Zivko Aeronautics, Inc. Supplier Cyber Regulatory Awareness

Cyber FAR & DFARS Requirements and CMMC

July 2024

POC: Katherine Lindley

k.lindley@zivko.com

Security Environment

- Increasing frequency, sophistication of cyber attacks
  - Can result in business disruption
  - Can result in the loss of Confidentiality and/or Integrity or Availability of data including your own, ours or governments.
- Loss of unclassified military technology and defense information can be put at risk
  - National security
  - Competitive technological advantage
  - US and allied warfighters
- DoD contractors and suppliers need to harden and make resilient unclassified systems
- New mandatory cyber regulations requiring:
  - Tighter security controls
  - Increased cyber incident reporting

Not Theoretical

"OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought" The Washington Post

600 million Samsung Galaxy phones were discovered to have a major security flaw is more than a bit unsettling. According to the cyber-security firm NowSecure, the Samsung flaw originated with one of its software suppliers.

http://www.forbes.com/sites/paulmartyn/2015/06/23/risky-business-cyber-security-and-supply-chain-management/#4aa24c70723b

In its publication, "Gazing into the Cyber Security Future: 20 Predictions for 2015," FireEye analysts predicted that cyber risks through the supply chain would only increase. Its advice to business:.. require suppliers to show evidence of good security controls…

"Target cyber breach hits 40 million payment cards at holiday peak" - Reuters

Broad Mandatory Requirements at all Tiers

Government is leveraging industrial base/supply chain to protect data by applying cyber controls on supply base networks at all tiers

- What is the FAR? USG Acquisition Statutory Requirements
- What is the DFARS? US Department of Defense Supplemental Requirements
- What is NIST SP 800-171? National Institute of Standards and Technology Special Publication

FAR 52.204-21 Basic Safeguarding Of Contractor Information Systems Reqts.

- Applies to all federal contracts and subcontracts at any tier (except those for COTS products) and requires basic safeguarding of contractor systems that contain ***Federal Contract Information***
  - Very broad definition likely to cover many companies.
  - Information, not intended for public release, provided by or generated for the Government, but not public information or transactional information, such as that necessary to process payments.
    - No implementation period, compliance required upon award
- Mandatory flow-down at all tiers
- Imposes 15 requirements that correlate to 17 NIST 800-171 security controls (limited subset)
- No incident reporting requirement

52.204-21 Basic Safeguarding of Covered Contractor Information Systems.

Basic Safeguarding of Covered Contractor Information Systems (Nov 2021)

(a) Definitions. As used in this clause—

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information systems.

(b) 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:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(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.

(c) Subcontracts. 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 products or commercial services, 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.

(End of clause)

DFARS Clause 252.204-7012 Safeguarding CDI and Cyber Incident Reporting

- Applies to all DoD contracts/subcontracts (except if solicitation is solely for COTS) and requires enhanced safeguarding of covered contractor information systems that contain *Covered Defense Information (CDI)*

- Mandatory flow down of clause in all subcontracts at all tiers for operationally critical support or for which subcontract performance will involve a covered system with CDI

- *Applies to cloud computing; If the Cloud Service Provider (CSP) is a subcontractor, then clause 7012 would flow down, otherwise, CSP with CDI* complies with requirements in paragraphs (c) through (g) of the clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

DFARS Clause 252.204-7012 Safeguarding CDI and Cyber Incident Reporting (cont'd)

- Must provide adequate security for covered internal systems with Covered Defense Information(CDI)
  - At a minimum must comply with all NIST 800-171 security controls (110 controls) to Reach Level 2 of CMMC.

- No third-party certification authority is recognized by DoD as of July 2024

DFARS Clause 252.204-7012 Safeguarding CDI and Cyber Incident Reporting (cont'd)

- In addition to security controls, contractors and subcontractors must report cyber incidents on covered contractor information systems with CDI, or that affect the contractor's ability to perform operationally critical support under a contract
  - Upon discovery must conduct a review for evidence of compromise
  - Rapidly report within 72 hours directly to DoD via specified online portal
  - Must provide DoD-assigned incident report number to prime/higher tiered subcontractor
  - Must preserve and protect images of known affected images and systems for 90 days
  - Must provide DoD access to additional information or equipment necessary to conduct forensics analysis
  - Must submit any malicious software uncovered to DC3, not the Contracting Officer

Key Changes in October 2016 Final Rule

- COTS exemption (does not extend to commercial items)
- Clarifies the definition of “operationally critical support”
- Contemplates that primes and higher tiered subcontractors may consult with contracting officer for guidance as to whether the clause needs to be flowed down
- Subs are required to notify higher tiered subcontractor or prime of requests for alternative but equally effective solutions
- Incident report ID Numbers must be provided to next higher tier subcontractor or prime
- Expands the definition of CDI, including items required on the CUI Registry

What is CDI?

"**Covered Defense Information**" (CDI) is unclassified information that:

- Covered contractor information system" means an **[unclassified]** information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

"Covered defense information" means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, and is—

- (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in the performance of the contract; or

- (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract

Note: Rules Focus on protecting systems with CDI not just the specific information.

Protect CDI
NIST SP 800-171 Security Control Families

- Access Control
- Awareness & Training
- Audit & Accountability
- Configuration Management
- Identification & Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity

ist Numb	Control Family	NIST SP 800-171 CUI Security Requirement	NIST SP 800-53 Relevant Security Controls	NIST SP 800-171 Security Description	Company Status Ov
1	Access Control	3.1.1	AC-2, AC-3, AC-17	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	
2	Access Control	3.1.2	AC-2, AC-3, AC-17	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	
3	Access Control	3.1.3	AC-4	Control the flow of CUI in accordance with approved authorizations.	
4	Access Control	3.1.4	AC-5	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	
5	Access Control	3.1.5	AC-6, AC-6(1), AC-6(5)	Employ the principle of least privilege, including for specific security functions and privileged accounts.	

DFARS 252.204-7012 Safeguarding CDI & Cyber Incident Reporting

- "**Cyber incident**" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on a Covered Contractor information system and/or the CDI residing on that system (this requirement is currently in effect)
- **Contractor shall rapidly report (i.e., within 72 hours of discovery):**
  - Directly to DoD at http://dibnet.dod.mil, **AND**
  - Provide incident number to Prime Contractor or next higher-tier Subcontractor
  - Must obtain & install medium level assurance cert before you have an event so you can report per the rule
- **In addition, Contractor shall:**
  - Conduct a review for evidence of compromise
  - Submit any related malicious software
  - Preserve and protect images of all known affected information systems
  - Upon request, provide:
    - access to conduct a forensic analysis
    - all of the related damage assessment information gathered

DFARS 252.204-7012 Flow-down to suppliers

- **ZAI will include mandatory flow-down clause in solicitations, POs and Subcontracts supporting all DFARS-applicable contracts**
  - Clause is ‘self-deleting’ if subcontractor/supplier’s system does not meet the definition of “covered contractor information system”
  - COTS Suppliers are exempted

- **Specifically applies to subcontractors who**
  - Provide “operationally critical support”, and/or whose
  - Work involves “covered contractor information systems”
- **All subcontractors currently must:**
  - Provide adequate security,
  - Report any NIST 800-171 gaps to the DoD CIO within 30 days of award, and
  - Sign up to DIBNet to facilitate reporting.
  - Full compliance to NIST Standard

What do you need to do?

Engage your Business

- **Start now** (if you haven't already)
- **Read the FAR, DFARS and NIST SP 800-171 (current Rev.)**
- **Complete assessment**
- **Work across functions**
  - IT, Info Security, Contracts, Supply Chain, *(Engineering, Quality)*
- **Designate Business Point of Contact**
  - Coordinate collection of existing practices, tools, standards
  - Lead cross-org analysis of requirements, gaps in compliance, review of new standards

Primary Resources & Links

Copy these links to your browser.

- FAR:
  https://www.acquisition.gov/browse/index/far
- DFARS:
  https://www.acquisition.gov/dfars
- NIST SP 800-171r3:
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf
- Cybersecurity Maturity Model Certification (CMMC):
  https://dodcio.defense.gov/CMMC/
- CUI Registry: **http://www.archives.gov/cui/registry/category-list.html**
- DoD's Defense Industrial Base (DIB) Cyber Incident Reporting **(Register Now):**
  http://dibnet.dod.mil.
- DoD CIA 30 Day Notice**:** **osd.dibcsia@mail.mil**

Additional Cyber Resources

- Council of Defense & Space Industry Association (CODSIA): http://www.codsia.org/
- DoD Cyber Security Strategy: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
- DHS' Stop Think Connect cyber resource page for small businesses https://www.dhs.gov/publication/stopthinkconnect-small-business-resources
- Federal Communications Commission (FCC), in collaboration with other government agencies and industry leaders, created the Small Biz Cyber Planner - an easy-to-use, free online tool that will help you create a customized planning guide to protect your business from cybersecurity threats.
- FTC's Start with Security: A Guide for Business
  This guide developed by the Federal Trade Commission offers10 practical lessons businesses can learn from the FTC's 50+ data security settlements. Visit https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business to download the guide, access videos, and more.
- NIST Manufacturing Extension Partnership (MEP): www.NIST.gov/MEP/
- Federal Bureau of Investigation: www.fbi.gov
- NIST Cybersecurity Resources for Manufacturers: https://www.nist.gov/mep/cybersecurity-resources-manufacturers

Acronyms

- CDI – Covered Defense Information
- CMMC - Cybersecurity Maturity Model Certification
- CUI - Controlled Unclassified Information
- FCI - Federal Contract Information
- NIST – National Institute of Standards and Technology
- FAR – Federal Acquisition Regulations
- DFARS – Defense Federal Acquisition Regulation Supplement
- POA&M – Plan of Action and Milestones


ZAi
Zivko
Aeronautics
Inc.
™