# Cybersecurity, NIST 800-171, and DFARS Interim Rules

Utah Governor's Office of Economic Development
PROCUREMENT TECHNICAL ASSISTANCE CENTER


THOMAS A GERKE
PTAC Regional Manager
801-863-8713
tgerke@utah.gov

# Quick Look –Good News

- With the interim rules, DoD is phasing in the rollout of CMMC. All contracts over the micro-purchase threshold (except for COTS) will require CMMC certification beginning September 30, 2025. Until then, the DoD, specifically, the Office of the Under Secretary of Defense for Acquisition and Sustainment, will decide which solicitations will include the CMMC requirement and the new associated DFARS clause at 252.204-7021, Cybersecurity Maturity Model Certification Requirements.
- However, **starting 1 Dec 2020**, DFARS 252.204-7019 requires reporting your cybersecurity readiness in the the Supplier Performance Risk System (SPRS)
- DFARS 7019 Is appicable to all DoD contracts.

# Projected CMMC Rollout

- **OUSD(A&S) is working with Services and Agencies to identify candidate programs that will have the CMMC requirement during FY21-FY25 phased roll-out**

| Total Number of New Prime Contracts Awarded Each Year with CMMC Requirement | | | | |
|---|---|---|---|---|
| FY21 | FY22 | FY23 | FY24 | FY25 |
| 15 | 75 | 250 | 479 | 479 |

| | Total Number of Prime Contractors and Sub-Contractors with CMMC Requirement | | | | |
|---|---|---|---|---|---|
| | FY21 | FY22 | FY23 | FY24 | FY25 |
| Level 1 | 899 | 4,490 | 14,981 | 28,714 | 28,709 |
| Level 2 | 149 | 749 | 2,497 | 4,786 | 4,785 |
| Level 3 | 452 | 2,245 | 7,490 | 14,357 | 14,355 |
| Level 4 | 0 | 8 | 16 | 24 | 28 |
| Level 5 | 0 | 8 | 16 | 24 | 28 |
| Total | 1,500 | 7,500 | 25,000 | 47,905 | 47,905 |

- **All new DoD contracts will contain the CMMC requirement starting in FY26**
- **Assumes for every unique prime contractor, there are ~ 100 unique subcontractors**

# CMMC Rollout Breakout

- **Total number of unique DoD contractors and subcontractors is 220,966**
  - The total number of unique DoD contractors and subcontractors with a new CMMC certification requirement achieves a steady state of 47,905 by Year 4
  - Completed CMMC assessments on all total 220, 966 unique DoD contractors and subcontractors is achieved in Year 7; as a result, the number of unique DoD contractors and subcontractors that require a new CMMC certification is only 43,251 for Year 7

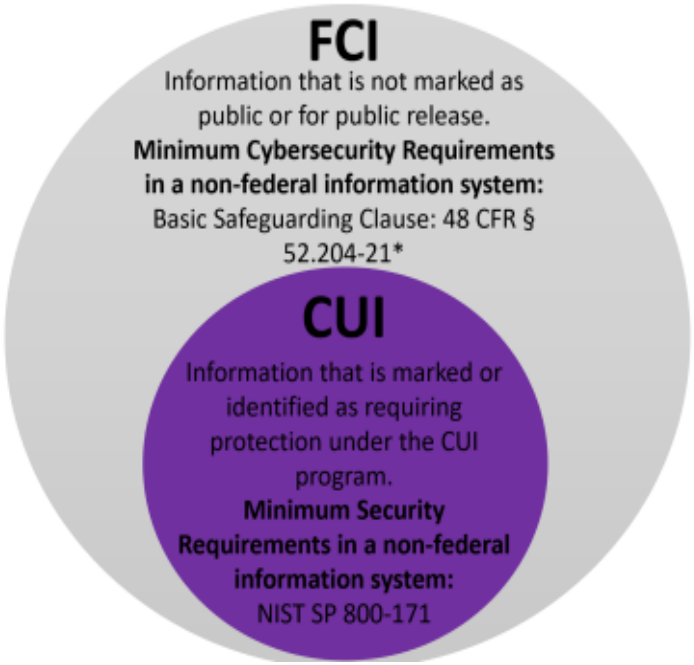
- **Phased rollout assumes the following percentages of DoD contractors and subcontractors require a CMMC certificate at each level:**
  - Level 1: approximately 60%
  - Level 2: approximately 10%
  - Level 3: approximately 30%
  - Level 4: approximately 0.06%
  - Level 5: approximately 0.06%

# Overview

- The DoD IG conducted a series of contractor audits and concluded that some DoD contractors were not consistently implementing mandated system security requirements or advancing their POA&Ms to achieve full compliance with all 110 security controls.
- Because of these identified shortcomings DoD has developed a two-pronged approach to assess and verify the ability of contractors to protect the controlled unclassified information (CUI) on their information systems.
- Those two prongs are: (1) compliance assessment using the NIST 800-171 DoD Assessment Methodology in the near term, and (2) certification under the CMMC Framework as a longer term remediation.

# Another Way of Looking at It

**Information that is collected, created, or received pursuant to a government contract**





*also excludes simple transactional information.

# DFARS 252.204-7012

- **Safeguarding Covered Defense Information and Cyber Incident Reporting,**

- This clause requires contractors to provide “adequate security” for covered defense information that is processed, stored, or transmitted on the contractor’s internal information system or network.

- The Department must mark, or otherwise identify in the contract, any covered defense information that is provided to the contractor, and must ensure that the contract includes the requirement for the contractor to mark covered defense information developed in performance of the contract.

- To provide adequate security, the contractor must, at a minimum, implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800- 171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,” not later than December 31, 2017.

# Interim Rules

- **DFARS clause 252.204-7019 (crawl phase):** *"The new DFARS provision 252.204-7019 advises offerors required to implement the NIST SP 800-171 standards of the requirement to have a current (not older than three years) NIST SP 800-171 DoD Assessment on record in order to be considered for award."* To take the NIST SP 800-171 assessment on the Project Spectrum website, log in or register for a free account.

- **DFARS clause 252.204-7020 (walk phase):** *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."*

- **DFARS clause 252.204-7021 (run phase):** *A new DFARS clause 252.204-7021, Cybersecurity Maturity Model Certification Requirements, is prescribed for use in all solicitations and contracts or task orders or delivery orders, excluding those exclusively for the acquisition of COTS items. This DFARS clause requires a contractor to: Maintain the requisite CMMC level for the duration of the contract; ensure that its subcontractors also have the appropriate CMMC level prior to awarding a subcontract or other contractual instruments; and include the requirements of the clause in all subcontracts or other contractual instruments."*

# DFARS 252.204-7019

- **Notice of NIST SP 800-171 DoD Assessment Requirements.**

- The Offeror shall verify that summary level scores of a current NIST SP 800-171 DoD Assessment (*i.e.,* not more than 3 years old unless a lesser time is specified in the solicitation) are posted in the Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*) for all covered contractor information systems relevant to the offer.

- This clause walks contractors through the logistics for performing and reporting a Basic DoD Assessment. As part of the process, each contractor must supply the following information with respect to each system being assessed: system security plan name, CAGE code, brief description of plan architecture, date of assessment, total score, and date that a score of 110 will be achieved.

# DFARS 252.204-7020

- **DFARS 252.204-7020 NIST SP 800-171 DoD Assessment Requirements**
- The clause 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.

*https://beta.sam.gov/help/new-to-sam*

# Flow Down Requirements

- DFARS 252.204-7019 does not contain a flow down provision, but the substance of DFARS 252.204-7020 must be flowed down to all subcontractors (except COTS suppliers). The clause further directs that prime contractors are required to ensure that applicable subcontractors (i.e., those that must meet NIST SP 800-171 requirements) have a current DoD Assessment posted in SPRS.

# Supplier Performance Risk System (SPRS)

- Supplier Performance Risk System (SPRS) "…is the authoritative source to retrieve supplier and product PI [performance information] assessments for the DoD [Department of Defense] acquisition community to use in identifying, assessing, and monitoring unclassified performance." (DoDI 5000.79)
  - https://www.sprs.csd.disa.mil/
- Login/Register via PIEE
  - https://piee.eb.mil/piee-landing/

# Excerpts from the Quick Entry Guide

- https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf
- A “SPRS Cyber Vendor Role” is required to enter Basic Assessment information.
  - There is an *SPRS Icon* after you log on
  - Then select the *NIST 800-171 Assessment* link

# The Basic Assessment

- To submit the Basic Assessment, contractors must complete 6 fields:
  - System security plan name (if more than one system is involved)
  - CAGE code associated with the plan
  - Brief description of the plan architecture
  - Date of the assessment
  - Total score
  - Date a score of 110 will be achieved
- To comply with NIST SP 800-171 a company must:
  - implement 110 security requirements on their covered contractor information systems; or
  - Document in a “system security plan” and “plans of action” those requirements that are not yet implemented and when the requirements will be implemented.
  - Complete a Basic Assessment and upload the resulting score (SPRS)-.
  - 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.

# Plan of Action and Milestones (POAMS)

- 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)

# The Assessment

- https://www.projectspectrum.io/#!/
- **CMMC Level 1 Controls**
  - Access **Control** (AC)
  - Identification and Authentication (IA)
  - Media Protection (MP)
  - Physical Protection (PE)
  - System and Communications Protection (SC)
  - System and Information Integrity (SI)

# Access Control

- **AC.1.001:** Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
  - What to do?: Use password/PIN protection on all devices and systems
- **AC.1.002:** Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
  - What to do?: Controlled user rights, i.e proper use of admin privileges etc.
- **AC.1.003:** Verify and control/limit connections to and use of external information systems.
  - What to do?: Use organizational wifi/connectivity only (no public or unauthorized)
- **AC.1.004:** Control information posted or processed on publicly accessible information systems.
  - What to do?: Limit sharing capabilities and use password protection on things like cloud services.

# Identification and Authentication

- **IA.1.076:** Identify information system users, processes acting on behalf of users, or devices.
  - What to do?: Don't allow password sharing and create individual accounts for all personnel.
- **IA.1.077:** Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
  - What to do?: Change default passwords and ensure all devices mobile, desktop, etc. are all password protected.

# Media Protection

- **MP.1.118:** Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
- What to do? Shred any physical documents that are no longer of use, or perform multiple data erasures before disposing of it.

# Physical Protection

- **PE.1.131:** Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
  - What to do?: Designate public and private areas within the organization, where devices are only accessible to authorized personnel.
- **PE.1.132:** Escort visitors and monitor visitor activity.
- **PE.1.133:** Maintain audit logs of physical access.
  - What to do?: Use sign in, sign out sheets for employees, or a keycard system that can log physical access to the building, also use of CCTV is encouraged.
- **PE.1.134:** Control and manage physical access devices.
  - What to do?: restrict the amount of personnel that can unlock areas or disable security parameters (such as CCTV or electronic locks).

# Systems & Communication Protection

- **SC.1.175:** Monitor, control, and protect organizational communications (What to do?: information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
  - What to do?: Ensure that firewalls block traffic from the internet by default, and that all devices and terminals of the organization fall within the boundaries of the firewall.
- **SC.1.176:** Implement sub-networks for publicly accessible system components that are physically or logically separated from internal networks.
  - What to do?: SMEs or an organization with limited resources should not attempt to run their servers that are directly connected to the internet. Web hosting should be done through a hosting company with integrated security.

# System and Information Integrity

- **SI.1.210:** Identity, report, and correct information and information system flaws in a timely manner.
  - What to do?: *Update, update, update*. Ensuring the organization updates systems with the latest patches, the organization could also enable an auto-updater for devices and operating systems to limit the possibility for hackers to exploit outdated devices and systems. It is also necessary to remove apps that are no longer being supported by the vendors.
- **SI.1.211:** Provide protection from malicious code at appropriate locations within organizational information systems.
  - What to do?: Ensure that all computers on the network have antivirus installed, preferably from a reputable source. Utilize emailing platforms that have inbuilt virus removal, such as Office 365. Given the company resources, it may also be useful to use routers that have threat detection capabilities.
- **SI.1.212:** Update malicious code protection mechanisms when new releases are available.
  - What to do?: Ensure that the antivirus and firewalls are eligible for updates. This is usually available through paid services and reputable antivirus/anti-malware etc. software.
- **SI.1.213:** Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
  - What to do?: Enable virus scanning capabilities on antivirus software and ensure the scans are run frequently enough (weekly).

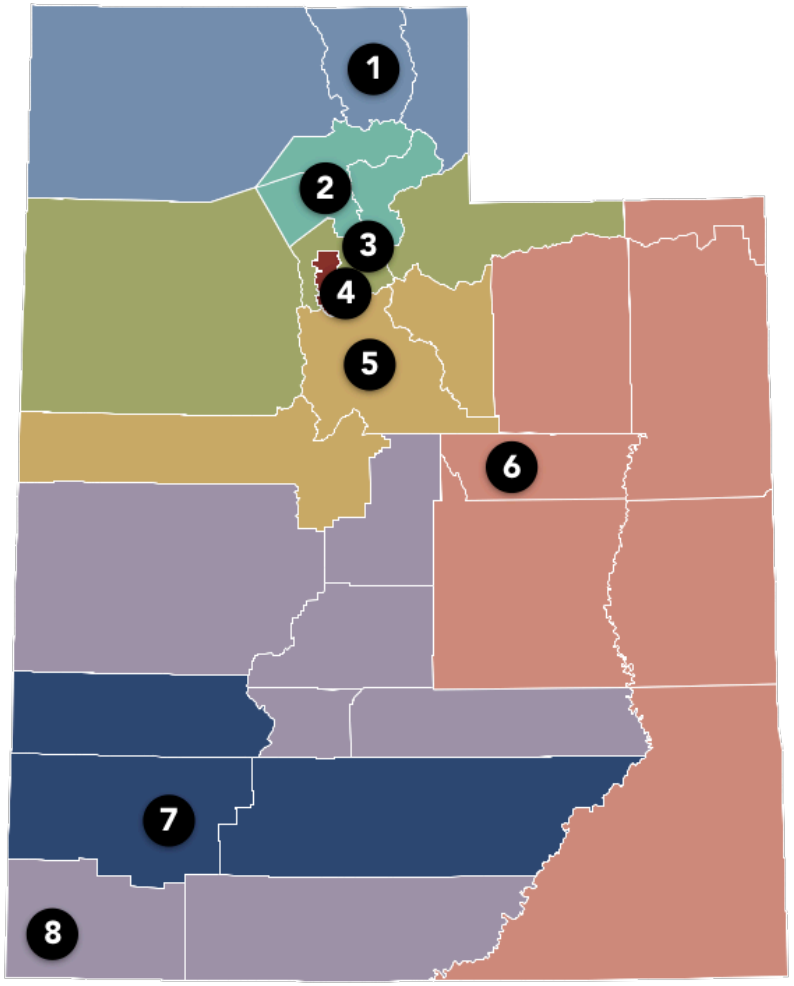
# Now What

- ***Select someone within your company to drive the effort***
- Review and complete the .pdf checklist provided by Spectrum.io
- Review NIST Handbook 162
  - https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf
  - NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements
  - **https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%206.24.2020.pdf**
- Go to https://projectspectrum.io/#!/assessment
- Select the NIST 800-171 Compliance Tool
- Complete the on-line assessment
- At this point you can upload your answers into the SPRS

# Submitting Your Assessment

- The interim rule (DFARS clause 252.204-7019 and 252.204-7020) currently states that the Offeror/Contractor may submit, via encrypted email, summary level scores of Basic Assessments conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology to webptsmh@navy.mil (email address) for posting to the Supplier Performance Risk System (SPRS)
- • SPRS now has increased functionality for Offerors/Contractors to enter scores directly – The NIST SP 800-171 DoD Assessment Methodology, posted at https://www.acq.osd.mil/dpap/pdi/cyber/index.html, states that "A contractor may post the results of their Basic Assessments… In SPRS (via the Procurement Integrated Enterprise Environment (PIEE))."
- A link to a Quick Entry Guide for entering assessment scores can be found at the SPRS homepage

# PTAC Regional Managers




| | |
|---|---|
| **1: Mark Alexander**<br>mark.cbrc@btech.edu<br>435-750-3261 | **2: Mary Ann Flinders**<br>mflinders@utah.gov<br>801-593-2242 |
| **3: Paula Kramer**<br>pkramer@utah.gov<br>801-538-8756 | **4: Alex Quayson-Sackey**<br>aquayson@utah.gov<br>801-957-5357 |
| **5: Thomas Gerke**<br>tgerke@utah.gov<br>801-863-8713 | **6: Jack Schons**<br>jschons@utah.gov<br>435-613-5198 |
| **7: Joni Anderson**<br>andersonjoni@suu.edu<br>435-586-8883 | **8: Cam Findlay**<br>findlay@utah.gov<br>435-652-7754 |

# Recap

- **To comply with NIST SP 800–171 a company must:**

– Implement 110 security requirements on their covered contractor information systems; or

– Document in a "system security plan" and "plans of action" those requirements that are not yet implemented and when the requirements will be implemented

- **Basic Assessment is a self-assessment done by the contractor using a specific scoring methodology**
  - Tells the DoD how many security requirements have not yet been implemented
  - Is valid for three years
- **All offerors that are required to implement NIST SP 800–171 per DFARS clause 252.204–7012, will be required to complete a Basic Assessment and upload the resulting score into SPRS . To submit the Basic Assessment, contractors must complete 6 fields:**
  - System security plan name (if more than one system is involved)
  - CAGE code associated with the plan
  - Brief description of the plan architecture
  - Date of the assessment
  - Total score
  - Date a score of 110 will be achieved

# My Contact Information


- Thomas A. Gerke

- Regional Manager
  Procurement Technical Assistance Center - PTAC
  Governor's Office of Economic Development
  Utah Valley University Business Resource Center

- Office: 801.863.8713
- Mobile: 801.815.7463

- tgerke@utah.gov

# Questions