CyberNINES
COMPLIANCE WITHOUT COMPLEXITY™

DoD Interim Final Rule

Scott Singer

9 December 2020

CyberNINES
COMPLIANCE WITHOUT COMPLEXITY™

OVERVIEW

- CyberNINES was created in 2020 as a spinoff of 5NINES cybersecurity group
- We are focused on addressing the complexity, cost and time associated with NIST SP 800-171 compliance and now CMMC
- CyberNINES is the preferred cybersecurity partner for all of 5NINES client's needs
- CyberNINES is a CMMC Registered Provider Organization (RPO) and registered to be a Certified 3rd Party Assessor Organization (C3PAO) Organization

Scott Singer

President, CyberNINES

Scott provides expert DOD experience on IT security from both his 25+ years of military and civilian experience. Most recently he was the CIO at PaR Systems, Minneapolis, since 2010. Scott has in-depth experience with information systems, cyber security, NIST compliance, global quality, export control, and continuous process improvement.

SOME BACKGROUND

CUI (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

  Examples:

  - ITAR (US Persons only)
  - EAR (It depends)
  - UCNI (Unclassified Controlled Nuclear Information) (US Citizens only)
  - FCI (Federal Contract Information)
    - Information developed under contract

3 NEW DFARS

(DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT

- Current Cybersecurity Protections Requirement
  - DFARS Clause 25.204-7012 since 31 DEC 2017, requires compliance through self-attestation
- Interim Rule 85 FR 61505, published on 29 SEP 2020
  - DFARS Provision 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements
  - DFARS Clause 252.204-7020, NIST SP 800-171 DoD Assessment Requirements
  - DFARS Clause 252.204-7021, Cybersecurity Maturity Model Certification Requirements
- Public comment period ends on 30 NOV 2020

INTERIM FINAL RULE

The Interim Final Rule was released on 29 September 2020 for public comment and went into effect on 30 November 2020. The rule is not retroactive to existing contracts and will only impact new contracts.

The rule creates two assessment frameworks:

- NIST SP 800-171 Assessment Methodology
- Cybersecurity Maturity Model Certification (CMMC) Framework

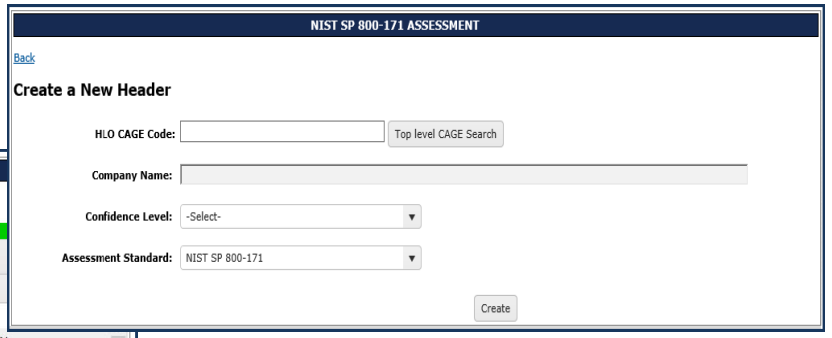
NIST SP 800-171 ASSESSMENT METHODOLOGY CHANGES

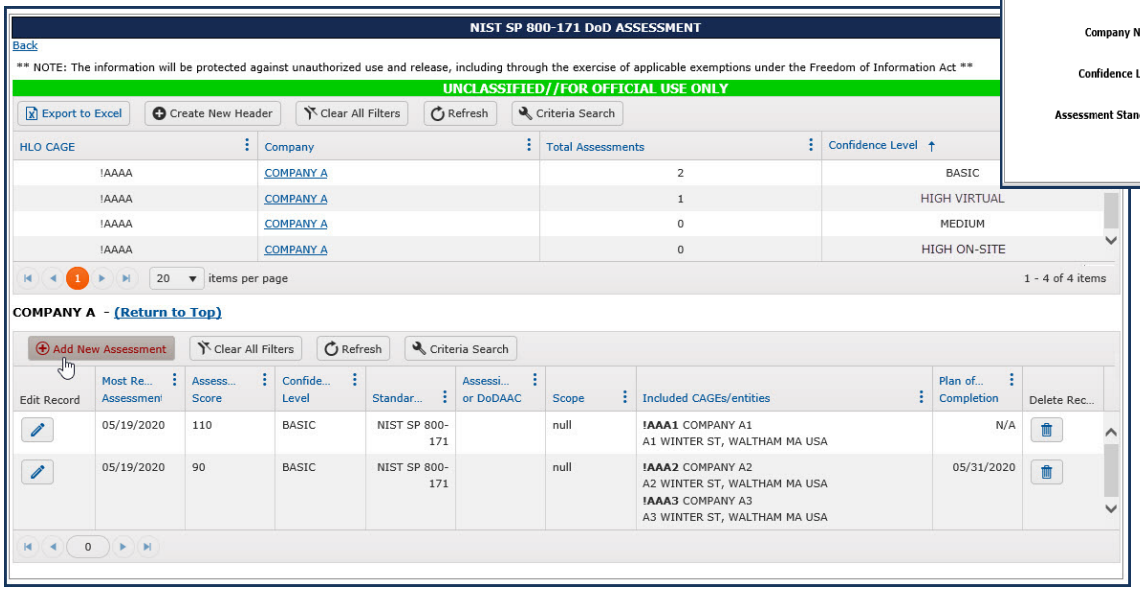
- All new contracts and contract flow downs will need to meet these changes
- The rule will require both primes and sub-contractors to submit their score from an assessment to the Supplier Performance Risk System (SPRS) at https://www.sprs.csd.disa.mil/
- The assessment must not be more than three years old before contract acceptance or sub-contractor acceptance of a flowed down requirement
- In addition, the DoD will classify you as needing either a Basic, Medium or High Assessment
- DCMA (Defense Contract Management Agency) will conduct a small number of audits in Medium or High assessments

CyberNINES
COMPLIANCE WITHOUT COMPLEXITY™

SPRS (PRONOUNCED SPURS)

- Make sure you have a sam.gov account setup with a DUNS number and CAGE code. Make sure you have designated a contract administer.
- Create an account in the Procurement Integrated Enterprise Environment (PIEE) in order to gain access to SPRS to post your score.



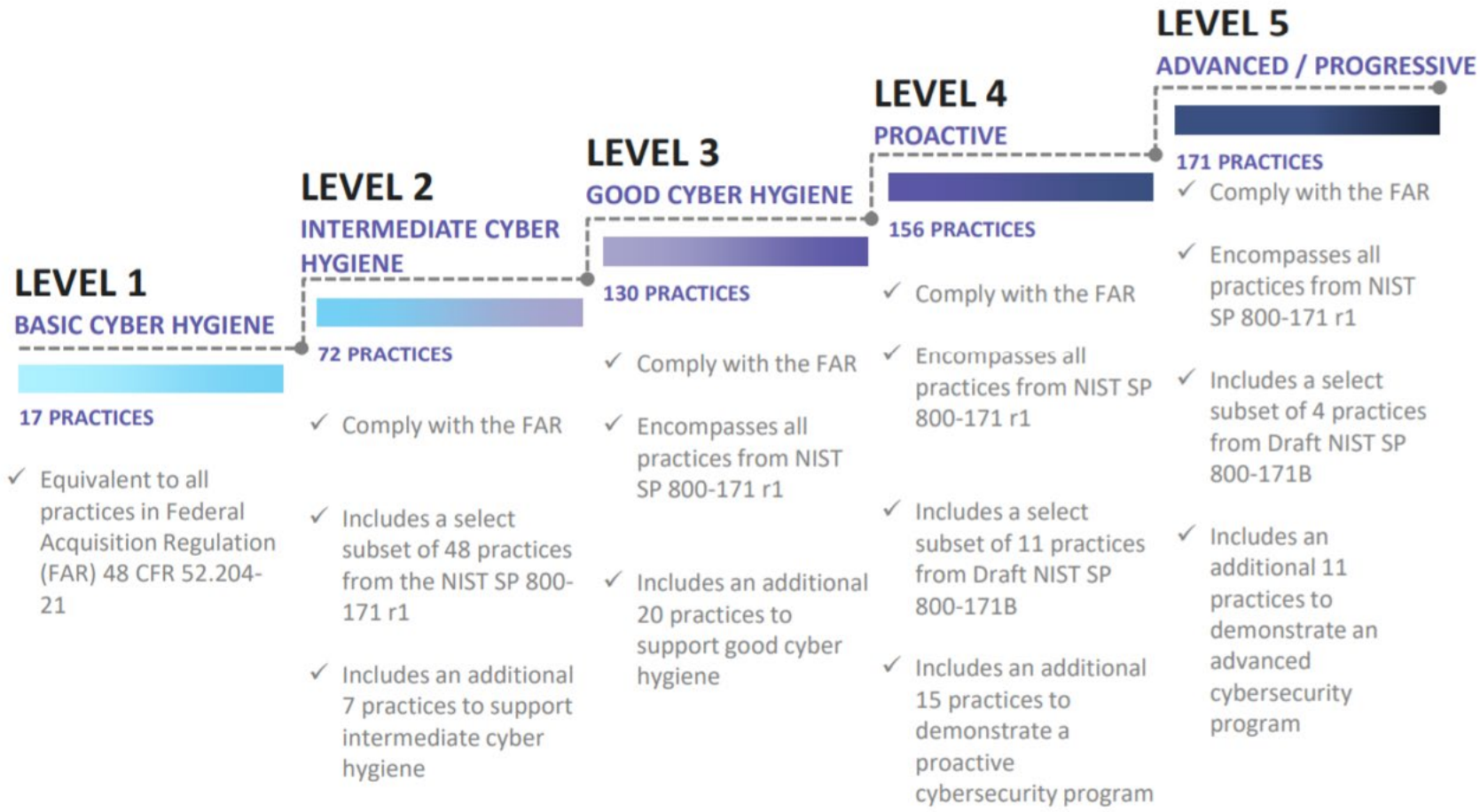


NEW CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) FRAMEWORK

- CMMC roll-out will be phased over five years
- Only the DoD can add CMMC DFARS to a new contract, 15 for next FY
- After 01 October 2025, all new contracts will be required to meet the CMMC framework
- The key difference between the current DFAR 7012 and DFAR 7021 is that DFAR 7012 allows for self-attestation while DFAR 7021 will require a third part audit
- The third-party audit will be conducted by accredited C3PAOs (Certified 3rd Party Assessment Organizations)
- Level 1 required for contractors handling FCI (Federal Contract Information)
- Level 3 required for contractors handling CUI (Controlled Unclassified Information, think ITAR and 600 Series)

CyberNINES
COMPLIANCE WITHOUT COMPLEXITY™

CYBERSECURITY MATURITY MODEL CERTIFICATION CMMC



CyberNINES
COMPLIANCE WITHOUT COMPLEXITY™

Please send your questions to:
info@cybernines.com

Thank you!
www.cybernines.com