Following the Cybersecurity DFARS in your small business contract
The Slides are Located at:

Federal Acquisition Regulation (FAR) and DFARS

Small Business contracts contains many FARS and DFARS, you must study them at length. These are not all of them, but these are some key security requirements.

What is a DFARS? The Defense Federal Acquisition Regulation Supplement (DFARS) contains requirements of law, DoD-wide policies, delegations of Federal Acquisition Regulation (FAR) authorities, deviations from FAR requirements, and policies/procedures that have a significant effect on the public.
DFARS Clause 252.204-7021
Cybersecurity Maturity Model Certification Requirement

This DFARS is under review and it’s status will not be known until early 2023 at the earliest.

Until then, compliance with and full implementation of DFARS Clause 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting” is sufficient.

For more information on the new version of CMMC, see this great webinar by the DCMA Director John Ellis.
https://www.preveil.com/resources/webinar-john-ellis-on-cmmc-2-0/

Stay up-to-date at https://dodcio.defense.gov/CMMC/
https://dodcio.defense.gov/CMMC/
Applies when a cloud solution is being used to process data on the DoD's behalf or DoD is contracting with Cloud Service Provider to host/process data in a cloud

**Ensures** that the cloud service provider:

- Use government-related data only to manage the operational environment that supports the Government data and for no other purpose
- Complies with requirements for cyber incident reporting and damage assessment

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, applies when a contractor intends to use an external cloud service provider to store, process, or transmit covered defense information in the performance of a contract. DFARS Clause 252.204-7012 requires the cloud service provider to meet security requirements equivalent to those established for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.
Safeguarding Requirements and Procedures

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

- The FAR lists 15 security controls, which are considered basic cyber hygiene

(2) Other requirements. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

Flow-Down the Requirement

The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.
DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

- Report cyber incidents
- Submit malicious software
- Facilitate damage assessment
- Safeguard covered defense information
What if There is a Potential Breach?

Don’t Panic. Cybersecurity occurs in a dynamic environment. Hackers are constantly coming up with new ways to attack information systems, and DoD is constantly responding to these threats. Even if a contractor does everything right and institutes the strongest checks and controls, it is possible that someone will come up with a new way to penetrate these measures. DoD does not penalize contractors acting in good faith. The key is to work in partnership with DoD so that new strategies can be developed to stay one step ahead of the hackers.

Contact DoD Immediately. Bad news does not get any better with time. These attacks threaten America’s national security and put service members’ lives at risk. DoD has to respond quickly to change operational plans and to implement measures to respond to new threats and vulnerabilities. Contractors should report any potential breaches to DoD within 72 hours of discovery of any incident.

Be Helpful and Transparent. Contractors must also cooperate with DoD to respond to security incidents. Contractors should immediately preserve and protect all evidence and capture as much information about the incident as possible. They should review their networks to identify compromised computers, services, data and user accounts and identify specific covered defense information that may have been lost or compromised.
What to Report to the Federal Government

**DHS Definition:** A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems.

**DFARS 7012 Definition** “Cyber incident” means actions 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.

Report all cyber incidents that may:
- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.
Where to Report Cyber Incidents/Malware

To report cyber incidents that affect covered defense information OR that affect the contractor’s ability to perform requirements designated as operationally critical support, the Contractor shall conduct a review for evidence of compromise and rapidly report cyber incidents to DoD at https://dibnet.dod.mil via an incident collection form (ICF).

If discovered and isolated in connection with a reported cyber incident, the contractor/subcontractor shall submit the malicious software to the DoD Cyber Crime Center (DC3). Also, https://dibnet.dod.mil

If DoD elects to conduct a damage assessment, the Contracting Officer will be notified by the requiring activity to request media and damage assessment information from the contractor.
Welcome to the DIBNet portal
DoD's gateway for defense contractor reporting and voluntary participation in DoD's DIB Cybersecurity Program.

Cyber Reports

A Medium Assurance Certificate is required to report a Cyber Incident, applying to the DIB CS Program is not a prerequisite to report.

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
DFARS 252.239-7010 Cloud Computing Services
FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities
FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

Need Assistance?
Contact DoD Cyber Crime Center (DC3)
DC3SE@d3.com
Hotline: (410) 981-0104
Toll Free: (877) 838-2174

DoD's DIB Cybersecurity (CS) Program

Apply Now!

The DIB CS Program is a voluntary public-private cybersecurity partnership in which DoD and participants share cyber threat information, mitigation and remediation strategies, and more.

DIB CS Participant Login Voluntary Report

Cyber Threat Roundup

The Cyber Threat Roundup is a weekly collection of recent open-source articles of interest for the Defense Industrial Base. If you'd like to receive the latest edition of the Cyber Threat Roundup, please click here.

For more information, please visit:
https://dibnet.dod.mil

A DoD-approved Medium Assurance Certificate is required to access DIBNet services. To obtain a DoD-approved Medium Assurance Certificate, please click here.
Cyber Threat Roundup

A collection of recent open-source items of interest to the Defense Industrial Base

Contents

Articles ........................................................................................................................................... 2

Cyber Incident at Boeing Subsidiary Causes Flight Planning Disruptions ............................................ 2
LockBit Ransomware Gang Claims the Hack of Continental Automotive Group ........................................ 2
FIN7 Cybercrime Group Likely Behind Black Basta Ransomware Campaign ............................................. 2
Supply Chain Attack Pushes Out Malware to More than 250 Media Websites ........................................ 2
U.S. Treasury Thwarts DDoS Attack from Russian Killnet Group .......................................................... 2
Microsoft Rolls Out Fix for Outlook Disabling Teams Meeting Add-In .................................................. 3
Safeguard Covered Defense Information (CDI)

CDI is defined as unclassified controlled technical information (CTI) or other information as described in the DOD CUI Registry

AND it is marked as CUI

OR otherwise identified in the contract and provided to the contractor by DoD in support of performance of the contract;

OR collected/developed/received/transmitted/used/ stored by the contractor in performance of contract.
Safeguard CDI: What is CUI?

The DOD CUI Registry and detailed training on what constitutes CUI is available from the DOD at this link: https://www.dodcui.mil
Safeguard CDI: What is CTI?

Controlled Technical Information (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.

Controlled technical information is to be marked.

The term does not include information that is lawfully publicly available without restrictions.

"Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items"

Examples of technical information include: research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.
**Implementation of NIST SP 800-171**

Implementation of the NIST SP 800-171 involves implementing and documenting the 110 security requirements listed in the document.

- The implementation of security requirements is recorded in a System Security Plan (NIST SP 800-171 security requirement 3.12.4) and
- Any un-implemented security requirement and its interim plan to provide alternative, but equally effective, security measure is recorded in a Plan of Action with Milestones, called a POAM (NIST SP 800-171 security requirement 3.13.2)

Help with understanding the NIST SP 800-171 security requirements is found at this link: [https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf](https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf)
NIST SP 800-171 System Security Plan (SSP)

Optional Template available on NIST.Gov

Optional Template to record the Plan of Action on NIST.gov
Safeguard Covered Defense Information (CDI)

To safeguard covered defense information contractors/subcontractors must implement NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations

The covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171

- The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017.
- The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO
“By submission of this offer, the Offeror represents that it will implement the security requirements specified by NIST SP 800-171, ... not later than December 31, 2017.

If the Offeror proposes to vary from any of the security requirements specified by NIST SP 800-171 ..., the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of:

- Why a particular security requirement is not applicable
- How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.
- An authorized representative of the DoD CIO will adjudicate offeror requests to vary from NIST SP 800-171 requirements in writing prior to contract award. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting contract.
DFARS Clause 252.204-7019/7020
NIST SP 800-171 DoD Assessment Requirements.

Self-Assessment
Submit information to SPRS.CSD.DISA.MIL
Flow the Requirement Down
Update your Self-Assessment
The Requirement in DFARS Clause 252.204-7019/7020 - NIST SP 800-171
DoD Assessment Requirements

In order to be considered for award, if the Offeror is required to implement NIST SP 800-171, the Offeror shall have a current assessment for each covered contractor information system that is relevant to the contract.

A Basic Assessment, which is a self-assessment assigned a low confidence level (because it is self-generated) is:

- Based on the Contractor’s review of their system security plan(s) associated with covered contractor information system(s)
- Conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology
Not All of the NIST SP 800-171 Security Requirements are Equal

The NIST SP 800-171 DoD Assessment Methodology identifies **42 security requirements** that, if not implemented, could lead to **significant exploitation of the network, or exfiltration of DoD CUI**. These high-risk security requirements are with 5 points in the DoD scoring rubric.

- For example, Failure to limit system access to authorized users (Requirement 3.1.1) **renders all the other Access Control requirements ineffective**, allowing easy exploitation of the network.
- For example, Failure to control the use of removable media on system components (Requirement 3.8.7) **could result in massive exfiltration of CUI and introduction of malware**.

---

### NIST SP 800-171 DoD Assessment Scoring Template

<table>
<thead>
<tr>
<th>Security Requirement</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1* Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>3.1.2* Limit system access to the types of transactions and functions that authorized users are permitted to execute.</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>3.1.3 Control the flow of CUI in accordance with approved authorizations.</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>3.1.6 Use non-privileged accounts or roles when accessing non-security functions.</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>3.1.8 Limit unsuccessful login attempts.</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

---

**DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.**

Approved, DCN# 543-577-23
How to Enter a Basic Assessment Data into SPRS

Post or email your business’ summary level scores of a current NIST SP 800-171 DoD Assessment to SPRS for all covered contractor information systems relevant to the contract.

Your entry consists of

1. **A system security plan** (NIST SP 800-171 item 3.12.4) supporting the performance of a DoD contract—

2. **Summary level score** (e.g., 95 out of 110, NOT the individual value for each requirement) using the NIST SP 800-171 DoD Assessment Methodology

3. **Date that all requirements are expected to be implemented** (i.e., a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171

The SPRS website offers numerous training videos which will help you get an account and make your entry.
How to enter a Basic Assessment Data into SPRS

SPRS Basic Assessment data entry fields

Example output of SPRS Basic Assessment
You Have Help with NIST SP 800-171A, Assessing Security Requirements for CUI

- The NIST SP 800-171A provides nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the CUI security requirements.

- The assessment procedures are flexible and can be customized to the needs of the organizations and the assessors conducting the assessments.
DON CISO’S BLUE CYBER

New Documentation Guides

https://dodcio.defense.gov/CMMC/
Why NIST SP 800-171 - Protecting CUI in Nonfederal Information Systems and Organizations?

The NIST SP 800-171 was written using performance-based security requirements to enable contractors to use systems and practices they already have in place to process, store, or transmit CUI.

- It eliminates unnecessary specificity and includes only those security requirements necessary to provide adequate protection.
- Though most requirements in NIST SP 800-171 are about policy, process, and configuring IT securely, some require security-related software or additional hardware.
Can I Give My Contractor CUI?

DFARS 7012 “Adequate Security” Quote

... (b) *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

   (i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

   (ii)(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017...
Answer Today:
Can I Give My Contractor CUI? You Need to Ask.

Yes, If:

• The decision to share CUI is a risk-based decision based upon a conversation with the contractor regarding if they are ready to provide adequate protection to DoD CUI.
• There is not a cut and dried answer rubric.
• CUI protection is a shared responsibility between the DoD and industry.
• Adequate security will vary depending on the nature and sensitivity of the information on any given non-DoD information system.

See DFARS 252.204-7012 “Safeguarding Covered Defense Information and Cyber Incident Reporting, December 2019,” “Section b”, for a description of “Adequate Security”

If you need help with this decision, please contact your Program or Wing cybersecurity office. Also, Kelley Kiernan from the DON CISO Office is available to talk with you. Keep your contracting officer informed of your activities.

This question is being studied across the DOD – check back for an updated answer.
Discuss with the Contractor Their Readiness to Provide Adequate Protection for DOD CUI

Risk-Based Decision Questions

- Review the contractor’s System Security Plan and associated POAM
  - Are all 42, 5-point weighted security requirements implemented with no POAM?
  - Are all 14, 3-point weighted security requirements implemented with no POAM?
- Is the CUI that the DON is considering sharing with the contractor in a sensitive category such as these categories? NOFORN, FED ONLY, NOCON, DL ONLY, REL TO [USA, LIST], DISPLAY ONLY, Attorney-Client, Attorney-WP or otherwise sensitive?
- Is the CUI that the DON is considering sharing with the contractor mission-essential?
- Is the CUI the DON is considering sharing with the contractor appropriate for research?
- Have you rejected the use of synthetic data in this contract?
- Apply these questions to contractor-created CUI and the government-provided CUI
DOD SAFE Creates Potential Exposure

DOD Safe will let a CAC-holder send CUI to any email address. You must ask contractors if they are ready to provide adequate protection to any CUI sent via DOD SAFE and be satisfied with the answer you receive.

- Contractors who are not ready to protect CUI should not accept CUI
Prohibition on Contracting for some items

SBIR/STTR contract contains many requirements. Many talk to not contracting with certain entities for certain items.

FAR 52.204-23
Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities

FAR 52.204-25
Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment
52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities.

Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from—

1. Providing
2. Using

You must report exceptions

In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or any other source, the Contractor shall report, in writing, to the Contracting Officer or, in the case of the Department of Defense, to the website at https://dibnet.dod.mil.

You must Flow the requirement down to subcontractors

All of these DFARS have many facets; this briefing is a high-level look
FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

Prohibition
Prohibits the head of an executive agency, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception has been granted.

- Nor may you enter into a contract, or extend or renew a contract, with a Covered foreign country, which means The People’s Republic of China.

Reporting requirement
In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information to the Contracting Officer, in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil.
Small Business Help From SCORE

SCORE has the largest network of free volunteer small business mentors in the nation. No matter what stage your business is at, SCORE has a mentor for you. Easily request a mentor to help you start, grow, or transition your business today.

Find a Mentor

SBIR/STTR Firms!

Grow with Google Digital Readiness Series

SCORE has partnered with Grow with Google to bring you a Digital Readiness Series. By completing this course you will receive a completion certificate from Google! Through video and on-demand classes you can go through this series at your own pace and schedule. After finishing these courses you’ll possess all the knowledge you need to launch and grow your business on a digital platform.

Take The Series
MEP is a public-private partnership with Centers in all 50 states and Puerto Rico dedicated to serving small and medium-sized manufacturers. Last year, MEP Centers interacted with 27,574 manufacturers, leading to $13.0 billion in sales, $2.7 billion in cost savings, $4.9 billion in new client investments, and helped create or retain 105,748 jobs.

www.nist.gov/mep

Coronavirus: Resources, Updates, and What You Should Know

EXECUTIVE ORDER 14005 ON ENSURING THE FUTURE IS MADE IN ALL OF AMERICA BY ALL OF AMERICA’S WORKERS

ALL 51 MEP CENTERS HELPING U.S. MANUFACTURERS MAKE SUCH THINGS AS PPE FROM THE $50M APPROPRIATED BY CONGRESS

MANUFACTURING VIDEOS: REAL STORIES, REAL RESULTS

Approved, DCN# 543-577-23

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.
Russia's invasion of Ukraine could impact organizations both within and beyond the region, to include malicious cyber activity against the U.S. homeland, including as a response to the unprecedented economic costs imposed on Russia by the U.S. and our allies and partners. Evolving intelligence indicates that the Russian Government is exploring options for potential cyberattacks. Every organization—large and small—must be prepared to respond to disruptive cyber incidents. As the nation's cyber defense agency, CISA stands ready to help organizations prepare for, respond to, and mitigate the impact of cyberattacks. When cyber incidents are reported quickly, we can use this information to render assistance and as warning to prevent other organizations and entities from falling victim to a similar attack.

Organizations should report anomalous cyber activity and/or cyber incidents 24/7 to report@cisagov or (888) 282-0870.
NSA Cybersecurity Services

Protective DNS/Secure Web Gateway
Vulnerability Scanning and Mitigation
Threat Intelligence Collaboration

Contact NSA DIB Defense

CYBERCENTER.NSA.GOV
@NSACYBER
DIB_DEFENSE@CYBER.NSA.GOV
Cybersecurity Services

CISA Cybersecurity Services

- Vulnerability Scanning
- Remote Penetration Testing
- Phishing Campaign Assessment
- Web Application Scanning
- External Dependencies Management
- Cyber Resilience Review
- & more

For more information on these services, visit
www.cisa.gov/publication/cisa-services-catalog
-or
https://www.cisa.gov/cyber-resource-hub
NIST 800-171 Score

Score: 0

Actions
Return to NIST 800-171 Assessment

History
No History available.

Access Control
These questions ask about your policies to control access to your company’s network systems.

1. Do you limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)?

   Authorized users are identified.
   Processes acting on behalf of authorized users are identified.
   Devices (and other systems) authorized to connect to the system are identified.
   System access is limited to authorized users.
   System access is limited to processes acting on behalf of authorized users.
   System access is limited to authorized devices (including other systems).

   Yes
   No
   Not Applicable
   Answer Later
### Other Resources

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Pager: Safeguarding Covered Defense Information – The Basics</td>
<td>Current Version</td>
</tr>
<tr>
<td>About the Cybersecurity Evaluation Tool (CSET) Tool</td>
<td>Current Version</td>
</tr>
<tr>
<td>Briefing Slides from June 23, 2017 Public Meeting on Network Penetration Reporting and Contracting for Cloud Services</td>
<td>Current Version</td>
</tr>
<tr>
<td>What Happens on December 31, 2017</td>
<td>Current Version</td>
</tr>
<tr>
<td>Approach to Implementing NIST SP 800-171</td>
<td>Current Version</td>
</tr>
<tr>
<td>Navigating Unclassified Information System Security Protections (1 of 2)</td>
<td>Current Version</td>
</tr>
<tr>
<td>Script for Navigation Slides (2 of 2)</td>
<td>Current Version</td>
</tr>
<tr>
<td>Webinars: Implementing DFARS Clause 252.204-7012 (Part 1)</td>
<td>Current Version</td>
</tr>
<tr>
<td>Webinars: Implementing DFARS Clause 252.204-7012 (Part 2)</td>
<td>Current Version</td>
</tr>
<tr>
<td>Webinars: Implementing DFARS Clause 252.204-7012 (Part 3)</td>
<td>Current Version</td>
</tr>
<tr>
<td>To Assist In Development of the System Security Plan and Plans of Action</td>
<td>Current Version</td>
</tr>
<tr>
<td>NIST MEP Handbook for NIST SP 600-171</td>
<td>Current Version</td>
</tr>
</tbody>
</table>

Daily Office Hours for answering/researching your questions about Small Business cybersecurity and data protection!

All FREE and PUBLIC events can be found on www.sbir.gov/events
All our Events are on SBA’s SBIR Event Site
Daily, Open Office Hours

DAILY OFFICE HOURS

- Register here: www.safcn.af.mil/CISO/small-business-cybersecurity-information/
- Nearly-daily opportunity to ask questions and get answers in-person.
- More information at https://www.safcn.af.mil/Contact-Us/
Every-Tuesday, Small Business Cybersecurity Ask-Me-Anything

WEEKLY – Every Tuesday 1pm Eastern

• Register here: www.sbir.gov/events

• A guest speaker will cover an ultra-relevant small business cybersecurity topic and get your cybersecurity/information protection questions answered.

• More information at https://www.safcn.af.mil/Contact-Us/
Department of the Navy
Cybersecurity Boot Camp
DON CISO's Blue Cyber
Walk Through of all 110 Requirements of NIST SP 800-171
Eight-Hour Boot Camp FREE and PUBLIC

REGULARLY – Month x and x, 2023  11am to 3pm Eastern

Register here: www.sbir.gov/events

• We will talk about what is gained by implementing NIST SP 800-171, which is a component of the DFARS 252-204-7012, which is a requirement in the small business contract you sign today. This talk is to help the C-suite understand the requirements as you ensure robust cybersecurity for your company’s intellectual property, your employee’s PII, your financial data and the protection of sensitive government data.

• More information at https://www.safcn.af.mil/Contact-Us/
Department of the Navy
Cybersecurity Boot Camp
DON CISO Small Business –
Academic/Research Contractor and Potential Contractors

MONTHLY – TBD

- Register here: www.sbir.gov/events
- Join hundreds of your peers at the DON CISO’s Cybersecurity Boot Camp. Come away having heard powerful speakers and learning what cybersecurity steps are necessary to protect your intellectual property and DoD Sensitive Data.
- More information at https://www.safcn.af.mil/Contact-Us/
Everybody Handles Federal Contracting Information!
Walk Through of the FAR 52.204-21 and proposed CMMC Level 1

MONTHLY – TBD

• Register here: www.sbir.gov/events

• The Blue Cyber Director, Kelley Kiernan will cover the 15 security requirements in the proposed CMMC Level 1 and FAR 52.204-21, which comprise basic cyber hygiene for your small business.

• More information at https://www.safcn.af.mil/Contact-Us/
Any Questions?

- This briefing is not a substitute for reading the FAR and DFARS in your contract.
- Please provide questions, feedback or if you just want to talk about your cybersecurity/data protection at https://www.safcn.af.mil/Contact-Us/questions

Daily Office Hours for answering/researching your questions about DON Small Business cybersecurity and data protection!

Every Tuesday, 1pm Eastern, dial in for the DON CISO’s Small Business Cybersecurity Ask-Me-Anything. Register at www.sbir.gov/events