How to Comply with DFAR 252-204-7012 & NIST SP 800-171 Rev. 2

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 www.uta.edu/crosstimbers/webinars.
The purpose of this webinar is to create awareness of the current cybersecurity regulations, the DFAR 252.204.7012, and to help you understand what is expected as it relates to the new CMMC cybersecurity requirements.

It is in the interest of National Security that ALL of the companies doing business with DoD will have to comply immediately with DFARS 252.204-7012 and have a Cybersecurity Maturation Model Certification (CMMC) level 1-3.
Agenda

1. DFAR 252.204-7012 Compliance Steps

2. Cybersecurity Maturation Model Certification (CMMC)

3. NIST SP 800-171: Control Families
DFAR 252.204-7012: By signing a DoD contract, the contractor agrees to comply with the terms of the contract and all requirements of the DFARS Clause 252.204-7012. The deadline for compliance was Dec 31, 2017. The regulations apply to ANY current DoD contractor with the DFARS 252.204-7012 clause within the contract.

False Claim Act: False Claims Act (FCA), 31 U.S.C. §§ 3729 - 3733, is a federal statute originally enacted in 1863 in response to defense contractor fraud during the American Civil War.

Cybersecurity Maturation Model Certification (CMMC): The intent is to incorporate CMMC into Defense Federal Acquisition Regulation Supplement (DFARS) and use it as a requirement for contract award. Contractors are subject to third Party Assessment Organizations (C3PAOs) certification auditors.
Current contracts including the DFARS 252.204-7012 will likely not be amended until the re-compete. Expect requirements to be more aggressively enforced through the Contracting Officer, Service investigative agencies, such as NCIS, DCMA, and referred to the Federal False Claims Act.

Enforcement of the current requirements is aggressively expanding through Defense Contact Management Agency (DCMA) audit, Federal False Claims Act referrals, and the individual military services authorization for criminal enforcement.

The regulations apply to ANY current DoD contractor with the DFARS 252.204-7012 clause within their contract. Those corporate (non-federal contractor information systems) that create, receive, share, store, or transmit CUI data... globally.

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting. | Acquisition.GOV
Types of Unclassified Information

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

**OUSD A&S - Cybersecurity Maturity Model Certification (CMMC) (osd.mil)**

**Controlled Unclassified Information:** 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://www.archives.gov/cui)  [https://youtu.be/egbAZ1f5r8g](https://youtu.be/egbAZ1f5r8g)
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

Complete questionnaire. Ask about Cross Timber’s Self Assessment Tool.

Review total scores to know and understand the weaknesses.

Develop plan and budget to fix the weaknesses. Hire professional company to help if needed.

NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements

https://doi.org/10.6028/NIST.SP.800-171A

Save Self Assessment results for CMMC auditors
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)


Save POAM results for CMMC Auditor.
## 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 sections</td>
</tr>
<tr>
<td>3.2 Awareness and Training</td>
<td>3 sections</td>
</tr>
<tr>
<td>3.3 Audit and Accountability</td>
<td>9 sections</td>
</tr>
<tr>
<td>3.4 Configuration Management</td>
<td>9 sections</td>
</tr>
<tr>
<td>3.5 Identification and Authentication</td>
<td>11 sections</td>
</tr>
<tr>
<td>3.6 Incident Response</td>
<td>3 sections</td>
</tr>
<tr>
<td>3.7 Maintenance</td>
<td>6 sections</td>
</tr>
<tr>
<td>3.8 Media Protection</td>
<td>9 sections</td>
</tr>
<tr>
<td>3.9 Personnel Security</td>
<td>2 sections</td>
</tr>
<tr>
<td>3.10 Physical Protection</td>
<td>6 sections</td>
</tr>
<tr>
<td>3.11 Risk Assessment</td>
<td>3 sections</td>
</tr>
<tr>
<td>3.12 Security Assessment</td>
<td>4 sections</td>
</tr>
<tr>
<td>3.13 System and Communications Protection</td>
<td>16 sections</td>
</tr>
<tr>
<td>3.14 System and Information Integrity</td>
<td>7 sections</td>
</tr>
</tbody>
</table>

Save SSP for CMMC Auditor
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

Save IRPR for CMMC Auditor
1. DFAR 252.204-7012 Compliance Steps

1.5 Subcontractor Flow Down Requirements

When should DFARS Clause 252.204-7012 flow down to subcontractors?

• The clause is required to flow down to subcontractors only when performance will involve operationally critical support or covered defense information.

• The contractor shall determine if the information required for subcontractor performance is, or retains its’ identity as, covered defense information and requires safeguarding.

• Flow down is a requirement of the terms of the contract with the Government, which must be enforced by the prime contractor as a result of compliance with these terms.

– If a subcontractor does not agree to comply with the terms of DFARS Clause 252.204–7012, then covered defense information shall not be shared with the subcontractor or otherwise reside on its’ information system.

Selection Criteria for Third Party Providers (TPP’s)
Regan Edens reganedens@dtcglobal.us CMMC AB Director

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.
Choose Consultants or Firms that engage you with best practices AND a variety of appropriate "turn-key solutions" often through trusted partners to address gaps (big and small). "Frankensteining" by piecing together disparate solutions is often FAR MORE EXPENSIVE and TIME INTENSIVE than needed. The importance of trusted relationships is worth emphasizing.

If you do not trust them to recommend MORE THAN THEIR SOLUTIONS, do not use them. Their strategy should best optimize WHAT YOU HAVE and ONLY THEN RECOMMEND WHAT YOU NEED. Compliance is THE objective, not getting you to buy "more stuff" or worse "more of their stuff".
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 help from IT companies

Save Compliance Steps documents for CMMC Auditor
2. CMMC- Cybersecurity Maturation Model Certification

The CMMC encompass multiple maturity levels that ranges from “Basic Cybersecurity Hygiene” to “Advanced/Progressive”. Contracting Officers will mark solicitation and award contracts with each level. Contractors will only be able to bid on their level issued by CMMC auditors.  

https://www.acq.osd.mil/cmmc/faq.html

The CMMC model consists of 17 domains or Control Families. In addition to the 14 NIST SP 800-171 families, the CMMC includes an additional three domains of Asset Management (AM), Recovery (RE) and Situational Awareness (SA).

The CMMC Accreditation Body (AB), a non-profit, independent organization, will accredit CMMC Third Party Assessment Organizations (C3PAOs) and individual assessors.

The CMMC audit guide is to be released shortly. For updates contact CMMC Board Director Regan Edens at reganedens@dtcglobal.us or bookmark https://www.cmmcab.org/

CMMC certification will apply to both Federal Contract Information (FCI) under FAR 52. 204-21 and Controlled Unclassified Information (CUI) DFARS 252.204-7012 (and the DoD rule change).
2. CMMC- Cybersecurity Maturation Model Certification

At this time, sellers of Commercial Off the Shelf (COTS) products don’t require CMMC certifications. However, companies that make COTS products will need to comply.

CMMC certification will apply to both Federal Contract Information (FCI) under FAR 52. 204-21 and Controlled Unclassified Information (CUI) DFARS 252.204-7012 (and the DoD rule change).

DoD, Federal law, and policy (DoDi 5200.48 and 32CFR, 2002, ISOO CUI Registry) require prime contractors to mark CUI and CMMC levels on their subcontracts.


In Oct, the Federal rule-making process is expected to be complete and is expected to expand across all Federal Agencies. The rule change is also expected to include CMMC certification requirements for Levels 1-5 for (at least) DoD contractors.

Enforcement of the current requirements is aggressively expanding through Defense Contact Management Agency (DCMA) audit, Federal False Claims Act referrals, and the individual military services authorization for criminal enforcement.

Please see [https://youtu.be/2g4sm7rVqjM](https://youtu.be/2g4sm7rVqjM)
2. Cybersecurity Maturation Model Certification

- **Level 1 – Basic Cyber Hygiene**: Includes basic cybersecurity appropriate for small companies utilizing a subset of universally accepted common practices. This level has 35 security controls that must be successfully implemented.

- **Level 2 – Intermediate Cyber Hygiene**: Includes universally accepted cybersecurity best practices. This level includes an additional 115 security controls beyond that of Level 1.

- **Level 3 – Good Cyber Hygiene**: Includes coverage of all NIST SP 800-171 Rev. 1 controls and additional practices beyond the scope of current CUI protection. This level requires an additional 91 security controls beyond those covered in Levels 1 and 2.

- **Level 4 – Proactive**: Includes advanced and sophisticated cybersecurity practices. This level has an additional 95 controls beyond the first three Levels.

- **Level 5 – Advanced / Progressive**: Includes highly advanced cybersecurity practices. This level requires an additional 34 controls.

Recap

2. Cybersecurity Maturation Model Certification (CMMC)

Level 1 – Basic Cyber Hygiene

Level 2 – Intermediate Cyber Hygiene

Level 3 – Good Cyber Hygiene

Level 4 – Proactive

Level 5 – Advanced / Progressive
### 3. NIST SP 800-171: Control Families

<table>
<thead>
<tr>
<th>Control Family</th>
<th>Number of 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>


https://doi.org/10.6028/NIST.SP.800-171A
3. NIST SP 800-171: Control Families
Access Control (3.1)

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 sections and 2+ questions. 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

ALL questions will need to be addressed and written into a DETAILED SSP.
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 sections and 12+ questions. 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

ALL questions will need to be addressed and written into a DETAILED SSP.
3. 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. An audit trail is a record of individuals who have accessed a system as well as what operations the user has performed during a given period.

This family contains 9 sections and 25+ questions. 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

ALL questions will need to be addressed and written into a DETAILED 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 sections and 34+ questions. 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

**ALL questions will need to be addressed and written into a DETAILED SSP.**
3. 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 sections and 40+ questions. 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

ALL questions will need to be addressed and written into a DETAILED SSP.
3. NIST SP 800-171: Control Families

Incident Response (3.6)

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 sections and 19+ questions. 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

ALL questions will need to be addressed and written into a DETAILED SSP.
3. 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 sections and 15+ questions. 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

**ALL questions will need to be addressed and written into a DETAILED SSP.**
3. 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 sections and 35+ questions. 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

ALL questions will need to be addressed and written into a DETAILED SSP.
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 sections and 7+ questions. 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

ALL questions will need to be addressed and written into a DETAILED SSP.
3. NIST SP 800-171: Control Families

Physical Protection (3.10)

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 sections and 15+ questions. 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

ALL questions will need to be addressed and written into a DETAILED SSP.
3. 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 sections and 14+ questions. 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

ALL questions will need to be addressed and written into a DETAILED SSP.
3. 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 sections and 23+ questions. 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

ALL questions will need to be addressed and written into a DETAILED SSP.
System and communications protection requirements provide an array of safeguards for the system. Some of the requirements in this family address the confidentiality of information at rest and in transit.

This family contains 16 sections and 35+ questions. 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

**ALL questions will need to be addressed and written into a DETAILED SSP.**
Integrity is defined as guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

This family contains 7 sections and 22+ questions. 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

ALL questions will need to be addressed and written into a DETAILED 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
# Key Websites

<table>
<thead>
<tr>
<th>252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting:</th>
<th><img src="https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012" alt="Image" /></th>
</tr>
</thead>
<tbody>
<tr>
<td>National Archives CUI Registry:</td>
<td><img src="https://www.archives.gov/cui" alt="Image" /></td>
</tr>
<tr>
<td>NIST 800-171 Hand Book:</td>
<td><img src="https://doi.org/10.6028/NIST.SP.800-171A" alt="Image" /></td>
</tr>
<tr>
<td>SP 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. See templates for SSP, POEMS and the SP 800-171 Rev. 2 (DOI)</td>
<td><img src="https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final" alt="Image" /></td>
</tr>
<tr>
<td>Computer Security Incident Handling Guide:</td>
<td><img src="https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf" alt="Image" /></td>
</tr>
</tbody>
</table>
## Key Websites

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOD Instruction 5200.48 CUI</td>
<td>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>Cybersecurity Maturity Model Certification (CMMC)</td>
<td></td>
<td><a href="https://www.acq.osd.mil/cmmc/">https://www.acq.osd.mil/cmmc/</a></td>
</tr>
<tr>
<td>Determining Authorized Holders of CUI</td>
<td></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></td>
<td><a href="https://youtu.be/2g4sm7rVqjM">https://youtu.be/2g4sm7rVqjM</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/dibscc/cyberassist/">https://ndisac.org/dibscc/cyberassist/</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>
</tbody>
</table>
Contact

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

Shelia Birdow shelia.birdow@uta 817-272-2081

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

The University of Texas at Arlington/Cross Timbers Procurement Technical Assistance Center is Funded in part through a cooperative agreement with the Department of Defense.

Additional Assistance

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

TMAC
Work Smart. Grow Smart.

PART OF THE MEP National Network™