TIME’S UP - ACT NOW

THE NEW DFARS INTERIM RULE

November 30, 2020

Start Here: Basic Cyber Hygiene

FAR Clause: FAR 52.204-21

FAR 52.204–21, "Basic Safeguarding of Covered Contractor Information Systems"

- ➢ Requires application of basic safeguarding requirements when processing, storing, or transmitting Federal Contract Information (FCI) in or from covered contractor information systems
- ➢ *Federal contract information* (FCI) 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.
- ➢ 15 Controls (they cross-map to 15 of the NIST 800-171 controls)
- ➢ Implements what the DoD refers to as "Basic cyber hygiene"

The DFARS Rule

DFARS 252.204-7012

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is required in all contracts except for contracts solely for the acquisition of COTS items

- *Controlled Unclassified Information (CUI)* - Law, regulation or Government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under EO 13526.
  - Classification for CUI Categories listed in NARA archives: https://www.archives.gov/cui/registry/category-list
- Requires defense contractors to provide "adequate security" for covered defense information which "at a minimum" requires contractors to implement 110 Security controls from NIST SP 800-171
- In addition, the contractor should include the clause in subcontracts for which performance will involve covered defense information or operationally critical support
- DFARS Clause 252.204-7012 requires contractors/subcontractors to:
  - Safeguard covered defense information (both in transmission and at rest)
  - Report cyber incidents within 72 hours of discovery
  - Report malicious software
  - Facilitate damage assessment

The Representation

Self-Attestation of Compliance

- DFARS 252.204-7008 *Compliance With Safeguarding Covered Defense Information Controls* is required in every solicitation, except for those solely for the acquisition of commercially available off-the-shelf (COTS) items

- The offeror represents that:

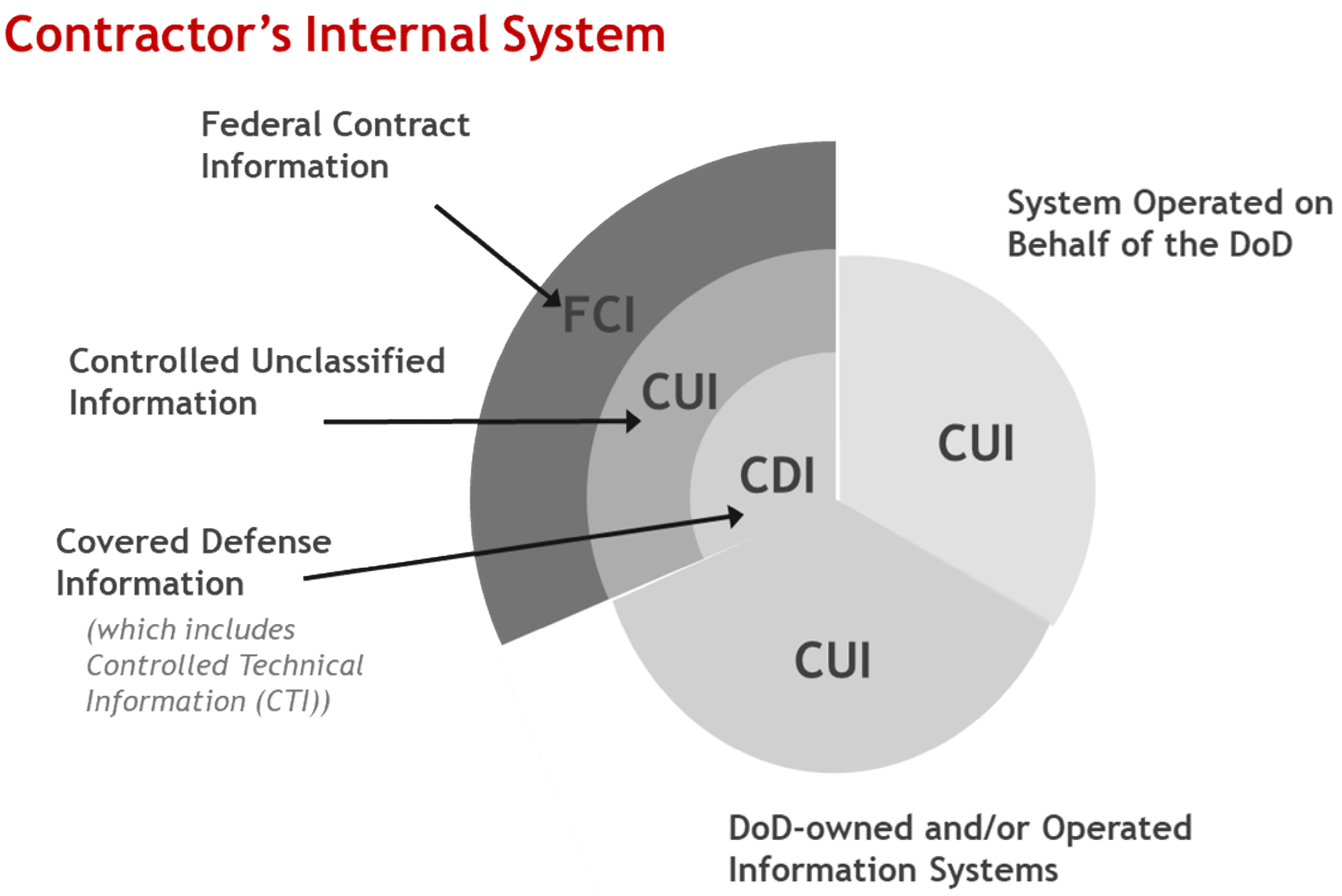
  > *"By submission of this offer, the offeror represents that it will implement the security requirements specified by [NIST SP 800-171] that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017."*

- DoD had interpreted "implementation" of NIST SP 800-171 as having a completed SSP and a PoA&M for the relevant covered contractor information systems.

The “Fork” of FCI and CUI

- The DFARS 7012 clause does not currently require verification of contractors’ implementation of NIST SP 800-171 prior to contract award.
- BOTH FCI and CUI may be:
    1. Provided to the contractor by the Government OR
    2. Developed by the contractor in performance of work under the contract.
- Many contractors erroneously believe that because they do not receive data from the Government marked as CUI, that they claim not to have processed any CUI on-site.
- This may not be true as CUI could be produced on the contractor’s site within normal performance of work products under the contract.
- Consult your Contract Officer for clarification on CUI being received or generated/received on the contractor’s site and/or information systems

Information Being Targeted


Contractor's Internal System
Federal Contract Information
FCI
Controlled Unclassified Information
CUI
Covered Defense Information
(which includes Controlled Technical Information (CTI))
CDI
System Operated on Behalf of the DoD
CUI
CUI
DoD-owned and/or Operated Information Systems

Graphic adapted from https://www.acd.osd.mil/dpap/pdi/p2p%20training%20presentations/Cybersecurity%20Initiatives%20Requirements.pdf

Increased Threats on Contractor Systems

- NIST SP 800-171 and DFARS 7012 were created by DoD to safeguard sensitive data but the DoD has found the -7012 Clause ineffective.
- DoD Inspector General Report DODIG-2019-105 found that DoD contractors did not consistently implement mandatory security for safeguarding CUI
- National threat actors, such as China and Russia, are launching persistent and advanced cyberattacks targeting sensitive data transmitted or stored by the Defense Supply Chain
- Even the lowest level classification of data, in aggregate, can be raised to a higher sensitivity level, and data collected from lower-level sources can produce “pieces of the puzzle” for how the military is strategically operating
- The DFARS 7012 clause does not currently require verification of contractors’ implementation of NIST SP 800-171 prior to contract award

New DFARS clauses issued

New requirements implemented in three new DFARS clauses:

DFARS 252.204-7019, *Notice of NIST SP 800-171 DOD Assessment Requirements*

- Amends DFARS 7012 by requiring KOs to verify offeror has current NIST 800-171 Assessment on record
- Summary-level assessment scores (out of 110) must be uploaded to SPRS
- Assessments may not be more than 3 years old, entered per CAGE code

DFARS 252.204-7020, *NIST SP 800-171, DOD Assessment Requirements*

- Provides DOD NIST SP 800-171 Assessment Methodology, formerly used during DIBCAC assessments, based on NIST 800-171 controls and a scoring range of -311-110.
- Basic, Medium, High level assessments

DFARS 252.204-7021, *Contractor Compliance with the Cybersecurity Maturity Model Certification (CMMC) Level Requirements*

- Cybersecurity Maturity Model Certification Requirements
- Prescribed for use in solicitations and contracts, including FAR part 12 procedures for the acquisition of commercial items (exl. COTS)

Scoring for NIST 800-171 Assessments

- To be eligible for awards on or after November 30, a contractor must complete the first level called a *Basic Assessment*.
- If all security requirements are implemented, a contractor is awarded a score of 110, consistent with the total number of NIST SP 800-171 security requirements.
- For each security requirement not met, the associated value is ***subtracted*** from 110. The score of 110 is reduced by each requirement not implemented, which may result in a negative score.
- Certain requirements have more impact on the security of the network and its data than others.
- This scoring methodology incorporates this concept by weighting each security requirement based on the impact to the information system and the DoD CUI created on or transiting through that system, when that requirement is not implemented.

SPRS: Weighted Security Controls

The cost of Security controls not implemented are weighted by vulnerability:

The cost of unimplemented security controls:			
“Significant Exploitation of the Network”		“Specific and confined effect”	
-5 points	-5 points	-3 points	-3 points
Basic Security Requirements: 3.1.1, 3.1.2, 3.2.1, 3.2.2, 3.3.1, 3.4.1, 3.4.2, 3.5.1, 3.5.2, 3.6.1, 3.6.2, 3.7.2, 3.8.3, 3.9.2, 3.10.1, 3.10.2, 3.12.1, 3.12.3, 3.13.1, 3.13.2, 3.14.1, 3.14.2, and 3.14.3.	Derived Security Requirements: 3.1.12, 3.1.13, 3.1.16, 3.1.17, 3.1.18, 3.3.5, 3.4.5, 3.4.6, 3.4.7, 3.4.8, 3.5.10, 3.7.5, 3.8.7, 3.11.2, 3.13.5, 3.13.6, 3.13.15, 3.14.4, and 3.14.6.	Basic Security Requirements 3.3.2, 3.7.1, 3.8.1, 3.8.2, 3.9.1, 3.11.1, and 3.12.2.	Derived Security Requirements 3.1.5, 3.1.19, 3.7.4, 3.8.8, 3.13.8, 3.14.5, and 3.14.7.

1 point is subtracted from the score of 110 for all remaining unimplemented Derived Security Requirements that have a limited or indirect effect on the security of the network and its data.

+1 point per control for each security control, if fully implemented for a maximum of 110.

Cybersecurity Maturity Model (CMMC)

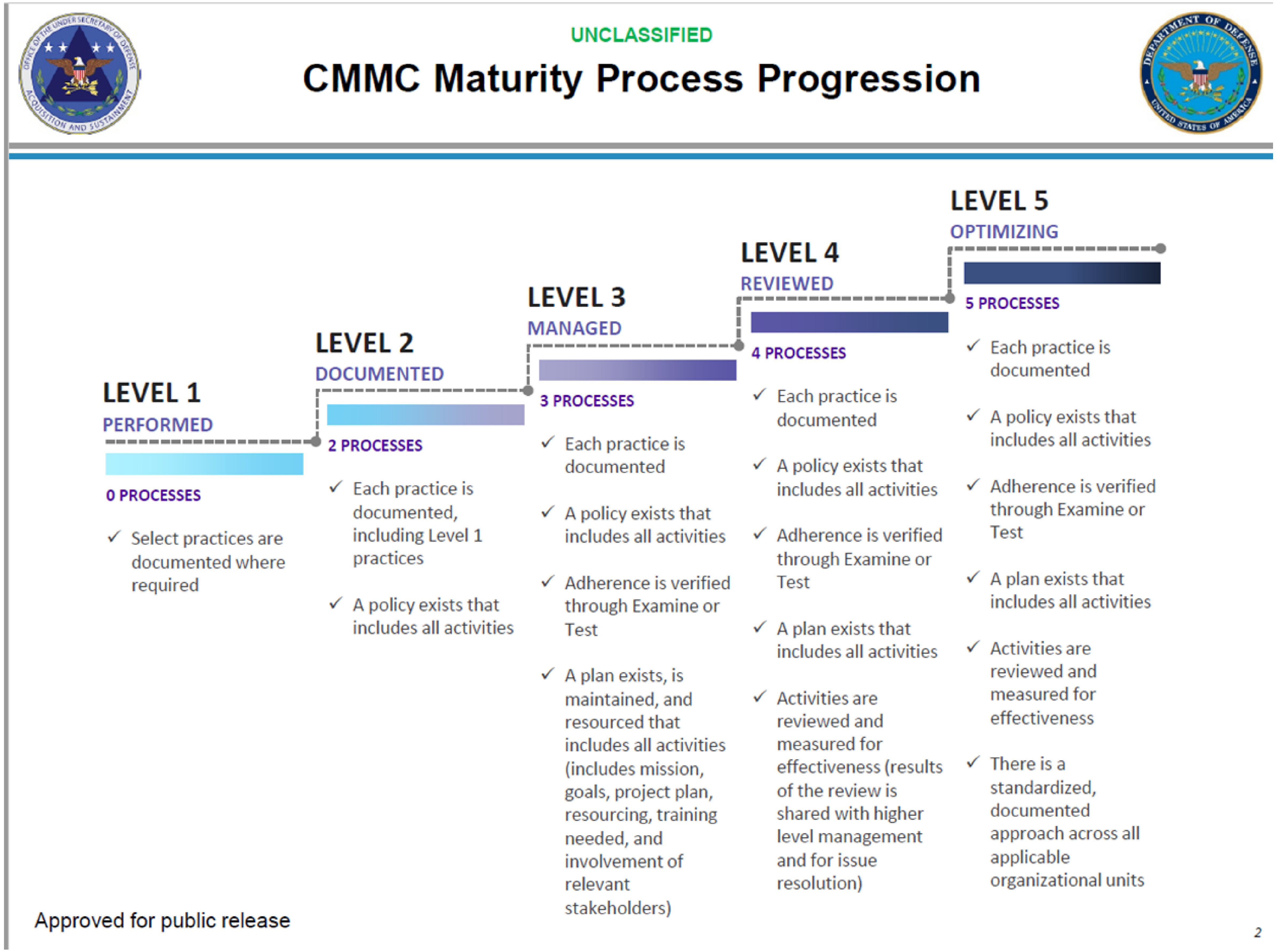
CMMC is a cybersecurity certification program advocated by the DoD

- Five cybersecurity maturity levels (1-5), builds on NIST 800-171, NIST 800-172, 800-53, CIS
- Measures a contractor's cybersecurity program maturity, evidenced by the implementation of prescribed NIST and other frameworks' security practices/processes
- CMMC requirements will appear in the requirement document or statement of work.

Crawl-Walk-Run Approach for Implementation

- DOD will begin to roll out CMMC requirements on November 30, 2020.
- By October 1, 2025, CMMC to be included in virtually all DOD contracts.
- Rule does not identify criteria for determining which solicitations or contracts will include CMMC requirements.
- Contracting officers will implement these requirements by including a third new clause introduced in the interim rule: DFARS 252.204-7021, *Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement*.

Approval is needed from the Office of the Undersecretary of Defense for Acquisition and Sustainment before including any CMMC requirements in a solicitation during this phase of the rollout.



UNCLASSIFIED

CMMC Maturity Process Progression

LEVEL 1
PERFORMED

0 PROCESSES

- ✓ Select practices are documented where required

LEVEL 2
DOCUMENTED

2 PROCESSES

- ✓ Each practice is documented, including Level 1 practices
- ✓ A policy exists that includes all activities

LEVEL 3
MANAGED

3 PROCESSES

- ✓ Each practice is documented
- ✓ A policy exists that includes all activities
- ✓ Adherence is verified through Examine or Test
- ✓ A plan exists, is maintained, and resourced that includes all activities (includes mission, goals, project plan, resourcing, training needed, and involvement of relevant stakeholders)

LEVEL 4
REVIEWED

4 PROCESSES

- ✓ Each practice is documented
- ✓ A policy exists that includes all activities
- ✓ Adherence is verified through Examine or Test
- ✓ A plan exists that includes all activities
- ✓ Activities are reviewed and measured for effectiveness (results of the review is shared with higher level management and for issue resolution)

LEVEL 5
OPTIMIZING

5 PROCESSES

- ✓ Each practice is documented
- ✓ A policy exists that includes all activities
- ✓ Adherence is verified through Examine or Test
- ✓ A plan exists that includes all activities
- ✓ Activities are reviewed and measured for effectiveness
- ✓ There is a standardized, documented approach across all applicable organizational units

Approved for public release

2

CMMC Maturity Levels

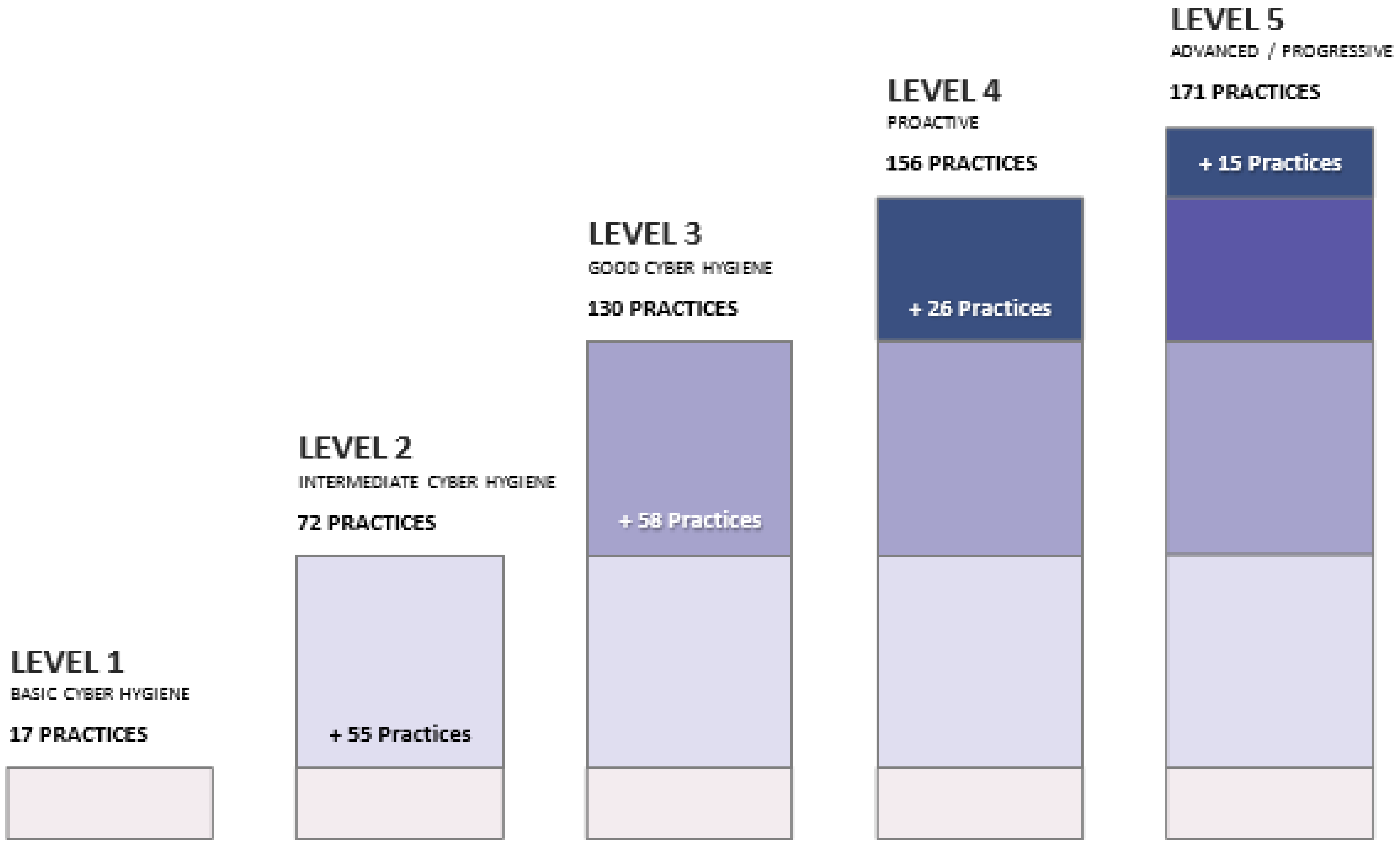


Figure 5. CMMC Practices Per Level

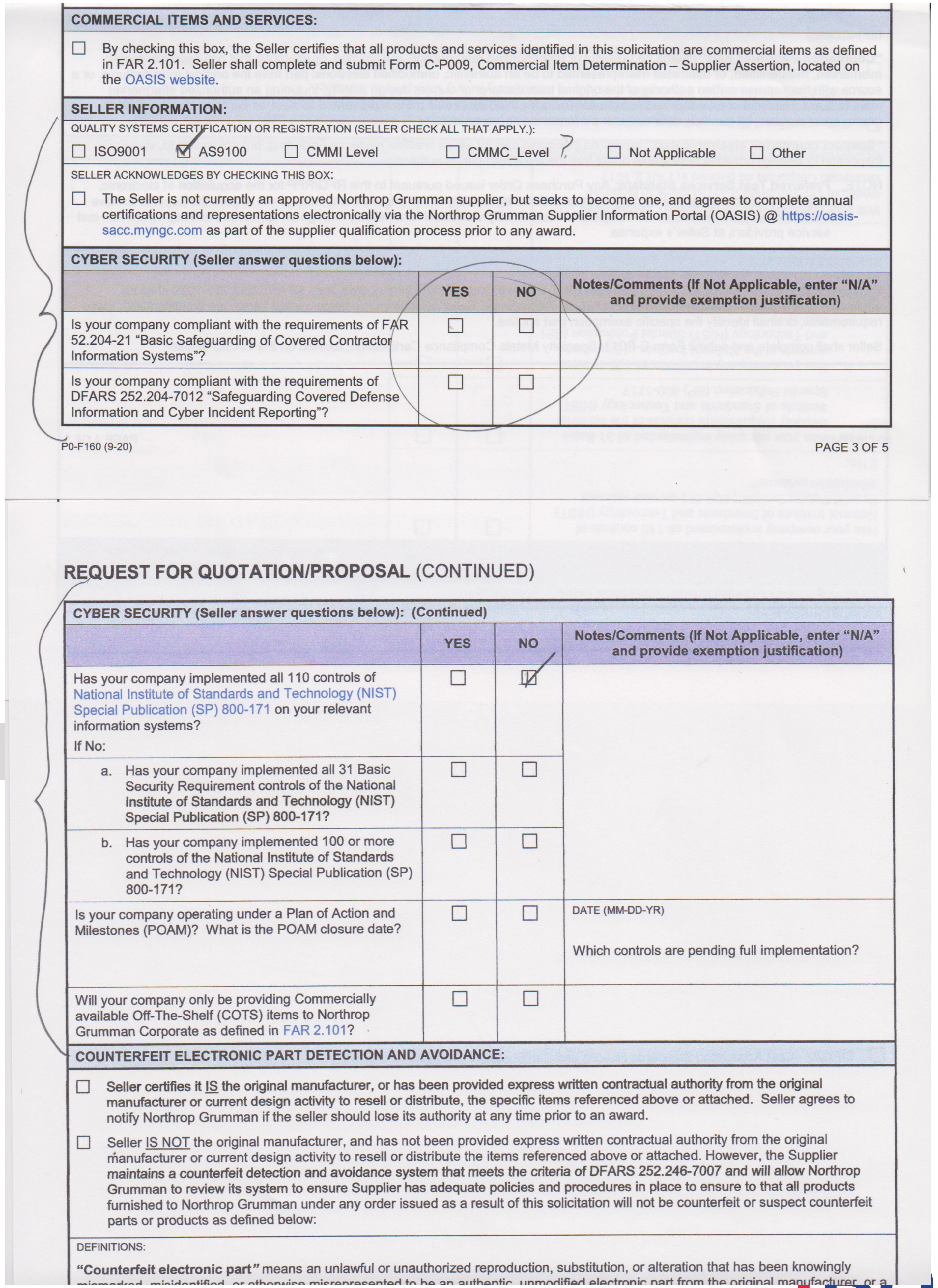
Prime Notifications to Subcontractors:

*"**Provide Status to [PRIME CONTRACTOR]. ***

In order for [PRIME CONTRACTOR] to assess risk and preparedness for the November 30 effective date of the new rules, we must receive the status of our applicable suppliers. You will be receiving a survey link on Thursday, October 29 asking to provide the following. Please complete the survey by Thursday, November 5.

- *Confirmation of NIST 800-171 Assessment Score in SPRS*
- *POAM ECD for any unimplemented NIST 800-171 requirements*
- *Status/ECD for additional 20 (7 Level 2 / 13 Level 3) CMMC practices*
- *Status/ECD for Level 2/3 maturity processes*

Going forward, we are requesting you provide updates to this set of information until all outstanding practices and processes are implemented. When responding to this email, please provide the estimated date for closure of all NIST SP 800-171 POAM items, and the expected closure date for the additional controls."



COMMERCIAL ITEMS AND SERVICES:

☐ By checking this box, the Seller certifies that all products and services identified in this solicitation are commercial items as defined in FAR 2.101. Seller shall complete and submit Form C-P009, Commercial Item Determination – Supplier Assertion, located on the OASIS website.

SELLER INFORMATION:

QUALITY SYSTEMS CERTIFICATION OR REGISTRATION (SELLER CHECK ALL THAT APPLY.):

☐ ISO9001 ☑ AS9100 ☐ CMMI Level ☐ CMMC_Level ? ☐ Not Applicable ☐ Other

SELLER ACKNOWLEDGES BY CHECKING THIS BOX:

☐ The Seller is not currently an approved Northrop Grumman supplier, but seeks to become one, and agrees to complete annual certifications and representations electronically via the Northrop Grumman Supplier Information Portal (OASIS) @ https://oasis-sacc.myngc.com as part of the supplier qualification process prior to any award.

CYBER SECURITY (Seller answer questions below):

	YES	NO	Notes/Comments (If Not Applicable, enter "N/A" and provide exemption justification)
Is your company compliant with the requirements of FAR 52.204-21 "Basic Safeguarding of Covered Contractor Information Systems"?	☐	☐	
Is your company compliant with the requirements of DFARS 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting"?	☐	☐	

REQUEST FOR QUOTATION/PROPOSAL (CONTINUED)

CYBER SECURITY (Seller answer questions below): (Continued)

	YES	NO	Notes/Comments (If Not Applicable, enter "N/A" and provide exemption justification)
Has your company implemented all 110 controls of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 on your relevant information systems? If No:	☐	☑	
a. Has your company implemented all 31 Basic Security Requirement controls of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171?	☐	☐	
b. Has your company implemented 100 or more controls of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171?	☐	☐	
Is your company operating under a Plan of Action and Milestones (POAM)? What is the POAM closure date?	☐	☐	DATE (MM-DD-YR) Which controls are pending full implementation?
Will your company only be providing Commercially available Off-The-Shelf (COTS) items to Northrop Grumman Corporate as defined in FAR 2.101?	☐	☐	

COUNTERFEIT ELECTRONIC PART DETECTION AND AVOIDANCE:

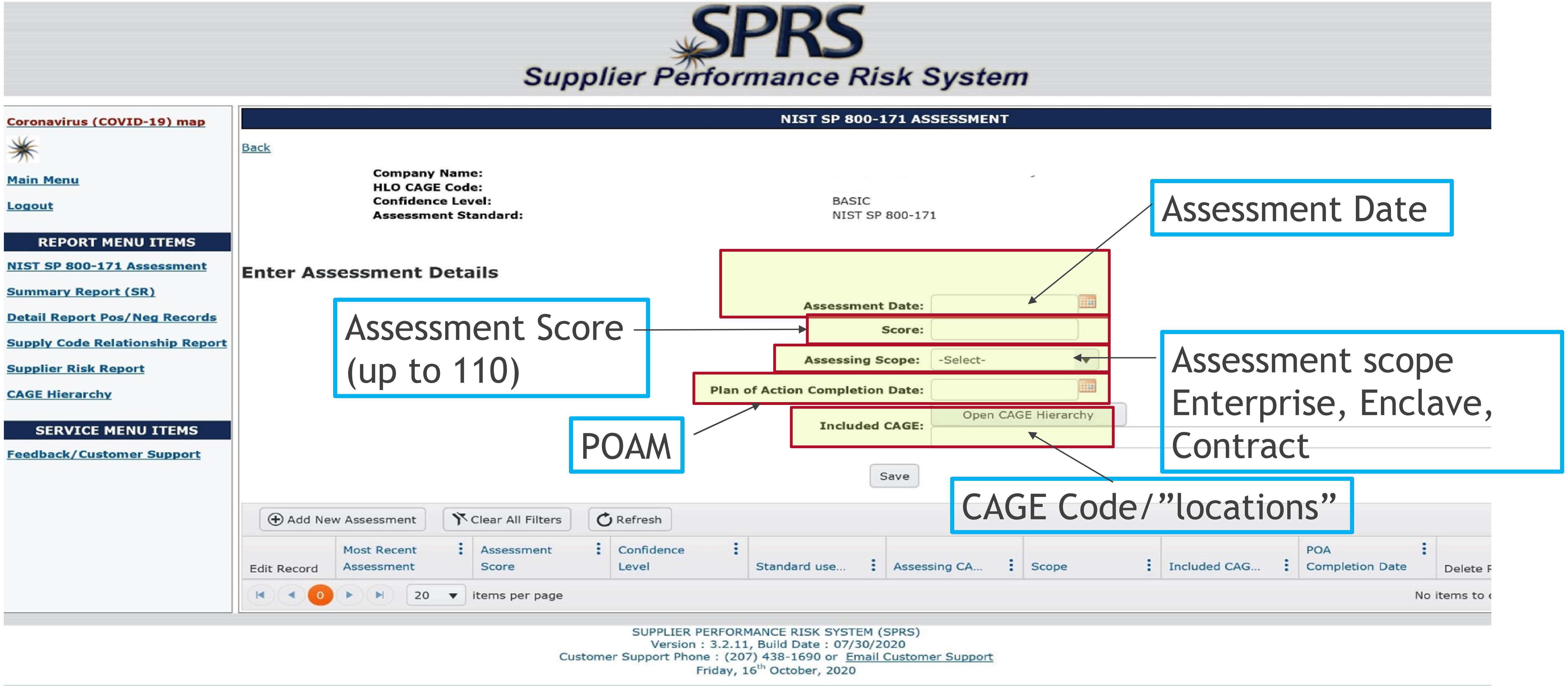
☐ Seller certifies it IS the original manufacturer, or has been provided express written contractual authority from the original manufacturer or current design activity to resell or distribute, the specific items referenced above or attached. Seller agrees to notify Northrop Grumman if the seller should lose its authority at any time prior to an award.

☐ Seller IS NOT the original manufacturer, and has not been provided express written contractual authority from the original manufacturer or current design activity to resell or distribute the items referenced above or attached. However, the Supplier maintains a counterfeit detection and avoidance system that meets the criteria of DFARS 252.246-7007 and will allow Northrop Grumman to review its system to ensure Supplier has adequate policies and procedures in place to ensure to that all products furnished to Northrop Grumman under any order issued as a result of this solicitation will not be counterfeit or suspect counterfeit parts or products as defined below:

DEFINITIONS:

"Counterfeit electronic part" means an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a

SPRS Assessment Entry Screen



SPRS
Supplier Performance Risk System

Coronavirus (COVID-19) map

Main Menu

Logout

REPORT MENU ITEMS

NIST SP 800-171 Assessment

Summary Report (SR)

Detail Report Pos/Neg Records

Supply Code Relationship Report

Supplier Risk Report

CAGE Hierarchy

SERVICE MENU ITEMS

Feedback/Customer Support

NIST SP 800-171 ASSESSMENT

Back

Company Name:
HLO CAGE Code:
Confidence Level: BASIC
Assessment Standard: NIST SP 800-171

Enter Assessment Details

Assessment Date:

Score:

Assessing Scope: -Select-

Plan of Action Completion Date:

Included CAGE: Open CAGE Hierarchy

Save

Assessment Date

Assessment Score (up to 110)

Assessment scope Enterprise, Enclave, Contract

POAM

CAGE Code/"locations"

Add New Assessment | Clear All Filters | Refresh

Edit Record	Most Recent Assessment	Assessment Score	Confidence Level	Standard use...	Assessing CA...	Scope	Included CAG...	POA Completion Date	Delete R

0 | 20 items per page | No items to

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS)
Version : 3.2.11, Build Date : 07/30/2020
Customer Support Phone : (207) 438-1690 or Email Customer Support
Friday, 16th October, 2020

Things you Need to Know (1)

You cannot get to 110 fully satisfied security controls overnight – *Plan time for assessments and your SSP!*

- 800-171 Assessment must be entered into the Supplier Performance Risk System (SPRS) – getting an account is a challenge
- Start with accounts in the PIEE system to gain access to SPRS. Must have a Contracts Administrator account in PIEE (CAM Account) before SPRS account can be made
- PIEE CAM account must be the same as the EB POC in SAM database
- Full gap assessments may take about 2 weeks, if you have everything implemented, and can take up to 6-9 months if the security controls are not 100% implemented
- Gap assessment should feed directly into the Plan of Action and Milestones (PoA&M)
- Systems Security Plan may take another 2-4 weeks to construct (longer if more items are on your POAM)

Things you Need to Know (2)

- Even if the new DFARS clauses **do not** appear in your contract, via the **Christian Doctrine**, they may be “read into” your contract
- Prime contractors must flow down these requirements “in all subcontracts and other contractual instruments” as long as neither of the two exceptions apply (micro-purchase threshold or COTS items).
- If a subcontractor does not have a current Basic Assessment, the prime “shall not award a subcontract or other contractual instrument.”
- If the Prime questions what contractual items to flow down, talk to Contract Officer. If Subcontractor thinks the DFARS clause should not be applied, ask the Contract Officer for variance.
- SPRS scores are only visible to DoD, so primes will need verification of compliance from their subcontractors.

Thank you!

Christina Reynolds| Director
C|HFI, C|EH, C|NDA
BDO Industry Specialty Services Group
+256-998-8093
creynolds@bdo.com