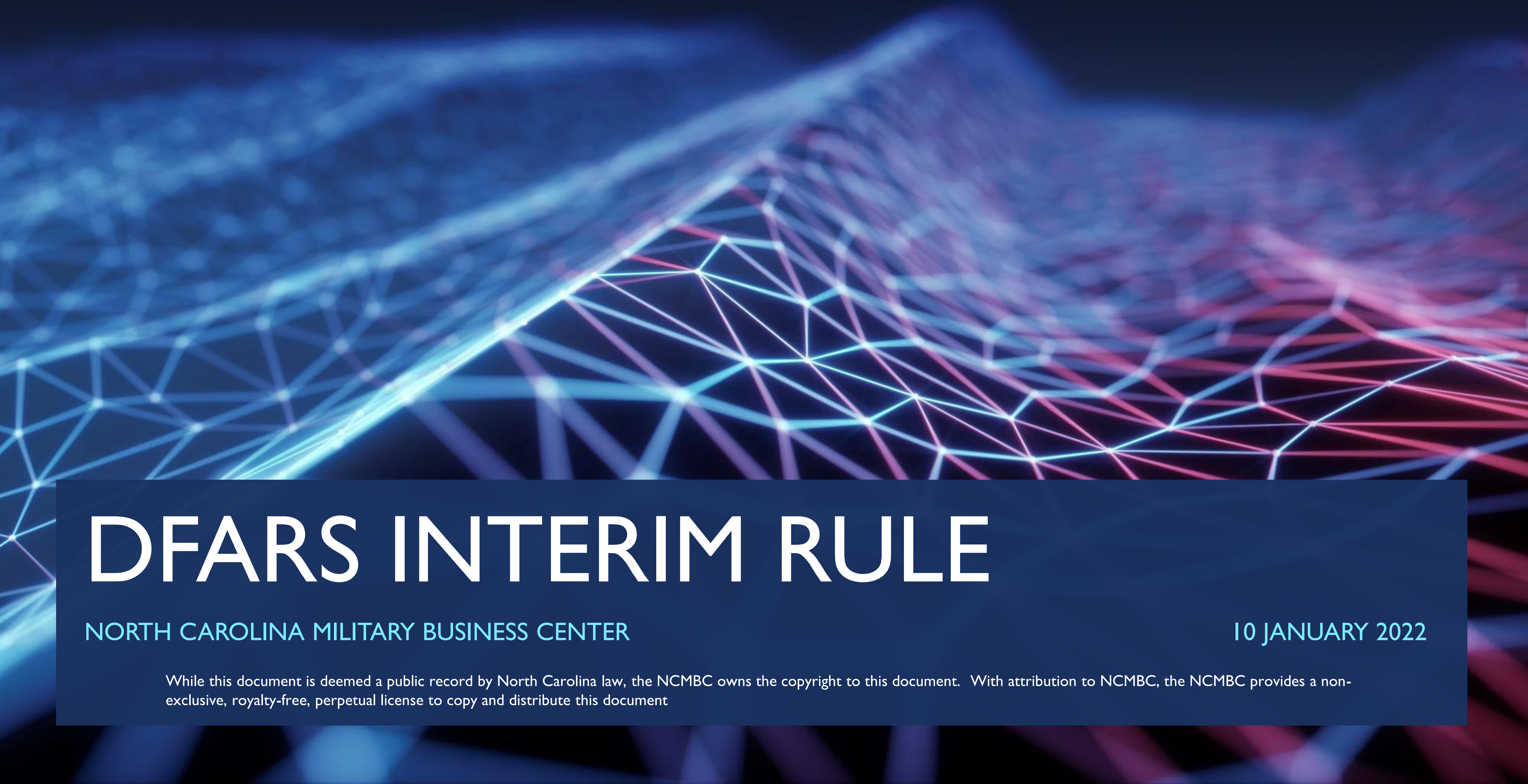


DFARS INTERIM RULE

NORTH CAROLINA MILITARY BUSINESS CENTER

10 JANUARY 2022

DFARS INTERIM RULE - DEFINITIONS

- Defense Federal Acquisition Regulation Supplement (DFARS) – supplement to the Federal Acquisition Regulation that is specific to DoD contracts.
- DFARS 252.204-7012 – cybersecurity regulation requiring that defense contractors self-attest to compliance with NIST SP 800-171 ***if you touch CUI.***
- NIST SP 800-171: National Institute of Standards and Technology Special Publication that contains 110 cybersecurity controls.
- DFARS Interim Rule Case 2019-D-041 – amends the DFARS to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification to enhance the protection of unclassified information in the DoD supply chain. Effective Date: 30 Nov 2020

DFARS INTERIM RULE - DEFINITIONS

- DoD Assessment Methodology
  - Documents a standard methodology that enables a strategic assessment of a contractor's implementation of NIST SP 800-171, a requirement for compliance with DFARS clause 252.204-7012.
  - Consists of three levels of assessments: Basic (self-assessment), Medium and High
  - Provides a scoring methodology – each of the 110 controls in NIST SP 800-171 have been assigned a score of 5, 3 or 1.
- Supplier Performance Risk System (SPRS) - a web-enabled enterprise application that gathers, processes, and displays data about supplier performance.

DFARS INTERIM RULE

- Directs contracting officers to verify in the Supplier Performance Risk System (SPRS) that a company has a current assessment on record prior to contract award (for companies that have DFARS 252.204-7012 in their contracts AND touch CUI).
- Adds DFARS 252.204-7019 and DFARS 252.204-7020 - directs contracting officers to add these 2 new clauses to contracts.
- Adds DFARS 252.204-7021 - CMMC (not applicable until the rule-making process is complete for CMMC 2.0)
- Does NOT apply to strictly COTS items or contracts below the micro-purchase threshold

NEW DFARS CLAUSES

DFARS 252.204-7019

- Requires contractors to perform a self-assessment to NIST SP 800-171 using the DoD Assessment Methodology (DoDAM)
- Results of the self-assessment must be uploaded to the SPRS
- Must have a current (not older than 3 years) Assessment on record in order to be considered for an award

DFARS 252.204-7020

- Requires contractors to provide the Government with access to its facilities, systems and personnel when it is necessary to conduct or renew a medium/high level assessment
- Requires contractors to ensure that applicable subcontractors also have the results of a current Assessment posted in SPRS prior to awarding a subcontract

DFARS 252.204-7021

- Implements the Cybersecurity Maturity Model Certification Framework – CMMC
- This clause will not be valid until the rule-making process for CMMC 2.0 is complete (9 to 24 months).

DOD ASSESSMENT METHODOLOGY - DODAM

Basic Assessment

- Self-assessment to 110 NIST controls
- Use DoDAM to calculate score
- Upload score to SPRS prior to award
- Valid for 3 years
- Confidence level - low

Medium Assessment

- Performed by (DCMA)
- Based on criticality of program and sensitivity of data
- Post-award assessment
- Valid for 3 years
- DoD uploads results to SPRS
- Confidence level – medium

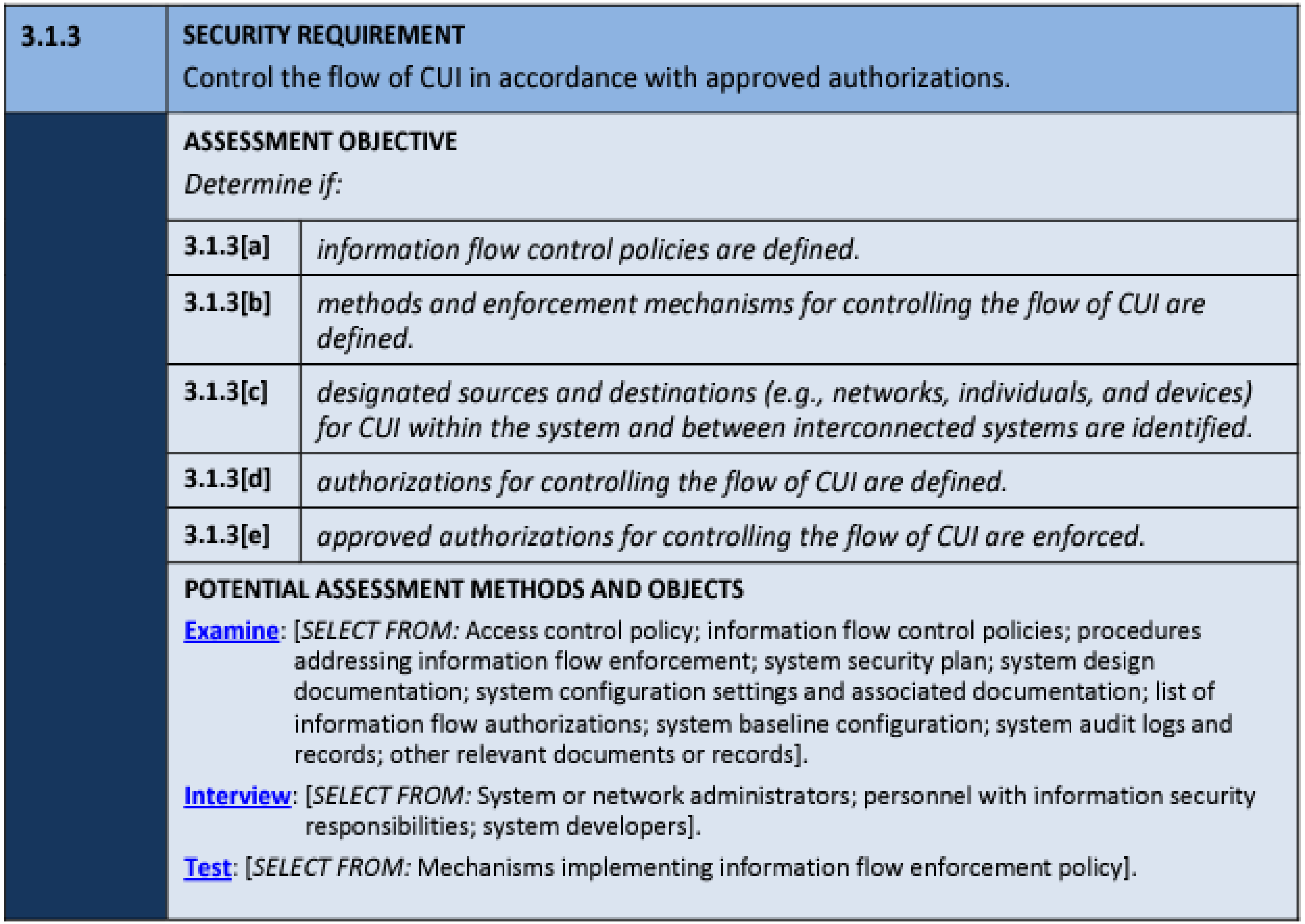
High Assessment

- Performed by (DCMA)
- Based on criticality of program and sensitivity of data
- Post-award assessment
- Valid for 3 years
- DoD uploads results to SPRS
- Confidence level – high

HOW TO PERFORM A SELF-ASSESSMENT

- The self-assessment of your cybersecurity program is performed against the 110 controls in NIST SP 800-171 and must be done using the NIST SP 800-171A Assessment Guide.
- To take credit for implementing control 3.1.3, you must meet each of the 6 assessment objectives and provide proof using at least one of the assessment methods.

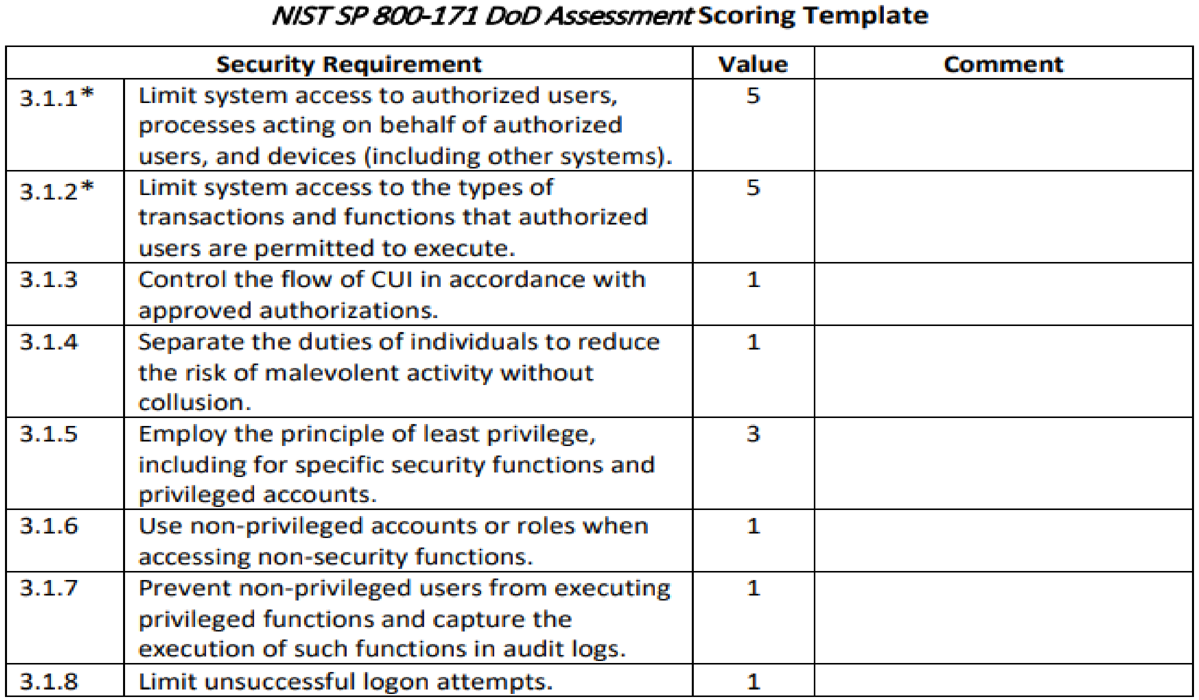
NIST SP 800-171A - Example



3.1.3	**SECURITY REQUIREMENT** Control the flow of CUI in accordance with approved authorizations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.3[a]	*information flow control policies are defined.*
	3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
	3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].	

SELF-ASSESSMENT – HOW TO SCORE

How to Score the Self-Assessment – a perfect score is 110, meaning the contractor has all 110 NIST controls in place. For every control that is not in place, subtract its value from 110 – see below (from the DoDAM).



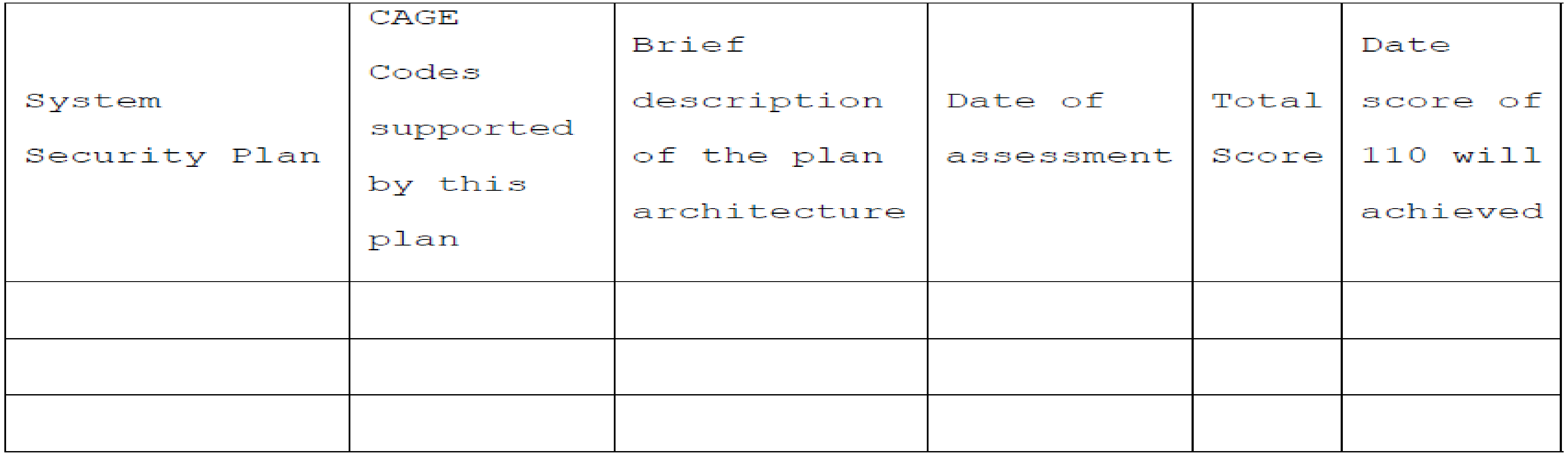
NIST SP 800-171 DoD Assessment **Scoring Template**

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

Example: If my company is not compliant with controls 3.1.1 and 3.1.5, I must subtract 8 points from 110.

SELF-ASSESSMENT - RESULTS

Assessment results uploaded to SPRS are available to DoD personnel only and are protected. The information below must be uploaded to SPRS.



System Security Plan	CAGE Codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total Score	Date score of 110 will achieved

PLAN OF ACTION AND MILESTONES

- For every control that is not in place a Plan of Action and Milestones (POAM) must be developed to show how you plan to implement the control and when the control will be implemented. NOTE: You may not have a POAM for a System Security Plan (SSP). If you don't have an SSP do not upload your score to SPRS – the SSP must be done before calculating your score.
- Description of the architecture – enterprise or enclave.
- The date that a score of 110 will be achieved should be the latest date on your POAMS.
- There has been no guidance on how long a POAM can be open, but it is in the best interest of national security to get your POAMs closed out, so your network is secure.
- Upload a new score to SPRS each time a POAM is closed (closing POAMS means your score will improve)

COMPLIANCE COSTS

- Since the DFARS Interim Rule is based on the NIST controls in DFARS 252.204-7012, which is already in most contracts, the DoD is only considering the cost of the self-assessments to be allowable. In other words, any labor and equipment expenses incurred to achieve compliance to the 110 NIST controls is not considered a billable cost and may not be billed directly to the customer. (roll the costs into your OH rates)
- Contractors do not have to pay the assessors for Medium and High assessments since they are federal government employees.

COMPLIANCE COSTS

- The DFARS Interim Rule - like DFARS 252.204-7012 – is about protecting CUI.
- Implementing a cybersecurity program that is fully compliant with DFARS 7012 is very expensive and complex. ***The best way to avoid the expense and complexity is to avoid CUI. With less CUI being transmitted, the risk to national security is reduced.***
- Work with your contracting officer or prime to discuss ways of eliminating the need to process, store or transmit CUI.
- Primes should not flow down these requirements unless it is absolutely necessary for their subs/suppliers to touch CUI.

RECOMMENDATIONS

1. Review your current contract(s) to see if DFARS 252.204-7012/7019/7020 are referenced. Remember – just because the DFARS clauses are referenced doesn't mean they are applicable. If you don't touch CUI, the clauses are not applicable.
2. If you are unsure about CUI, review the CUI Registry Categories . If you're still unsure, work with your contracting officer. Your KO can send an email to the CUI Executive Agent for the DoD if they need help with CUI - osd.pentagon.ousd-intel-sec.mbx.dod-cui@mail.mil
3. If there is any doubt about CUI in your contract(s), get something in writing from your contracting officer. **CUI = $$ and Risk**
4. Perform a self-assessment to NIST SP 800-171 using the DoDAM and the NIST SP 800-171A assessment guide. The CMMC 2.0 Level 2 in a Box tool can be used to perform your self-assessment and calculate your score.

RECOMMENDATIONS

5. Upload your score to SPRS.
6. Put POAMs in place for each unimplemented control.
7. Begin working to get the POAMs closed out and update your score.

Be wary of consulting companies that over-sell, advertise false and/or misleading information about the DFARS Interim Rule, and/or try to scare you into using their services.

Using a Cloud Service Provider (CSP) will not provide 100% compliance – it is NOT possible. If a company promises 100% compliance, they do not understand the regulations. The defense contractor is responsible for compliance – which means you must thoroughly understand how the services the CSP provides helps maintain compliance and be able to prove it. Insist on a shared compliance matrix from your CSP.

LINKS TO RESOURCES

Links to SPRS, the DoDAM, NIST SP 800-171A and other resources can be found on the cybernc.us website under the DFARS tab.

DFARS INTERIM RULE

NORTH CAROLINA MILITARY BUSINESS CENTER

10 JANUARY 2022