-7012 requirements if they receive, store, and transmit CUI data under DFARS 252.204-7012(m).

Those TPP's that only provide services such as "maintenance", "consulting services", etc. and only require "access", but do not require receiving, transmitting, or storing FCI/CUI from an OSC's environment, could then be included as any other "1099 subcontractor" with remote or direct system access.

TPP’s should have a deep knowledge of DFARS 7008,7009, 7012, NIST 800-171r2, DoDi 5200,48, 32CFR, part 2002, FAR 52.204-21, CUI Registry; CUI determination and marking; DFARS 7012 2(ii)(D) compliant cloud solutions architecture, and CUI Supply Chain Risk Management.
Recap

Types of Unclassified Information

It’s The Law

1. DFAR 252.204-7012 Compliance Steps:
   1.1 NIST SP 800-171 Self-Assessment
   1.2 POAMS
   1.3 System Security Plan (SSP)
   1.4 Incident Response Plan and Reporting
   1.5 Sub Contractor Flow Down Requirements

Selection Criteria for TPP

Save Compliance Steps documents for CMMC Auditor
2.1 CMMC- Cybersecurity Maturation Model Certification Version #1

The new DFARS clause 252.204-7021, Cybersecurity Maturity Model Certification Requirement, will require the contractor to have the CMMC certification at the level required in the solicitation by contract award and maintain the required CMMC level for the duration of the contract. In order to achieve a specific CMMC level, a Defense Industrial Base (DIB) company must demonstrate both process institutionalization or maturity and the implementation of practices commensurate with that level. A DIB contractor can achieve a specific CMMC level for its entire enterprise network or particular segment(s) or enclave(s), depending upon where the information to be protected is processed, stored, or transmitted.

The CMMC model encompasses the basic safeguarding requirements for FCI specified in FAR clause 52.204-21, Basic Safeguarding of Covered Start Printed Page 61506Contractor Information Systems, and the security requirements for CUI specified in NIST SP 800-171 per DFARS clause 252.204-7012. Furthermore, the CMMC model includes an additional processes and practices across Levels 2-5 that demonstrate a progression of cybersecurity maturity.
2.1 CMMC- Cybersecurity Maturation Model Certification 2.0

Major Changes:

• Removes two levels (former CMMC Levels 2 and 4) from the maturity model framework
• Designates CMMC Level 1 as a **self-attestation only**.
• Eliminate additional practices from CMMC Version 1
• The Plans of Action and Milestone (POAMS) is now as an acceptable form of remediation for certain CMMC practices

EFFECTIVE DATE: ???
With the implementation of CMMC 2.0, the Department intends to introduce the following changes to the CMMC Model relative to CMMC 1.0:

**CMMC 1.0**
- 5 increasingly progressive levels from Basic to Advanced
- Levels 2 and 4 intended as transition stages between Levels 1, 3, and 5

**CMMC 2.0**
- 3 increasingly progressive levels:
  - Foundational / Level 1 (same as previous level 1)
  - Advanced / Level 2 (previous level 3)
  - Expert / Level 3 (previous level 5)
2.1 CMMC- Cybersecurity Maturation Model Certification

**CMMC 1.0**
- Requirements include cybersecurity standards and maturity processes at each level
- Cybersecurity standards consist of certain requirements from NIST SP 800-171 as well as CMMC-unique standards

**CMMC 2.0**
- Eliminates all maturity processes
- Eliminates all CMMC unique security practices:
  - Advanced / Level 2 will mirror NIST SP 800-171 (110 security practices)
  - Expert / Level 3 will be based on a subset of NIST SP 800-172 requirements
2.1 CMMC- Cybersecurity Maturation Model Certification 2.0

What Did Not Change:

• All levels of the CMMC 2.0 require the NIST SP 800. 171 standards
• Level 1 is still based on only 17 NIST Standards

The EFFECTIVE DATE is still: ???
### 2.2 NIST SP 800-171: Control Families

<table>
<thead>
<tr>
<th>Access Control: 22 sections</th>
<th>Media Protection: 9 sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness and Training: 3 sections</td>
<td>Personnel Security: 2 sections</td>
</tr>
<tr>
<td>Audit and Accountability: 9 sections</td>
<td>Physical Protection: 6 sections</td>
</tr>
<tr>
<td>Configuration Management: 9 sections</td>
<td>Risk Assessment: 3 sections</td>
</tr>
<tr>
<td>Identification and Authentication: 11 sections</td>
<td>Security Assessment: 4 sections</td>
</tr>
<tr>
<td>Incident Response: 3 sections</td>
<td>System and Communications Protection: 16 sections</td>
</tr>
<tr>
<td>Maintenance: 6 sections</td>
<td>System and Information Integrity: 7 sections</td>
</tr>
</tbody>
</table>

**Note:** To be Level 2 compliant, you must address all standards and document them in the System Security Plan (SSP).
Access is the ability to make use of any system resource. Access control is the process of granting or denying requests to use information, use information processing services, and enter company facilities.

This family contains 22 standards. Selected sample questions include:

- Does the company use passwords? 3.1.1
- Does the company have an authentication mechanism? 3.1.1
- Do applications used to remotely access the system use approved encryption methods? 3.1.13

*Note: Address all standards and document them in the System Security Plan (SSP).*
2.2 NIST SP 800-171: Control Families
Awareness & Training (3.2)

Users of a system can be viewed as the weakest link in securing systems. Often users are not aware of how their actions may impact the security of a system. Making system users aware of their security responsibilities and teaching them correct practices helps change their behavior.

This family contains 3 inquires. Selected sample questions include:

Is basic security awareness training provided to all system users before authorizing access to the system when required by system changes and at least annually thereafter? 3.2.1

Do all users, managers, and system administrators receive initial and annual training commensurate with their roles and responsibilities? 3.2.1

Note: Address all standards and document them in the System Security Plan (SSP).
2.2 NIST SP 800-171: Control Families
Audit and Accountability (3.3)

An audit is an independent review and examination of records and activities to assess the adequacy of system requirements and ensure compliance with established policies and operational procedures.

This family contains 9 inquiries. Selected sample questions include:

Can the company uniquely trace and hold accountable users responsible for unauthorized actions? 3.3.2

Does the company review and update audited events annually or in the event of substantial system changes or as needed. 3.3.3

Does the system maintain audit records on host servers until log delivery to central repositories can be re-established? 3.3.4

Note: Address all standards and document them in the System Security Plan (SSP).
Configuration management is a collection of activities focused on establishing and maintaining the integrity of information technology products and systems through the control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the System Development Life Cycle (SDLC).

This family contains 9 inquires. Selected sample questions include:

Are baseline configurations developed, documented, and maintained for each information system type? 3.4.1

Are changes to the system authorized by company management and documented? 3.4.4

*Note: Address all standards and document them in the System Security Plan (SSP).*
2.2 NIST SP 800-171: Control Families
Identification & Authentication (3.5)

For most systems, identification and authentication is often the first line of defense. Identification is the means of verifying the identity of a user, process, or device, typically as a prerequisite for granting access to resources in a system.

This family contains 11 inquires. Selected sample questions include:

Do all passwords follow best practice of at least 12 characters, and require a mix of upper and lower case letters, numbers, and special characters? 3.5.2

Is multifactor authentication used for local access to privileged accounts? 3.5.3
Are accounts uniquely assigned to employees, contractors, and subcontractors? 3.5.5

Note: Address all standards and document them in the System Security Plan (SSP).
Systems are subject to a wide range of threat events, from corrupted data files to viruses to natural disasters. Vulnerability to some threat events can be lessened by having standard operating procedures that can be followed in the event of an incident.

This family contains 3 inquires. Selected sample questions include:

Is there a company incident response policy which specifically outlines requirements for handling of incidents involving CUI? 3.6.2

Is cybersecurity incident information promptly reported to company management and authorities? 3.6.2

*Note: Address all standards and document them in the System Security Plan (SSP).*
2.2 NIST SP 800-171: Control Families

Maintenance (3.7)

Controlled maintenance of a system deals with maintenance that is scheduled and performed in accordance with the manufacturer’s specifications.

This family contains 6 inquires. Selected Sample questions include:

Does the company perform maintenance on the information system? 3.7.1

Is there a company media sanitization policy? 3.7.3

Are all activities of maintenance personnel (who do not normally have access to a system) monitored? 3.7.6

Note: Address all standards and document them in the System Security Plan (SSP).
2.2 NIST SP 800-171: Control Families

Media Protection (3.8)

Media protections can restrict access and make media available to authorized personnel only, apply security labels to sensitive information, and provide instructions on how to remove information from media so that the information cannot be retrieved or reconstructed.

This family contains 9 inquires. Selected sample questions include:

Do only approved individuals have access to media from CUI systems? 3.8.1

Are all CUI data on media encrypted or physically locked prior to transport outside of the company’s secure locations? 3.8.3

Are all CUI systems identified with an asset control identifier, for example, does each company laptop have an asset id tag with a unique number? 3.8.4

Note: Address all standards and document them in the System Security Plan (SSP).
2.2 NIST SP 800-171: Control Families
Personnel Security (3.9)

Almost no system can be secured without properly addressing these aspects of personnel security. Personnel security seeks to minimize the risk that staff (permanent, temporary, or contractor) pose to company assets through the malicious use or exploitation of their legitimate access to the company’s resources.

This family contains 2 inquires. Selected samples questions include:

Are individuals requiring access screened before access is granted? 3.9.1

Are electronic and physical access permissions reviewed when employees are reassigned or transferred? 3.9.2

Does the company disable information system access prior to employee termination or transfer? 3.9.2

*Note: Address all standards and document them in the System Security Plan (SSP).*
The term physical and environmental security refers to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment.

This family contains 6 inquire. Selected sample questions contain:

Are all visitors to sensitive areas always escorted by an authorized employee? 3.10.3

Are keys, combinations, and other physical access devices secured? 3.10.5

Are logs of physical access to sensitive areas maintained per retention policies? (This includes authorized access as well as visitor access.) 3.10.4

Note: Address all standards and document them in the System Security Plan (SSP).
2.2 NIST SP 800-171: Control Families
Risk Assessment (3.11)

Risk assessments identify and prioritize risks to company operations, assets, employees, and other organizations that may result from the operation of a system.

This family contains 3 inquiries. Selected sample questions include:

Does the company have a risk management policy? 3.11.1

Is vulnerability scanning performed? 3.11.2

Are reports regarding the scans made available to system owners and company management in a timely manner? 3.11.2

*Note: Address all standards and document them in the System Security Plan (SSP).*
2.2 NIST SP 800-171: Control Families

Security Assessment (3.12)

A security requirement assessment is the testing and/or evaluation of the management, operational, and technical security requirements on a system to determine the extent to which the requirements are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

This family contains 4 inquiries. Selected sample questions include:

Has a periodic (e.g., annual) security assessment been conducted to ensure that security controls are implemented correctly and meet the security requirements? 3.12.1

Is the assessment conducted by an independent security auditor/consultant? 3.12.1

*Note: Address all standards and document them in the System Security Plan (SSP).*
2.2 NIST SP 800-171: Control Families

System and Communications Protection (3.13)

System and communications protection requirements provide an array of safeguards for the system. Some of the requirements in this family address the confidentiality information at rest and in transit.

This family contains 16 inquires. Selected sample questions include:

Does the system monitor and manage communications at the system boundary and at key internal boundaries within the system? 3.13.1

Are processes and automated mechanisms used to provide encryption of CUI during transmission? Are processes and automated mechanisms used to provide encryption of CUI during transmission? 3.13.8

Note: Address all standards and document them in the System Security Plan (SSP).
2.2 NIST SP 800-171: Control Families
System and Information Integrity (3.14)

Integrity is defined as guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

This family contains 7 inquiries. Selected sample questions include:

Does the system automatically update malicious code protection mechanisms? 3.14.2

Does the company receive security alerts, advisories, and directives from reputable external organizations? 3.14.3

Does the company perform real-time scans of files from external sources as the files are downloaded, opened, or executed? 3.14.5

Note: Address all standards and document them in the System Security Plan (SSP).
Recap

DFAR 252.204-7012 Compliance Steps

1.1 NIST SP 800-171 Self Assessment
1.2 Plan of Action and Milestones (POAMS)
1.3 System Security Plan (SSP)
1.4 Incident Response Plan and Reporting
1.5 Sub Contractor Flow Down Requirements

Cybersecurity Maturation Model Certification (CMMC)

NIST SP 800-171: Control Families
Current Cybersecurity DFARS

DFARS 252.204-7019/20:
Interim Rule

Compliance Steps:
1.1 NIST SP 800-171 Self-Assessment
1.2 Plan of Action and Milestones (POAMS)
1.3 System Security Plan (SSP)
1.4 Incident Response Plan and Reporting
1.5 Subcontractor Flow Down Requirements
1.6 Upload Score in SPRS
   - This score is good for three years
Up Coming Webinars

Please visit the Cross Timbers Calendar page:

https://www.uta.edu/crosstimbers/pages/events-workshops/upcoming-events.php

CMMCSmart Basics Webinars-

These six, free webinars, presented by Regan Edens of DTC Global, a follow up to this cybersecurity awareness webinar, go in-depth into the NIST and CMMC.

The First Webinar in the series, CMMCsmart Basics 1: CMMC 2.0/DFARS Ecosystem Updates, begins April 14th. Don’t miss it!!!
<table>
<thead>
<tr>
<th>Key Websites</th>
</tr>
</thead>
<tbody>
<tr>
<td>252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting: <a href="https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012">https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012</a></td>
</tr>
<tr>
<td>National Archives CUI Registry: <a href="https://www.archives.gov/cui">https://www.archives.gov/cui</a></td>
</tr>
<tr>
<td>Computer Security Incident Handling Guide: <a href="https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf">https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf</a></td>
</tr>
<tr>
<td>Supplier Performance Risk System (SPRS): <a href="https://www.sprs.csd.disa.mil/">https://www.sprs.csd.disa.mil/</a></td>
</tr>
</tbody>
</table>
# Key Websites

<table>
<thead>
<tr>
<th>Category</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOD INSTRUCTION 5200.48 CONTROLLED UNCLASSIFIED INFORMATION (CUI)</td>
<td><a href="https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF">https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF</a></td>
</tr>
<tr>
<td>Cyber Incident Reporting</td>
<td><a href="https://dibnet.dod.mil/portal/intranet/">https://dibnet.dod.mil/portal/intranet/</a></td>
</tr>
<tr>
<td>CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)</td>
<td><a href="https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf">https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf</a></td>
</tr>
<tr>
<td>CMMC Level 1 &amp; Level 3 Assessment Guides</td>
<td><a href="https://www.acq.osd.mil/cmmc/draft.html">https://www.acq.osd.mil/cmmc/draft.html</a></td>
</tr>
<tr>
<td>Determining Authorized Holders of CUI</td>
<td><a href="https://youtu.be/egbAZ1f5r8g">https://youtu.be/egbAZ1f5r8g</a></td>
</tr>
<tr>
<td>DFARS &amp; NIST 800-171 Compliance 101</td>
<td><a href="https://youtu.be/2g4sm7rVqjM">https://youtu.be/2g4sm7rVqjM</a></td>
</tr>
<tr>
<td>Export Controls</td>
<td><a href="http://www.access.gpo.gov/bis/ear/ear_data.html">http://www.access.gpo.gov/bis/ear/ear_data.html</a></td>
</tr>
</tbody>
</table>
**Key Websites**

<table>
<thead>
<tr>
<th>Website</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>TMAC/MEP</td>
<td><a href="https://tmac.org/additional-services/">https://tmac.org/additional-services/</a></td>
</tr>
<tr>
<td>DIB SCC CyberAssist</td>
<td><a href="https://ndisac.org/dibsccc/cyberassist/">https://ndisac.org/dibsccc/cyberassist/</a></td>
</tr>
<tr>
<td>CMMCsmart Virtual Helpdesk</td>
<td><a href="https://www.cmmcsmart.com/">https://www.cmmcsmart.com/</a></td>
</tr>
<tr>
<td>CMMC Accreditation Body</td>
<td><a href="https://www.cmmcab.org/">https://www.cmmcab.org/</a></td>
</tr>
<tr>
<td>Info Defense</td>
<td><a href="https://www.infodefense.com/">https://www.infodefense.com/</a></td>
</tr>
<tr>
<td>DTC Global</td>
<td><a href="https://dtcglobal.us/contact-us">https://dtcglobal.us/contact-us</a></td>
</tr>
<tr>
<td>CUI Program Blog</td>
<td><a href="https://isoo.blogs.archives.gov/">https://isoo.blogs.archives.gov/</a></td>
</tr>
<tr>
<td>ITAR</td>
<td><a href="http://www.fas.org/spp/starwars/offdocs/itar/p121.htm">http://www.fas.org/spp/starwars/offdocs/itar/p121.htm</a></td>
</tr>
<tr>
<td>DoD CUI Program</td>
<td><a href="https://www.dodcui.mil/">https://www.dodcui.mil/</a></td>
</tr>
</tbody>
</table>
Additional Assistance

Darold Tippey  
Darold.Tippey@tmac.org  
(817) 789-9249 | TMACdfw.org
The University of Texas at Arlington

For FREE Interim Rule Compliance tools, schedule a cybersecurity review with CTPTAC.
Contact

Cross Timbers Procurement Technical Assistance Center
University of Texas at Arlington
202 East Border St, #323
Arlington Texas 76010
www.uta.edu/crosstimbers

Spelile Rivas Spelile.rivas@uta.edu 817-689-3570

Gregory James gjames@uta.edu 817-272-5978

This procurement technical assistance center is funded in part through a cooperative agreement with the Defense Logistics Agency.