Frequently Asked Questions (FAQs) regarding the implementation of DFARS Subpart 204.73 and PGI Subpart 204.73 DFARS Subpart 239.76 and PGI Subpart 239.76

This document adds to and revises previously published FAQs. Additions/edits to the April 2, 2018 rev 1 document are shown in blue.

Quick Look for FAQ Topics

THE FOLLOWING QUESTIONS ARE ADDRESSED IN THIS DOCUMENT:

Safeguarding Covered Defense Information and Cyber Incident Reporting (DFARS provision 252.204-7008 and DFARS clause 252.204-7012)

- **General**

Q1: When is DFARS clause 252.204-7012 required in contracts? Is the clause required in contracts for commercial items?

Q2: When does DoD's purchase of a commercial item (sold to, but not developed for, DoD) mean that data associated with the item requires protection as covered defense information? For example, does a contract with DFARS clause 252.204-7012 for purchase of a standard commercial item, with a requirement to deliver the standard technical data package for that item (e.g., operations or maintenance data) with the only change to mark the cover page with a Controlled Technical Information Distribution Statement (e.g., Distribution D), mean the company now has to protect this data as covered defense information?

Q3: What is the purpose of DFARS clause 252.204-7012?

Q4: How will the Department manage the multiple versions of DFARS clause 252.204-7012 that currently exist?

Q5: How can I change my contract to incorporate the current version of NIST SP 800-171? For example, I want to implement revision 1 of NIST SP 800-171 published in December 2016, but my contract was awarded before December 2016.

Q6: When must the requirements in DFARS clause 252.204-7012 be implemented?

Q7: Our company has outsourced its IT support and systems to a third-party contractor. Are we still responsible for complying with DFARS clause 252.204-7012 and implementing NIST SP 800-171?"

Q8: Can the requirements in DFARS clause 252.204-7012, specifically the NIST SP 800-171 security requirements, be waived?

Q9: Can you provide clarification with regard to what is a "Covered contractor information system"?

Q10: When and how should DFARS clause 252.204-7012 flow down to subcontractors?

Q11: In working with foreign subcontractors, how do we resolve issues with clause requirements (e.g., reporting cyber incidents or providing digital images to DoD) that cannot be flowed down due to a conflict with local laws?

Q12: What are the cost recovery options for complying with DFARS clause 252.204-7012?

Q13: Can primes/higher tiered subcontractors include the cost associated with regulatory compliance of their next lower tiered covered defense information suppliers in proposals on solicitations including the 252.204-7008 provision and 252.204-7012 clause? Is the cost chargeable to specific contracts where there is an expectation for this level of regulatory compliance oversight?

Q14: Who in DoD can I contact for clarification on DFARS clause 252.204-7012 or NIST 800-171 in support of DFARS clause 252.204-7012?

Q15: Will the DoD certify that a contractor is compliant with the required security requirements?

Q16: Is a 3rd Party assessment of compliance required?

Q17: Does the Government intend to monitor contractors to ensure implementation of the required security requirements?

Q18: Will Prime Contractors be responsible for the auditing of their sub-contractors? If so, how will compliance be demonstrated? How does a small company audit their supply chain?

Q19: What are the consequences for non-compliance? The system security plan allows organizations to extend the deadline for full compliance by building a POAM which allows for the planned and future implementation of security controls. Will there be follow-on reviews of the POAMs and monitoring of a company's efforts to achieve full compliance?

Q20: How often should our company review our compliance to the NIST SP 800-171 security requirements?

- ## Covered Defense Information

Q21: Who is responsible for identifying/marking covered defense information?

Q22: What information should be identified/marked in accordance with DFARS clause 252.204-7012?

Q23: How will covered defense information that is provided to the contractor by or on behalf of DoD in support of the performance of the contract be identified/marked?

Q24: How will covered defense information that is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract be marked?

Q25: Is information identified as FOUO considered to be covered defense information?

Q26: What is Controlled Technical Information (CTI)?

Q27: If a Contract document (i.e., DD Form 1423-1) mandates the use of a Distribution Statement (B-F) on a contractor generated document for submission to the government but does not use the term CUI, should the contractor understand the document to be CUI and protect/control accordingly? Is it correct to say that any document with a Distribution Statement B-F is CUI?

Q28: Should export controlled information be treated as covered defense information?

Q29: When export controlled information meets the definition of covered defense information, does that mean that I now need to protect all of my export controlled information, which previously had no such requirement? How does this affect EAR99 items?

Q30: Can you provide common examples of Proprietary CUI? This category could raise big challenges in the area of business development and proposals and things such as employee rosters, quality processes etc.

Q31: What should the Contractor do if covered defense information or operationally critical support is not identified in the contract, task order, or delivery order, and the Contractor becomes aware of covered defense information or operationally critical support during performance of the contract?

Q32: What is meant by the phrase "by or on behalf of DoD in support of the performance of the contract" in the definition of covered defense information?

Q33: What is the relationship between Controlled Unclassified Information (CUI), as defined in the National Archives and Record Administration (NARA) final rule published in the Federal Register on September 14, 2016 (81 FR 63324), DoD CUI, and covered defense information? Are the definitions aligned?

Q34: Will contract documents clearly identify specific items/documents that are CUI using the term 'Controlled Unclassified Information (CUI)'?

- **Operationally Critical Support**

Q35: What is "Operationally Critical Support"? How will it be identified?

- **Safeguarding Covered Defense Information**

Q36: How are the security protections required for a contractor's internal information system different than the protections required for a DoD information system?

Q37: Why did the security protections required by DFARS clause 252.204-7012 change from a table of selected NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, security controls to NIST Special Publication (SP) 800-171? How does NIST SP 800-171 compare to NIST SP 800-53?

Q38: How should a contractor deal with a situation where HIPAA applies, in addition to the protections required by NIST SP 800-171?

- **Cyber Incidents and Reporting**

Q39: Cyber incidents are defined as "a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein." Can you provide examples of cyber incidents that have an "adverse effect" and cyber incidents that have a "potential adverse effect" to help clarify the differences?

Q40: If a workstation without covered defense information has antivirus software installed and operating, but malware gets through the antivirus software and gets installed and not activated on the workstation, and the workstation is part of a covered contractor information system, is this considered a cyber incident?

Q41: If a commercial sandbox/detonation chamber is used as part of a workstation's protection, and malware is launched in the sandbox/detonation chamber, is that still considered a cyber incident?

Q42: How does the Contractor report a cyber incident?

Q43: How can the contractor obtain DoD-approved medium assurance External Certificate Authority (ECA) certificate in order to report?

Q44: What should the contractor do when they do not have all the information required by the clause within 72 hours of discovery of any cyber incident?

Q45: What happens when the contractor submits a cyber incident report?

Q46: How are subcontractors required to report cyber incidents? Can you provide clarification regarding the types of information that must be disclosed by a subcontractor to a prime contractor?

Q47: Does the requirement at DFARS clause 252.204-7012(e) to preserve all relevant monitoring/packet capture data…" imply that there is a requirement to do packet capture?

Q48: How does the contractor submit media?

- **Submission of Malicious Software**

Q49: If antivirus identifies and quarantines a piece of malware as part of its check on a downloaded file, does the quarantined malware need to be submitted to the DoD Cyber Crime Center (DC3)? If so, is this considered a cyber incident?

- **Cyber Incident Damage Assessment**

Q50: What is meant by the language at 252.204-7009 (b)(5)(i) which states, "A breach of these obligations or restrictions may subject the contractor to criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States"?

Basic Safeguarding of Contractor Information Systems (FAR Clause 52.204.21)

Q51: Will FAR clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, and DFARS clause 252.204-7012 be used in the same solicitation/contract?

NIST SP 800-171

- **General Implementation Issues**

Q52: What is the difference between the Basic and Derived Requirements in NIST SP 800-171? Do all requirements have to be met (i.e., if the Basic Requirement is met, does that mean the 'Derived' Requirements are met, since they are 'derived' from the Basic Requirement)?

Q53: Is it appropriate for a program office or requiring activity to add to the NIST SP 800-171 security requirements, or to specify how a contractor should implement the various requirements in NIST SP 800-171 (e.g., specify password length or complexity, use of specific monitoring equipment, etc.)?

Q53.1: Are there minimum standards for password length or complexity?

Q53.2: Are there minimum requirements to configure session lock on systems and networks after periods of inactivity and unsuccessful logon attempts?

Q54: What is the significance of the change in Revision 1 to NIST SP 800-171 from 'information systems' to 'system.'

Q55: Does the change from 'Information System' to 'System' mean that NIST SP 800-171 applies to individual devices, such as stand-alone test equipment?

Q56: Why was the requirement for a system security plan added to Revision 1 of NIST SP 800-171?

Q57: How can the DoD consider an offeror's implementation of NIST SP 800-171 in the source selection process?

Q58: If a contractor meets the requirements of NIST SP 800-171, can a DoD requiring activity use the evaluation/source selection process to define the acceptability of 'how' a contractor meets those requirements?

Q59: How will the DoD account for the fact that compliance with NIST SP 800-171 is an iterative and ongoing process? The DFARS clause imposing NIST SP 800-171 requires that the entire system be in 100% compliance all the time, a condition that in practice (in industry or Government) is almost never the case.

For example:

- **It is not possible to apply session lock or termination (Requirements 3.1.10/11) to certain computers (e.g., in a production line or medical life-support machines).**
- **Applying a necessary security patch can "invalidate" FIPS validated encryption (Requirement 3.13.11) since the encryption module "with the patch" has not been validated by NIST.**
- **Segments of an information system may be incapable of meeting certain requirements, such as correcting flaws/patching vulnerabilities (Requirement 3.14.1) without disrupting production/operations that may be critical to the customer.**

How should a contractor deal with situations such as these?

Q60: How might a small business with limited information technology (IT) or cybersecurity expertise approach meeting the requirements of NIST SP 800-171?

Q61: Will DoD provide additional guidance or training to smaller companies that may initially find these requirements overwhelming?

Q62: What if the contractor thinks a required security control is not applicable, or that an alternative control or protective measure will achieve equivalent protection?

Q63: What is the process used by the DoD CIO to adjudicate alternative/non-applicable controls?

Q64: What are the criteria used by the DoD CIO in adjudicating alternative/non-applicable controls?

Q65: Are there circumstances when DoD CIO adjudication of 'Alternative' or 'Not Applicable' solutions is not required?

Q66: Are contractors required to submit previously approved DOD CIO assessments of "not applicable" requirements or "alternative security measures" for any deficiency not being remediated? For example: Once a contracting officer accepts a request from a contractor for a NIST SP 800-171 requirement to be deemed "not applicable" or an "alternative security measure," is the contractor required to submit that documentation for every current contract with the DFARS clause 252.204-7012?

Q67: Why does the DoD CIO require notification of the security requirements not implemented at the time of award? What is required for the notification requirement if the contract in question ends prior to the 31 December 2017 compliance date? Will the DoD allow for a single corporate-wide notification, such that the notification requirement could be accomplished at annual or semi-annual intervals, and not on every single transaction within 30 days? [Note: Not required for contracts awarded after October 1, 2017]

Q68: Is post-award notification of the security requirements not implemented at the time of award also required within 30 days of award of subcontracts?

Q69: Can contractors and subcontractors negotiate the provisions for providing notifications to higher tiered contractors when submitting the required statements of NIST non-compliance, non-applicability, and/or equally effective and alternate controls to the contracting officer for adjudication by the DOD CIO?

Q70: How does NIST SP 800-171 relate to the NIST Cybersecurity Framework?

Q71: NIST SP 800-171 is focused on confidentiality of information. In a manufacturing environment, there may also be the need for availability and integrity controls. How will operational environments influence the selection and/or implementation of additional security controls? Will the DoD develop implementation guides or case scenarios to demonstrate implementation of security controls in a manufacturing environment?

- **Specific NIST SP 00-171 Security Requirements**

Q72: Security Requirements 3.1.13, 3.1.17, 3.1.19, 3.13.8, and 3.13.11 – Do all of the 171 security requirements for cryptography have to be FIPS validated, and if so, what does that mean? If the algorithm is FIPS approved, is that sufficient?

Q73: Security Requirement 3.1.7 and 3.5.3 - If regular users' computer accounts are "administrator accounts" or have 'limited administrative rights" only on their computers, are they considered a "privileged account" requiring audit for privileged functions (3.1.7) or requiring multifactor authentication (3.5.3) at the "local access level"?

Q74: Security Requirement 3.1.9 – 3.1.9 requires "privacy and security notices consistent with applicable CUI rules." Which CUI rules are being referenced?

Q75: Security Requirement 3.1.20 – 3.1.20 requires that an organization "verify and control/limit connections to and use of external systems." What is meant by 'external systems' and how are they controlled/limited?

Q76: Security Requirement 3.1.21 – 3.1.21 requires limiting the use of organizational portable storage devices on external information systems. Is this expected to be done using technical means or by policy? If there are technical options, can you provide any examples?

Q77: Security Requirement 3.1.21 – Can you provide a definition of "portable device", as that is not defined in NIST guidance?

Q78: Security Requirement 3.2.1, 3.2.2, and 3.2.3 – The requirement to ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems (3.2.1), the requirement to ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities (3.2.2), and the requirement to provide security awareness training on recognizing and reporting potential indicators of insider threat (3.2.3) address the training required to be compliant with NIST SP 800-171. Where can we find training materials to address these requirements?

Q79: Security Requirement 3.4.9 and 3.13.13 – The requirement to control and monitor user-installed software (3.4.9) and the requirement to control and monitor the use of mobile code (3.13.13) seem outside the scope of protecting CUI. Shouldn't the requirement be to control CUI processing to authorized software?

Q80: Security Requirement 3.5.3 – Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. What is meant by "multifactor authentication?"

Q81: Security Requirement 3.5.3 – Can one of the factors in multifactor authentication be where you are (e.g., within a controlled access facility)?

Q82: Security Requirement 3.5.3 – Native 2-factor authentication support for network access on all platforms is problematic; how is the multifactor requirement met?

Q83: Security Requirement 3.5.3 – Do I need to use "multifactor authentication" for a smartphone or tablet?

Q84: Security Requirement 3.5.3 – What if I have covered defense information on my smartphone or tablet (e.g., in company e-mail) – do I need to use multifactor authentication in that case?

Q85: Security Requirement 3.5.3 – If a systems administrator has already been authenticated as a normal user using multifactor authentication, does using his administrative password to install software on the system violate the multifactor requirement?

Q86: Security Requirement 3.5.4 – The requirement to employ replay resistant authentication mechanisms for network access to privileged and non-privileged accounts. What defines replay resistant?

Q87: Security Requirement 3.5.5 and 3.12.1 – Are there minimum acceptable values for "periodic" or "conditional" in requirements such as 3.5.5 "Prevent reuse of identifiers for a defined period" and 3.12.1, "Periodically assess the security controls in organizational systems…"?

Q88: Security Requirement 3.5.10 – Store and transmit only encrypted representations of passwords (in Revision 1, "encrypted representations of passwords" is changed to "cryptographically-protected password)." Is a HASH considered an "encrypted representation" of a password or a cryptographically-protected password?

Q89: Security Requirement 3.7.5 – Can the requirement for multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete be met using other authentication and access control combinations such as remote IP address restrictions, session monitoring, and "One-Time-Pads"?

Q90: Security Requirement 3.8.2 – Can digital rights management protections or discretionary access control lists meet the intent of the requirement to "limit access to CUI on information system media to authorized users?"

Q91: Security Requirement 3.8.4 – Mark media with necessary CUI markings and distribution limitations. Is this for all media, to include cell phones, for example, or just for removable media?

Q92: Security Requirement 3.8.4 – Mark media with necessary CUI markings and distribution limitations. Can DoD provide further guidance on DoD's covered defense information marking requirements? In the NIST SP 800-171 Revision 1 document, this control contains a footnote that indicates, "The implementation of this requirement is per marking guidance in 32, Part 2002, and the CUI Registry." In light of this, is DoD's position that contractors must mark all CUI processed through covered contractor information systems, or only covered defense information processed through covered contractor information systems? Also, is DoD's position that contractors must use the National Archives and Records Administration ("NARA") CUI marking handbook?

Q93: Security Requirement 3.10.1 – Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. This requirement has a feel of handling classified data and treating the data as need to know within the organization. Is this the case? Does covered defense information need to be handled as need to know? Can covered defense information-authorized and non-covered defense information-authorized personnel use the same set of cubicles?

Q94: Security Requirement 3.10.6 – Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites). Is this expected to be done using technical means or by policy? If there are technical options, can you provide any examples?

Q95: Security Requirement 3.11.1 – Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. Is there a minimum requirement for risk assessment methodology (including risk calculation methodology) and reporting format and a defined minimum period?

Q96: Security Requirements 3.12.1 and 3.12.3 – Periodically assess the security controls in organizational systems to determine if the controls are effective in their application; Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. Is there a defined period for assessment; what content is required in a DFARS clause 252.204-7012 compliant Security Controls Assessment report?

Q97: Security Requirements 3.12.2 and 3.12.4 - System security plans are being interpreted differently by various federal departments and agencies. Can you clarify the role of the system security plan and plans of action in contract formation and contract administration? Can full compliance with SP 800-171 be achieved after December 31, 2017, with a company specific system security plan and plans of action?

Q98: Security Requirement 3.12.4 – Is there a prescribed format/level of specificity for a system security plan?

Q99: What are the minimum requirements for a system security plan to be 'compliant'?

Q100: Security requirement 3.13.6 – The requirement to "deny network communications traffic by default and allow network communications traffic by exception" (i.e., deny all, permit by exception) is unrealistic if it must be implemented on all systems that host or transit CUI information. Can this requirement be met if there is a mechanism to implement "deny all, permit by exception" rule within the path between the external network and the CUI information?

Q101: Security Requirement 3.13.8 – When implementing the requirement to "Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards," is encryption required for a Multiprotocol Label Switching (MPLS) private network (thus an extension of a local network) but it is multi-tenant protected by VLANs?

Q102: Security Requirement 3.13.8 – Can Transport Layer Security (TLS) protocol be used to protect CUI during transmission over the Internet?

Q103: Regarding security requirement 3.13.8– How is CUI to be protected when transmitted over Common Carrier telecommunications lines/Plain Old Telephone Service (POTS)?

Q104: Security Requirement 3.13.14 – The description for the security requirement in Section 3 (3.13.14) "control and monitor the use of Voice over Internet Protocol (VoIP) technologies" is different from the corresponding Appendix D entry, "Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies and monitor/control use of VoIP." Which is correct? How should this be handled for 3rd party VoIP service offerings where control is outsourced. (i.e., Vonage)? Does this security requirement only apply when the VoIP service is shared on a network that transits CUI?

Q105: Security Requirement 3.13.16 – Protect the Confidentiality of CUI at rest. Can CUI be stored at rest in any non-mobile devices or data center, unencrypted, as long as it is protected by other approved logical or physical methods?

Cloud Computing

- **General**

Q106: Can you clarify when DFARS Clause 252.239-7010 applies to cloud computing services and when DFARS Clause 252.204-7012 applies?

Q107: Why is DFARS Clause 252.239-7010 addressed in DFARS Clause 252.204-7012?

Q108: Will the DoD require physical access to cloud computing data centers in order to conduct forensic analysis under DFARS clause 252.204-7012(f) or 252.239-7010(g) and (i)?

- **Cloud solution being used to store data on DoD's behalf (DFARS provision 252.239-7009 and DFARS clause 252.204-7010, Cloud Computing Services, apply)**

  Q109: How is the requirement for a provisional authorization waived by the DoD CIO, allowing a contracting officer to award a contract to acquire cloud services from a cloud service provider (CSP) that has not been granted a provisional authorization by the Defense Information System Agency (DISA)?

- **Contractor using cloud solution to store covered defense information (DFARS provision 252.204-7008 and DFARS clause 252.204-7012 apply)**

  Q110: How can a contractor ensure that the cloud service provider can comply with requirements 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 (i.e., paragraphs (c) through (g) of DFARS clause 252.204-7012?

  Q111: Do cloud service providers (CSP) have to follow DFARS clause 252.204-7012 (c)-(g) if there is a breach inside a hosted customer Virtual Machine (VM)?

  Q112: What security requirements apply when using a cloud solution to process/store covered defense information?

  Q113: Can you clarify what is meant by 'equivalent' to FedRAMP, so that companies will know what cloud services they can use and the relationship to NIST SP 800-171 in order to assess what the cloud service providers and what the company may need to furnish to meet the required cybersecurity controls?

  Q114: Why 'equivalent to FedRAMP moderate'? Why is NIST SP 800-171 not sufficient in the case of a cloud service provider?

  Q115: The DFARS states "the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline". If the cloud provider is not FedRAMP certified, how can a contractor ensure that the cloud provider meets security requirements equivalent to FedRAMP Moderate? How can a contractor ensure that the cloud provider meets security requirements equivalent to FedRAMP "moderate"?

Q116: If a company is using an external Cloud Service Provider (CSP) to provide processing and storage of covered defense information, (i.e., DFARS clause 252.204-7012 requires that the CSP meet requirements equivalent of to the FedRAMP Moderate baseline), depending on the service provided (i.e., IaaS, PaaS or SaaS), some of these FedRAMP requirements are allocated to the client. In this case, does the client (the company contracting with the CSP) have to meet FedRAMP "Moderate" requirements that are NOT mapped to the NIST SP 800-171 requirements per Appendix D of NIST SP 800-171?

Q117: Is the contractor required to flow down DFARS clause 252.704-7012 when utilizing a cloud service provider? Is the contractor responsible for ensuring that cloud service providers comply with DFARS clause 252.204-7012?

Assessing Contractor Implementation of NIST SP 800-171 Security Requirements

Q118: What is the *NIST SP 800-171 DoD Assessment Methodology*?

Q119: What is meant by a 'strategic' or 'corporate' assessment?

Q120: Will NIST SP 800-171 DoD Assessments be completed for a given facility at a specific location, as identified by the Commercial and Government Entity (CAGE) code, or by contractor?

Q121: How is the *NIST SP 800-171 DoD Assessment Methodology* different than *NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information*? Why is the DoD methodology needed?

Q122: What is the difference between a Basic, Medium, and High *NIST SP 800-171 DoD Assessment*?

Q123: How is a *NIST SP 800-171 DoD Assessment* scored?

Q124: Why are some requirements worth more points than others in the *NIST SP 800-171 DoD Assessment* Scoring Template?

Q125: How long are the results from a *NIST SP 800-171 DoD Assessment* valid? How often does the assessment need to be done? Annually?

Q126: Will there be a pass/fail scoring threshold utilized in the future?

Q127: How will Software as a Service solutions be scored? For example: Integration with Office 365, which holds a FedRAMP moderate certificate, may create an issue as the vendor will not share specific details with clients.

Q128: What is the Supplier Performance Risk System (SPRS)? Who can access SPRS?

Q129: Who can post *NIST SP 800-171 DoD Assessment* results to the Supplier Performance Risk System (SPRS)? What will be posted?

Q130: How are Plans of Action (security requirement 3.12.2) addressed in the NIST SP 800-171 Assessment results posted in Supplier Performance Risk System (SPRS)?

Q131: How will DoD use the results posted in to the Supplier Performance Risk System (SPRS)?

Q132: How do I know if the *NIST SP 800-171 DoD Assessment* results posted in Supplier Performance Risk System (SPRS) SPRS are for a contractor's Basic self-assessment, or for a Medium or High level assessment conducted by DoD?

Q133: Is the NIST SP 800-171 DoD Assessment required for contracts with DFARS clause 252.204-7012 and a requirement to protect DOD CUI?

Q134: If a prime contractor chooses to assess a subcontractor using this methodology, on what basis should it decide whether to assess at a 'Basic,' 'Medium' or 'High' level?

Q135: What is the maximum acceptable duration for which a "temporary deficiency" may be active?

Q136: Is a scheduled change management action sufficient for inclusion in a POAM? For example: Implementation issue identified, the solution is known and the remediation date set.

FREQUENTLY ASKED QUESTIONS AND ANSWERS:

Safeguarding Covered Defense Information and Cyber Incident Reporting (DFARS provision 252.204-7008 and DFARS clause 252.204-7012)

- **General**

Q1: When is DFARS clause 252.204-7012 required in contracts? Is the clause required in contracts for commercial items? Commercially available off-the-shelf (COTS) items?

A1: DFARS clause 252.204-7012 is required in all solicitations and contracts, including solicitations and contracts using Federal Acquisition Regulation (FAR) part 12 procedures for the acquisition of commercial items. The clause is not required for solicitations and contracts solely for the acquisition of COTS items. COTS is a commercial item that has been sold in the commercial marketplace in substantial quantities, and is offered to the government in a contract or subcontract without modification. Procurements solely for the acquisition of COTS items are extremely unlikely to involve covered defense information.

Commercial items include COTS, but also other commercial items that are or about to be available in the marketplace, but which also can be modified to meet Government requirements. If a commercial item must be modified to meet Government requirements, such modification may require the use and safeguarding of covered defense information, or the resulting service could be operationally critical for DoD. When the acquisition of commercial items involves covered defense information, such as in some cases when commercial items, services, or offerings are tailored to meet a particular customer's requirement, DFARS clause 252.204-7012 will apply to commercial items involving covered defense information.

The clause is not required to be applied retroactively, but that does not preclude a contracting officer from modifying an existing contract to add the clause.

Q2: When does DoD's purchase of a commercial item (sold to, but not developed for, DoD) mean that data associated with the item requires protection as covered defense information? For example, does a contract with DFARS clause 252.204-7012 for purchase of a standard commercial item, with a requirement to deliver the standard technical data package for that item (e.g., operations or maintenance data) with the only change to mark the cover page with a Controlled Technical Information Distribution Statement (e.g., Distribution D), mean the company now has to protect this data as covered defense information?

A2: No. In the example provided, commercial items (in this case, software) or their associated data are not considered covered defense information and their purchase by DoD

would not, alone, change that status. Superficial changes, such as marking a manual with a particular distribution statement, absent other substantive changes, would not mean such documents require protection as covered defense information. Substantive changes to a commercial item, documents describing its use or integration within DoD or as part of a DoD system or platform, etc., may be sensitive and require protection as covered defense information. This would only apply to the information/data related to the changes required by DoD however, not to the standard commercial item itself or associated data. When in doubt, consult with the Contracting Officer/Requiring Activity.

Q3: What is the purpose of DFARS clause 252.204-7012?

A3: DFARS clause 252.204-7012 was structured to ensure that controlled unclassified DoD information residing on a contractor's internal information system is safeguarded from cyber incidents, and that any consequences associated with the loss of this information are assessed and minimized via the cyber incident reporting and damage assessment processes. In addition, by providing a single DoD-wide approach to safeguarding covered contractor information systems, the clause prevents the proliferation of safeguarding controlled unclassified information clauses and contract language by the various entities across DoD.

Q4: How will the Department manage the multiple versions of DFARS clause 252.204-7012 that currently exist?

A4: The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations, build upon the table of NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, controls contained in the November 2013 version of DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. While there is additional effort for the difference, none of the effort to implement the original controls is lost. Due to the differences in the multiple versions of 252.204-7012, however, amending the contract requires contracting officer authority and is generally bilateral, requiring contractor signature. "Block changes" and "mass mods," generally reserved for administrative changes, such as a payment office address change, are not an option for this situation. There is nothing, however, that precludes a contracting officer from considering a modification of the contract upon request of the contractor. DoD guidance is for contracting officers to work with contractors who request assistance in situations where multiple versions of the rule are being implemented simultaneously, and when possible, work towards consistent implementation of the final version.

Q5: How can I change my contract to incorporate the current version of NIST SP 800-171? For example, I want to implement revision 1 of NIST SP 800-171 published in December 2016, but my contract was awarded before December 2016.

A5: Many companies utilize the same information system for multiple contracts, so it is possible that the updated standard is required by more recent contracts (and the covered information system is now required to conform to the current version of NIST SP 800-171.) However, when this is not the case, the contractor can request the contracting officer to modify the contract(s) to require implementation of the current version of NIST SP 800-171.

Q6: When must the requirements in DFARS clause 252.204-7012 be implemented?

A6: The requirements in DFARS clause 252.204-7012 must be implemented when covered defense information is processed, stored, or transits through an information system that is owned, or operated by or for, the contractor, or when performance of the contract involves operationally critical support. The solicitation/contract shall indicate when performance of the contract will involve, or is expected to involve, covered defense information or operationally critical support. All covered defense information provided to the contractor by the Government will be marked or otherwise identified in the contract, task order, or delivery order.

If performance of the contract does not involve covered defense information or operationally critical support, then the clause does not apply and compliance is not required. If the contract does involve covered defense information, but the information is not processed, stored or transmitted on the contractor's unclassified information system, the requirements related to covered defense information do not apply and compliance is not required.

You only have to implement the security requirements in NIST SP 800-171 if your contract includes DFARS clause 252.204-7012 AND you are provided covered defense information by DoD (or are developing covered defense information for DoD) AND you are processing, storing or transmitting that covered defense information on your information system/network.

DFARS clause 252.204-7012 does apply to contracts for commercial items, but not to contracts solely for the acquisition of commercial-of-the-shelf (COTS) items. If you are primarily selling commercial items and not modifying them for DoD (i.e., COTS), DFARS clause 252.204-7012 (even if included) and NIST SP 800-171 would not apply. If you are modifying a commercial item for DoD, and that modification involves covered defense information/DoD CUI that you process on your information system, DFARS 252.205-7012 and NIST SP 800-171 do apply. If in doubt, consult with the appropriate Contracting Officer.

Q7: Our Company has outsourced its IT support and systems to a third-party contractor. Are we still responsible for complying with DFARS clause 252.204-7012 and implementing NIST SP 800-171?"

A7: Outsourcing your IT to another company does not transfer your DFARS clause 252.204-7012 responsibilities or implementation of NIST SP 800-171 requirements. Your company is responsible and accountable for meeting the contractual obligations with the Government as per the contract. The key to successfully demonstrating compliance with DFARS clause 252.204-7012 and NIST SP 800-171 is having a well written contract with the third-party that describes your requirements, and includes deliverables that meet or exceed requirements to protect DoD CUI. If your IT service support is deemed to be less than or non-compliant with the contract, the company contracting with DoD is ultimately responsible.

Q8: Can the requirements in DFARS clause 252.204-7012, specifically the NIST SP 800-171 security requirements, be waived?

A8: DFARS clause 252.204-7012 does not allow for "waivers" to the NIST SP 800-171 security requirements. It does allow an offeror/contractor to propose variances from any of the security requirements specified by NIST SP 800-171. The offeror/contractor must submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of why a particular security requirement is not applicable, or how an alternative but equally effective security measure effectively meets the capability in order to satisfy a particular requirement and achieve equivalent protection. An authorized representative of the DoD CIO will adjudicate offeror/contractor requests to vary from NIST SP 800-171 requirements in writing (see DFARS clause 252.204-7012 (b)(2)(ii)(B) and FAQs 62-66).

Q9: Can you provide clarification with regard to what is a "Covered contractor information system"?

A9: DFARS clause 252.204-7012(a) defines "covered contractor information system" as "an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information." The final rule clarified that a covered contractor information system is specifically an ''unclassified'' information system. A covered contractor information system requires safeguarding in accordance with 252.204-7012(b) because performance of the contract requires that the system process, store, or transmit covered defense information.

Q10: When and how should DFARS clause 252.204-7012 flow down to subcontractors?

A10: DFARS clause 252.204-7012 flows down to subcontractors without alteration, except to identify the parties, when performance will involve operationally critical support or covered defense information. Per 252.204-7012(m)(1), the prime contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information, thus necessitating flow-down of the clause. The contractor should consult with the contracting office if clarification is required. The Department's emphasis is on the deliberate management of information requiring protection. Prime contractors should minimize the flow down of information requiring protection.

Flow down is a requirement of the terms of the contract with the Government, which should be enforced by the prime contractor as a result of compliance with these terms. If a subcontractor does not agree to comply with the terms of DFARS clause 252.204–7012, then covered defense information shall not be on that subcontractor's information system.

Q11: In working with foreign subcontractors, how do we resolve issues with clause requirements (e.g., reporting cyber incidents or providing digital images to DoD) that cannot be flowed down due to a conflict with local laws?

A11: The DFARS is generally written for U.S. contractors, and does not consider complications introduced by foreign partners/sub-contractual relationships. Potential conflicts have been identified between the requirements of DFARS clause 252.204-7012 and existing country agreements/national laws in areas such as the reporting of cyber incidents directly to the DoD, the submission of malware and media to the DoD, and providing access to information and equipment. OUSD(A&S), OUSD(R&E), and DoD CIO are currently working with the Defense Technology Security Administration (DTSA), under OUSD(Policy), to resolve these potential conflicts on a country-by country basis, and to provide guidance for U.S. Contractors on how to implement the rule within National Law and Country Agreements. Contractors should notify the Department at osd.dibscia@mail.mil if they require assistance with regard to this issue.

Q12: What are the cost recovery options for complying with DFARS clause 252.204-7012?

A12: DoD does not develop ''cost recovery models'' for compliance with DFARS rules. The requirements levied by this rule should be treated the same as those levied by any other new DFARS rule and the cost related to compliance should be considered during proposal preparation. Contractors should continue to comply with their own internal accounting processes. Contractors should consult with their Audit Compliance/ Accounting/Finance departments for guidance on this matter. If the contractors' Audit Compliance/Accounting/Finance departments have any questions regarding this matter they should contact their cognizant Defense Contract Management Administration and/or Defense Contract Audit Agency offices.

Q13: Can primes/higher tiered subcontractors include the cost associated with regulatory compliance of their next lower tiered covered defense information suppliers in proposals on solicitations including the 252.204-7008 provision and 252.204-7012 clause? Is the cost chargeable to specific contracts where there is an expectation for this level of regulatory compliance oversight?

A13: Unless prohibited by the FAR/DFARS, all costs associated with compliance of DFARS clause 252.204-7012 are allowable.

Q14: Who in DoD can I contact for clarification on DFARS clause 252.204-7012 or NIST SP 800-171 in support of DFARS clause 252.204-7012?

A14: Contractors should email their query to osd.dibcsia@mail.mil. Emails received at this address are reviewed daily and distributed as appropriate to a cross-functional team of subject matter experts for action.

Q15: Will the DOD certify that a contractor is compliant with the require security requirements?

A15: No. No new oversight paradigm is created through this rule.

Compliance with DFARS clause 252.204-7012 requires contractors/subcontractors to comply with all requirements in the clause. By signing the contract, the contractor agrees to comply with the contract terms. If oversight related to these requirements is deemed necessary, then it can be accomplished through existing FAR and DFARS allowances, or an additional requirement can be added to the terms of the contract. DoD can validate compliance in this way, but will not certify that a contractor is compliant with DFARS clause 252.204-7012.

An implemented system security plan and associated plans of action for any planned implementations or mitigations demonstrate implementation or planned implementation of the security requirements in NIST SP 800-171.

USD(A&S) memorandum, "Assessing Contractor Implementation of Cybersecurity Requirements," dated November 14, 2019, provides a standard DoD methodology to assess a contractor's implementation of the security requirements in NIST SP 800-171. The NIST SP 800-171 DoD Assessment Methodology, available at https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.1%20%203.13.2020.pdf, is intended for assessment purposes only and does not add any substantive requirements to either NIST SP 800-171 or DFARS clause 252.204-7012.

Q16: Is a 3rd Party assessment of compliance required?

A16: 3rd party (that is, an outside commercial company) assessments or certifications are not required, authorized, or recognized by DoD to assert compliance with DFARS clause 252.204-7012. By signing the contract, the contractor agrees to comply with the terms of the contract.

In order to safeguard covered defense information, companies with limited cybersecurity expertise may choose to seek outside assistance in determining how best to meet and implement the NIST SP 800-171 requirements in their company. But, once the company has implemented the requirements, there is no need to have a separate entity assess or certify that the company is compliant with DFARS clause 252.204-7012.

Q17: Does the Government intend to monitor contractors to ensure implementation of the required security requirements?

A17: Yes, but the DFARS rule did not add any unique or additional requirement for the Government to monitor contractor implementation of the required security requirements. Contractor compliance with these requirements would be subject to any existing generally applicable contractor compliance monitoring mechanisms.

Where applicable, DCMA, as part of its Contract Receipt and Review process, will verify that applicable cybersecurity clauses are in the contract. In addition, as part of its normal software surveillance activities, DCMA personnel will engage with contractors to implement the following actions in regards to cyber-security:

- Verify that the contractor has a system security plan and associated plans of action as appropriate. DCMA will not perform a technical assessment of the system security plan against the NIST 800-171 security requirements.
- Verify that the contractor possesses the necessary DoD approved External Certificate Authority (ECA) issued medium assurance public key infrastructure (PKI) certificate required to report cyber incidents.
- If DCMA detects or is made aware of a potential cybersecurity issue, DCMA will notify the contractor, DoD program office, and the DoD CIO.
- As required, facilitate the entry of government external assessment team into applicable contractor facilities via coordination with cognizant government and contractor stakeholders.

In June 2019, DCMA's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), in partnership with DIB companies, initiated an effort to review contractor adherence to NIST SP 800-171 security requirements. Using the *NIST SP 800-171 DoD Assessment Methodology* (available at https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.1%20%203.13.2020.pdf) the

DIBCAC can strategically assess a contractor's implementation of NIST SP 800-171 on existing contracts which include DFARS clause 252.204-7012, and can provide DoD Components with visibility to the summary level scores of strategic assessments completed by DoD, thus providing an alternative to a contract-by-contract assessment approach.

The Department is pursuing implementation of the *NIST SP 800-171 DoD Assessment Methodology* via DFARS Case 2019-D041, Strategic Assessment and Cybersecurity Certification Requirements.

Q18: Will Prime Contractors be responsible for the auditing of their sub-contractors? If so, how will compliance be demonstrated? How does a small company audit their supply chain?

A18: The prime contractor is responsible for executing the flow down requirements for this rule. The prime contractor may use whatever mechanisms it normally employs to audit or evaluate its subcontractors.

The Defense Contract Management Agency (DCMA) can now leverage their review of contractor purchasing systems in accordance with DFARS clause 252.244-7001, Contractor Purchasing System Administration, to review contractor cybersecurity procedures. In accordance with USD(A&S) memorandum, Subject: Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review, dated January 21, 2019, DCMA updated the Contractor Purchasing System Review Guidebook, available at https://www.dcma.mil/Portals/31/Documents/CPSR/CPSR_Guidebook_062719.pdf, to address the review of contractor procedures to ensure contractual requirements for identifying/marking DoD CUI flow down appropriately to their Tier 1 Level Suppliers, and the review of contractor procedures to assess compliance of Tier 1 Level Suppliers with DFARS clause 252.204-7012 and NIST SP 800-171.

Q19: What are the consequences for non-compliance? The system security plan allows organizations to extend the deadline for full compliance by building a plan of action to address planned implementation of security requirements. Will there be follow-on reviews of these plans and monitoring of a company's efforts to achieve full compliance?

A19: As noted in Chapter 3 of NIST SP 800-171, Revision 1, the system security plan and associated plans of action demonstrate the nonfederal organization's implementation or planned implementation of the security requirements. The system security plan and plans of action may also be considered by the requiring activity in an overall risk management decision to determine whether it is advisable to pursue a contract with the contractor, or to determine what other actions can be taken to achieve an acceptable level of risk. Under these conditions, the contract may include a provision to review progress in implementing the plan(s) of action.

DFARS clause 252.204-7012 did not change the existing penalties or remedies for noncompliance with any contract requirements. The rule does not direct contracting officers or the requiring activity towards specific actions to take in circumstances when a contractor is noncompliant. Oversight to verify compliance can be specified on case-by-case basis depending on the risk involved on a contract in accordance with the quality assurance surveillance plan that is in place.

Depending on the contract terms and factual circumstances, and on a contract-by-contract basis, the Government may consider the following actions in the event a contractor fails to comply with contract terms and conditions:

- Contractual
  - Withhold payment for non-compliant contract performance
  - Disapprove business system/contractor purchasing system
  - Decline to issue future orders on contract
  - Decline to exercise future contract options
  - Document negative past performance rating
  - Issue a stop work order
  - Issue a cure notice
  - Issue a show cause notice
  - Consider contract termination proceedings
  - Find the contractor non-responsive
  - Issue the contractor a Corrective Action Request (CAR)
- Administrative/Judicial
  - Suspension and Debarment proceedings
  - Pursuit of civil claims/penalties
  - Pursuit of criminal prosecution/penalties

Q20: How often should our company review our compliance to the NIST SP 800-171 security requirements?

A20: When compliance with DFARS clause 252.204-7012 requires implementation of NIST SP 800-171, the company is required to implement the following requirements in order to assess the risk and security of their system (s):

- Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI (NIST SP 800-171 security requirement 3.11.1)

- Periodically assess the security controls in organizational systems to determine if the controls are effective in their application (NIST SP 800-171 security requirement 3.12.1)
- Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems (NIST SP 800-171 security requirement 3.12.2)
- Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls (NIST SP 800-171 security requirement 3.12.3)
- Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems (NIST SP 800-171 security requirement 3.12.4)

A discussion of each of these requirements, to include frequency, can be found in chapter three of the NIST SP 800-171, and in sections 3.11 and 3.12 of the NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information.

- **Covered Defense Information**

Q21: Who is responsible for identifying/marking covered defense information?

A21: The requiring activity is responsible for:

- Identifying the requirement for covered defense information in the solicitation/contract
- Notifying the contracting officer when a solicitation is expected to result in a contract that will require covered defense information to be furnished by the Government and/or developed or delivered by the contractor;
- Marking or otherwise identifying information that will be provided to the contractor in support of the performance of the contract; and
- Determining if covered defense information will be collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

The contracting officer shall ensure covered defense information is marked or otherwise identified in the contract, task order, or delivery order, and ensure that the contract, task order, or delivery order includes the requirement, as provided by the requiring activity (such as a contract data requirements list) for the contractor to mark covered defense information developed in the performance of the contract. The prime is responsible for the safeguarding of covered defense information throughout its entire supply chain.

Q22: What information should be identified/marked in accordance with DFARS clause 252.204-7012?

A22: Any information provided by or developed for DoD that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies should be safeguarded in accordance with DFARS clause 252.204-7012. The Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html is a public registry of authorized categories and subcategories of information that require safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies. DoDM 5200.01 Volume 4, DOD Controlled Unclassified Information, and DoDI 5230.24, Distribution Statements on Technical Documents, describes the DoD information that requires safeguarding or dissemination controls. DoDM 5200.01 Volume 4 and DoDI 5230.24, Distribution Statements on Technical Documents, also describe the procedures to designate, mark and disseminate DoD CUI. In the DoD, such information typically includes controlled technical information (CTI), export control, proprietary, Privacy, and Foreign Government Information.

DoD Instruction (DoDI) 5200.48 Controlled Unclassified Information (CUI), was published on March 6, 2020, replacing and cancelling DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information." The new instruction establishes the official DoD CUI Registry, which provides an official list of the Indexes and Categories used to identify the various types of DoD CUI. The DoD CUI Registry mirrors the National CUI Registry, but provides additional information on the relationships to DoD by aligning each Index and Category to DoD issuances.

Q23: How will covered defense information that is provided to the contractor by or on behalf of DoD in support of the performance of the contract be identified/marked?

A23: The requiring activity should identify the requirement for covered defense information in Section C, Description/Specifications/Work Statement, of the contract.

The requiring activity should mark the covered defense information in accordance with DoDM 5200.01 Volume 4 and DoDI 5230.24. DoDM 5200.01, Volume 4, provides procedures for the designation, marking, and dissemination of DoD CUI. DoDI 5230.24, establishes the DoD methodology to apply a secondary distribution, release, and dissemination marking without additional approvals/authorizations. The requiring activity may also provide Government Furnished Information (GFI) that contains safeguarding or dissemination controls in Section J of the contract.

DoD Instruction (DoDI) 5200.48 Controlled Unclassified Information (CUI), published on March 6, 2020, replaces and cancels DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information," and addresses the essential marking requirements for initial phased implementation of the DoD CUI Program. Newly created CUI documents will have to be marked using the new CUI markings addressed in DoDI 5200.48, and a revision to DoDI 5230.24, Distribution Statements on Technical Documents, will be forthcoming. Specific marking requirements will be promulgated by the USD(I&S) in future guidance.

Q24: How will covered defense information that is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract be marked?

A24: The marking requirements will typically be found in Block 9 of the Contract Data Requirements List (CDRL), which is located in Section J, List of Attachments. If the contract does not contain a CDRL, the marking requirements may also be found in Section C.

Q25: Is information identified as FOUO considered to be covered defense information?

A25: Information that is identified as For Official Use Only (FOUO) alone does not indicate that it is covered defense information. Information identified as FOUO should only be treated as covered defense information when the information falls within the definition of covered defense information. In order for information marked as FOUO to require safeguarding, it must also include the applicable dissemination, release, and where appropriate, distribution statements pursuant to and consistent with law, regulation, or government-wide policies. Most FOUO information does not meet this requirement. DoD Manual 5200.01, DoD Information Security Program: Controlled Unclassified Information (CUI), Volume 4, Enclosure 3, described processes and procedures for applying FOUO markings.

Requiring activities/contracting officers should not identify all FOUO to contractors as covered defense information. However, there may be cases where the covered defense

information provided by requiring activities (e.g., privacy information) may be marked as FOUO. For contracts that include requirements for FOUO markings, continue to use this marking until otherwise directed.

DoD Instruction (DoDI) 5200.48 Controlled Unclassified Information (CUI), published on March 6, 2020, replaces and cancels DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information." The cancellation of this issuance cancels the marking of FOUO.

Q26: What is Controlled Technical Information (CTI)?

A26: Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

"Technical information" means technical data or computer software, as those terms are defined in the clause at DFARS clause 252.227-7013, Rights in Technical Data—Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

The authoritative source for the term 'controlled technical information' is DoDI 5230.24, Distribution Statements on Technical Documents.

DoD Instruction (DoDI) 5200.48 Controlled Unclassified Information (CUI), was published on March 6, 2020, replacing and cancelling DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information." The new instruction states that the USD(R&E):

- Establishes a standard process to identify CTI; guidelines for sharing, marking, safeguarding, storing, disseminating, decontrolling, and destroying CTI; and CTI records management requirements contained in contracts, as appropriate., and
- Establishes DoD CUI processes, policies, and procedures for grants and cooperative research and development arrangements, agreements, and contracts involving controlled technical information (CTI).

DoDI 5230.24, Distribution Statements on Technical Documents, will be revised to align with DoDI 5200.48.

Q27: If a Contract document (i.e., DD Form 1423-1) mandates the use of a Distribution Statement (B-F) on a contractor generated document for submission to the government but does not use the term CUI, should the contractor understand the document to be CUI and protect/control accordingly? Is it correct to say that any document with a Distribution Statement B-F is CUI?

A27: CUI, as defined by 32 CFR 2002, 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. Because Distribution Statements B-F as set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents, are in fact 'dissemination controls', this information is – by definition – CUI.

Q28: Should export controlled information be treated as covered defense information?

A28: Export control is considered covered defense information when it 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 support of 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. When DoD contractors hold information that is export controlled and is related to the DoD activity in performance of the contract, the information requires safeguarding. See DoDI 5230.24 for procedures for marking export controlled information.

Q29: When export controlled information meets the procedures in DoDI 5230.24 for controlled technical information, which also meets the definition of covered defense information, does that mean that I now need to protect all of my export-controlled information, which previously had no such requirement? How does this affect EAR99 items?

A29: The clause only applies to export-controlled information that meets the definition of covered defense information. While export control is a category of information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies (described in DoDI 5230.24), generally the type of export controlled information provided to the contractor by the DoD or collected, developed, received, transmitted, used, or stored by the contractor for DoD (necessary conditions to be considered covered defense information) is also Controlled Technical Information (CTI).

The requirement to safeguard covered defense information does not have any effect on the EAR99 designation. DFARS clause 252.204-7012 requires the contractor to provide adequate security on the information systems that process, store, or transmit covered defense information – it does not assign any specific safeguarding requirements to the information itself. The fact that the export-controlled information (which may also be designated as EAR99) is covered defense information does not have any effect on the EAR99 designation which applies to the information itself.

Q30: Can you provide common examples of Proprietary CUI? This category could raise big challenges in the area of business development and proposals and things such as employee rosters, quality processes etc.

A30: General Proprietary Business Information is described in the CUI Registry as "Material and information relating to, or associated with, a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications." The CUI Registry also includes the category General Procurement and Acquisition. It is described as "Material and information relating to, or associated with, the acquisition and procurement of goods and services, including but not limited to, cost or pricing data, contract information, indirect costs and direct labor rates." Information falling into either of these categories would require safeguarding in accordance with DFARS clause 252.204-7012.

Q31: What should the Contractor do if covered defense information or operationally critical support is not identified in the contract, task order, or delivery order, and the Contractor becomes aware of covered defense information or operationally critical support during performance of the contract?

A31: Contact the contracting officer.

Q32: What is meant by the phrase "by or on behalf of DoD in support of the performance of the contract" in the definition of covered defense information?

A32: "In support of performance of the contract" refers to covered defense information (controlled technical information or other information requiring safeguarding or dissemination controls) that is provided by DoD or developed, produced or used by a contractor to produce the product or service being contracted for. It is meant to include any covered defense information used in performance of the contract and exclude other information that may be developed by the contractor but not associated with contract performance. It does NOT mean that all information used by the contractor to support contract performance, e.g., information in the contractor's human resources or financial/accounting systems, is considered to be covered defense information.

Q33: What is the relationship between Controlled Unclassified Information (CUI), as defined in the National Archives and Record Administration (NARA) final rule published in the Federal Register on September 14, 2016 (81 FR 63324), DoD CUI, and covered defense information? Are the definitions aligned?

A33: CUI is information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls.

Covered defense information is a term used to identify information that requires protection under DFARS clause 252.204-7012 and is consistent with DoDI 5200.48, CUI. DoDI 5200.48 establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD in accordance with Part 2002 of Title 32, Code of Federal Regulations (CFR). Like CUI, covered defense information applies to DoD controlled unclassified information, as described in DoDI 5200.48, CUI, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. This ensures that even if the CUI Registry changes, covered defense information will continue to be aligned with the CUI categories and subcategories.

Covered defense information requires protection under DFARS clause 252.204-7012 only if the information is EITHER marked or otherwise identified in the contract, task order, or delivery order and provided to contractor by or on behalf of, DoD in support of the performance of the contract; OR collected, developed, received, transmitted, used, or stored by, or on behalf of, the contractor in support of the performance of the contract.

Like CUI, adequate security for covered defense information requires, at a minimum, the implementation of NIST SP 800-171. DFARS clause 252.204-7012(l) further states the safeguarding requirements in the clause in no way abrogate the Contractor's responsibility

to comply with other applicable clauses of the contract, or as a result of other applicable U.S. Government statutory or regulatory requirements. This statement accounts for any added requirements that may result from covered defense information that is categorized as CUI specific.

Q34: Will contract documents clearly identify specific items/documents that are CUI using the term 'Controlled Unclassified Information (CUI)'?

A34: DoDI 5200.48, Controlled Unclassified Information (CUI), published on March 6, 2020 by OUSD(I&S), replaces/cancels DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information," and addresses the essential marking requirements for initial phased implementation of the DoD CUI Program. OUSD(I&S) published CUI Marking Guidelines to accompany the DoDI 5200.48 on May 18, 2020. The guidelines state that, at a minimum, CUI markings for newly created unclassified documents will include the acronym "CUI" at the top and bottom of each page. The requiring activity should identify the requirement for DoD CUI in Section C, Description/Specifications/Work Statement, of the contract, and mark DoD CUI in accordance with DoDI 5200.48 and DoDI 5230.24, Distribution Statements on Technical Documents.

- **Operationally Critical Support**

Q35: What is "Operationally Critical Support"? How will it be identified?

A35: Operationally critical support is defined as supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation. The contract will include notification of when the contractor will provide operationally critical support.

DoD identifies three types of operationally critical support. Examples include but are not limited to the following:

i. Operationally critical support for mobilization, which is addressed under (ii) and (iii).
ii. Operationally critical support for distribution includes, but is not limited to:
    a. Airlift, sealift, aeromedical, and intermodal transportation services and their associated material handling and ground handling labor or stevedore services.
    b. U.S. railroad, truck, barge, ferry, and bus services provided by passenger and freight carriers and their associated material handling and ground handling labor services.
    c. Third party logistics (3PL) services provided by non-equipment owned brokers and freight-forwarders.

d. Transportation Protection Services for arms, ammunition, and explosives (AA&E) and courier materiel.
e. Transportation and packaging of hazardous material.
f. Information technology systems and network providers essential to the command, control operation, and security of contingency transportation mission functions delineated in “a” through “e”.

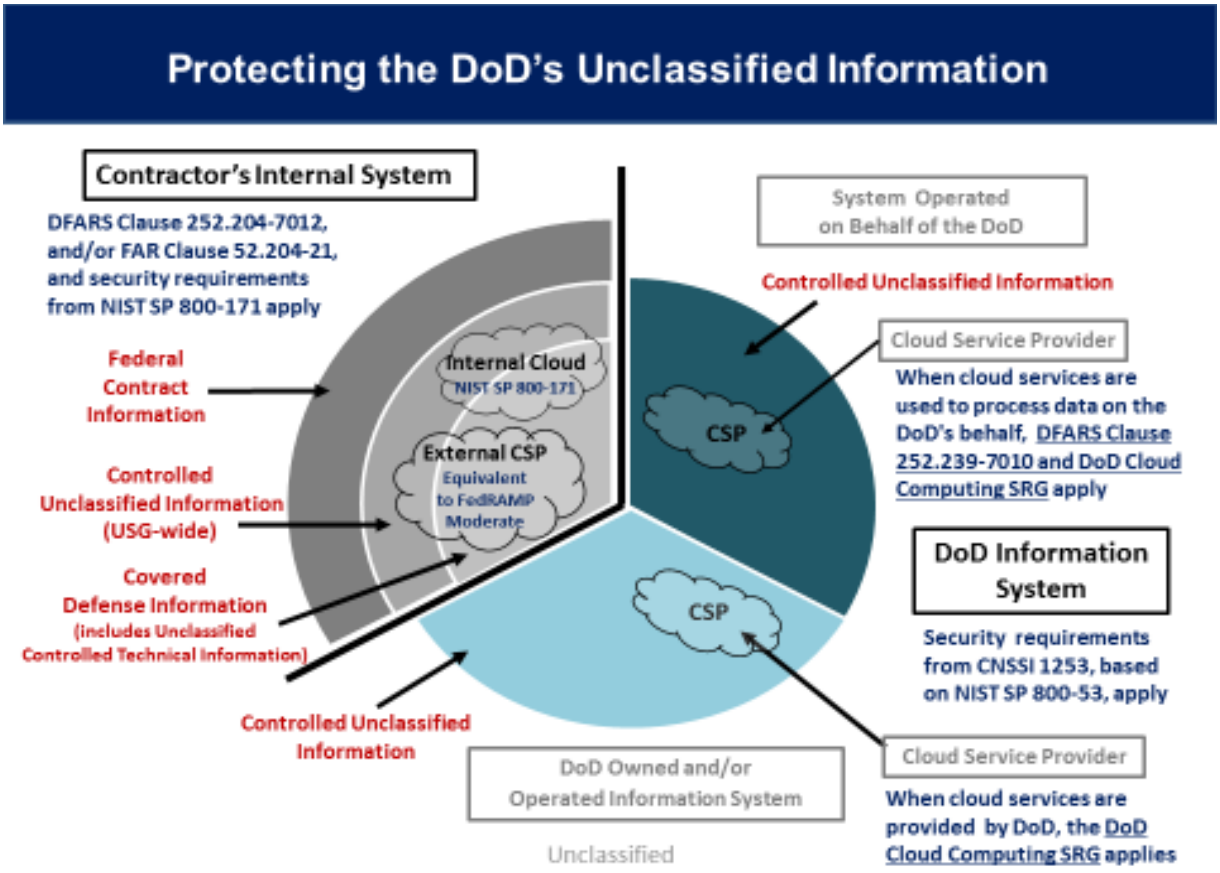
iii. Operationally critical support for sustainment includes, but is not limited to:
a. Local acquisition of liquid logistics (water, fuel-all types); Class 1, fresh fruits and vegetables; local meat/bread products, and bottled gases (e.g., helium, oxygen, acetylene).
b. Supply chain for rare earth metals.
c. Procurement and product support for critical weapons systems identified by the requiring activity.
d. The prime contractors and subcontractors for critical weapons systems in development and sustainment that are fielded to the Area of Responsibility (AOR).
e. Contractor Logistics (maintenance and supply) Support.
f. Depot-level maintenance for critical items, particularly in Public-Private Partnerships.
g. Information technology systems and network providers essential to the command, control operation, and security of contingency supply and maintenance mission functions delineated in “a” through “f”.

The contracting officer will be notified by the requiring activity when the contractor will provide operationally critical support. The contracting officer shall ensure that notification of operationally critical support provided is included in the contract, task order, or delivery order.

- **Safeguarding Covered Defense Information**

Q36: How are the security protections required for a contractor's internal information system different than the protections required for a DoD information system?

A36: The protections required to protect Government information are dependent on the type of information we are protecting, and on the type of system on which the information is processed or stored. The following diagram illustrates the requirements for protecting covered defense information, controlled unclassified information, and Federal contract information when processed or stored on a contractor's internal information system, or on a DoD information system. For a more thorough description of this diagram, go to Cybersecurity in DoD Acquisition Regulations page at http://dodprocurementtoolbox.com/.



Q37: Why did the security protections required by DFARS clause 252.204-7012 change from a table of selected NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, security controls to NIST Special Publication (SP) 800-171? How does NIST SP 800-171 compare to NIST SP 800-53?

A37: The change in required security protections was made for several reasons. The full set of NIST SP 800-53 security controls is intended for internal use by the Federal Government.

It contains requirements that often do not apply to a contractor's internal information system, which is why the November 2013 publication of DFARS clause 252.204-7012 included only a subset of those controls. In contrast, the NIST SP 800-171 security requirements were developed specifically to be applied to, and by, nonfederal organizations. They are performance-based to avoid mandating specific solutions, and to make it easier to apply to existing systems in use by industry. NIST SP 800-171 also provides a standardized and uniform set of requirements for all CUI security needs, allowing nonfederal organizations to comply with statutory and regulatory requirements, and to consistently implement safeguards for the protection of this information.

It is important to note that the contracting officer should ensure that the requiring activity describes the security requirements and assessments based on the contents of NIST SP 800-171 and its Basic and Derived Security Requirements only, and not on NIST SP 800-53 security controls, i.e., they should not reference a NIST SP 800-53 control (e.g., AC-4) in order to identify a NIST SP 800-171 security requirement (e.g., 3.1.3).

DFARS clause 252.204-7012 amends the security controls required to provide "adequate security" – replacing a table of controls based on NIST SP 800-53, with security requirements found in NIST SP 800-171. A comparison of these requirements is shown below:

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations	**NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations, June 2015**
• Facilitates consistent and repeatable approach for selecting/specifying security controls • Uniquely Federal (i.e., primarily the responsibility of the Federal Government) • Controls address diverse set of security and privacy requirements across Federal Government/critical infrastructure	• Developed for use on contractor and other nonfederal information systems to protect CUI. • Tailored to eliminate requirements that are: – Uniquely Federal – Not related to CUI – Expected to be satisfied without specification (i.e., policy and procedure controls)
• "Build It Right" strategy provides flexible yet stable catalog of security controls to meet current information protection needs and the demands of future needs-based threats, requirements, and technologies	• Enables contractors to comply using systems and practices they already have in place • Intent is not to require the development or acquisition of new systems to process, store, or transmit CUI
• Provides recommended security controls for information systems categorized in accordance with FIPS 199, Standards for	• Provides standardized/uniform set of requirements for all CUI security needs • Allows nonfederal organizations to consistently implement safeguards for

Security Categorization of Federal Information and Information Systems • Allows organizations to tailor relevant security control baseline to align with their mission/business environment	the protection of CUI (i.e., one CUI solution for all customers) • Allows contractor to implement alternative, but equally effective, security measures to satisfy every CUI security requirement

Q38: How should a contractor deal with a situation where HIPAA applies, in addition to the protections required by NIST SP 800-171??

A38: Data falling under the Health Insurance Portability and Accountability Act (HIPAA) has always required protections (HIPAA Security Rule, 45 CFR Parts 160 - 164) in addition to and beyond the scope of the NIST SP 800-171. DFARS clause 252.204-7012 addresses such out of scope protections at section (l) Other safeguarding or reporting requirements, which states "The safeguarding requirements in this clause in no way abrogate the Contractor's responsibility to comply with other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements."

NIST SP 800-66, "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule," provides a cross-reference in Appendix D to related NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, security controls. A similar cross-reference of NIST SP 800-171 requirements to NIST SP 800-53 controls is provided in Appendix D to NIST SP 800-171. The tables in NIST SP 800-171 can be used to identify which requirements of the HIPAA security rule have been accomplished by implementing NIST SP 800-171 and what additional security requirements may need to be implemented to fully address the HIPAA requirements.

- **Cyber Incidents and Reporting**

Q39: Cyber incidents are defined as "a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein." Can you provide examples of cyber incidents that have an "adverse effect" and cyber incidents that have a "potential adverse effect" to help clarify the differences?

A39: An example of a cyber incident where there is an adverse effect would be when covered defense information is exfiltrated from a contractor information system or network. An example of a potential adverse effect would be the discovery of malware on a contractor information system or network that was not blocked (e.g., by antivirus, or endpoint protection). In that case, malware was delivered via some mechanism and may or may not have affected covered defense information. Additionally, a "denial of service attack" potentially presents an

adverse effect on the information system associated with operationally critical support and would be reportable.

Q40: If a workstation without covered defense information has antivirus software installed and operating, but malware gets through the antivirus software and gets installed and not activated on the workstation, and the workstation is part of a covered contractor information system, is this considered a cyber incident?

A40: Yes, this is a cyber incident in that it resulted in a 'potentially adverse effect' on a covered contractor information system. While antivirus software is a requirement in the NIST SP 800-171, it may not detect when malware is executed. Since the workstation is part of the covered contractor information system the execution of the malware could be used to enable lateral movement across the covered contractor information system.

Q41: If a commercial sandbox/detonation chamber is used as part of a workstation's protection, and malware is launched in the sandbox/detonation chamber, is that still considered a cyber incident?

A41: No, this would not be considered a cyber incident. The protections worked as designed, preventing an actual or potentially adverse effect.

Q42: When and how does the Contractor report a cyber incident?

A42: Per DFARS clause 252.204-7012, a report is required when the contractor discovers a cyber incident that affects a covered contractor system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support. Per DFARS clause 252.239-7010, the contractor shall report all cyber incidents that are related to the cloud computing service provided under the contract. If there is evidence of an intrusion to the network, there is a potentially adverse effect on the information/information system and would be reportable.

When reporting a cyber incident under DFARS clause 252.204-7012 or DFARS clause 252.239-7010, the contractor will access the DIBNet portal (https://dibnet.dod.mil) and complete the fields in the Incident Collection Format (ICF). Access to this form requires a DoD-approved medium assurance public key infrastructure (PKI) certificate. In the event a company does not have anyone with a DoD-approved medium assurance certificate, they may contact the DoD Cyber Crime Center (DC3) (contact information is also on the portal) for additional information. The DIBNet portal is DoD's single reporting mechanism for DoD contractor reporting of cyber incidents on the contractor's unclassified information systems. The rule streamlines the reporting processes for DoD contractors and minimizes duplicative reporting processes.

Q43: How can the contractor obtain DoD-approved medium assurance External Certificate Authority (ECA) certificate in order to report?

A43: For information on obtaining a DoD-approved ECA certificate, please visit the ECA website at https://public.cyber.mil/eca/.

Q44: What should the contractor do when they do not have all the information required by the clause within 72 hours of discovery of any cyber incident?

A44: When a cyber incident is discovered, the contractor/subcontractor should report whatever information is available to the DIBNet portal (https://dibnet.dod.mil) within 72 hours of discovery. If the contractor/subcontractor does not have all the information required on the Incident Collection Form (ICF) at the time of the report, the contractor should submit a follow-on report when additional information becomes available.

Q45: What happens when the contractor submits a cyber incident report?

A45: When a cyber incident report is submitted to DoD via https://dibnet.dod.mil, the DoD Cyber Crime Center (DC3) reviews the report, provides a copy to the Contracting Officer(s) identified on the report, and conducts analysis to identify trends. The contracting officer is directed in the DFARS Procedures, Guidance and Information (PGI) 204.7303-3 to provide the cyber incident report to the requiring activities whose contracts were affected.

The DoD Cyber Crime Center (DC3) serves as the DoD operational focal point for receiving cyber incident reporting. DC3 also receives malicious software from defense contractors.

Q46: How are subcontractors required to report cyber incidents? Can you provide clarification regarding the types of information that must be disclosed by a subcontractor to a prime contractor?

A46: The rule clarifies that subcontractors who are required to safeguard covered defense information in accordance with DFARS clause 252.204-7012 are required to rapidly report cyber incidents directly to DoD at https://dibnet.dod.mil, and to provide the incident report number, automatically assigned by DoD, to the prime contractor (or next higher-tier subcontractor) as soon as practicable. Any requirement for the subcontractor to provide anything more than the incident report number to the prime contractor (or next higher-tier subcontractor) is a matter to be addressed between the prime and the subcontractor. The DoD will protect against the unauthorized use or release of cyber incident information reported by the contractor or subcontractor in accordance with applicable statutes and regulations.

Q477: Does the requirement at DFARS clause 252.204-7012(e) to "preserve… all relevant monitoring/packet capture data…" imply that there is a requirement to do packet capture?

A47: No, it does not mean that there is a requirement to do packet capture – but if a contractor is doing packet capture and there is a cyber incident – the contractor is requested to preserve all relevant monitoring/packet capture data in accordance with 252.204-7012(e).

Q48: How does the contractor submit media?

A48: The contracting officer will provide instructions for submitting media when a request to submit media is made. The contracting officer does not handle nor personally submit media.

- **Submission of Malicious Software**

Q49: If antivirus software identifies and quarantines a piece of malware as part of its check on a downloaded file, does the quarantined malware need to be submitted to the DoD Cyber Crime Center (DC3)? If so, is this considered a cyber incident?

A49: No, the malware identified by the antivirus software does not need to be submitted to the DoD Cyber Crime Center (DC3). If detected by antivirus software, then the malware is known to that vendor, and there is no requirement to submit the sample. If the antivirus detected and quarantined the malware as part of the download process, then the incident was prevented and a cyber incident did not occur. If the malware was detected during a scan of the system or when the file was executed, then a cyber incident did occur and must be reported.

- **Cyber Incident Damage Assessment**

Q50: What is meant by the language at 252.204-7009 (b)(5)(i) which states, "A breach of these obligations or restrictions may subject the contractor to criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States"?

A50: The statement quoted above is found in DFARS clause 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information. This clause limits the access, use, release, and disclosure of covered defense information by support services contractors directly supporting DoD activities related to safeguarding covered defense information and cyber incident reporting (e.g., providing forensic analysis services, damage assessment services, or other services that require access to data from another contractor), and requires contractors to ensure that their employees are subject to

use and non-disclosure obligations consistent with the clause. The clause operates as a non-disclosure agreement (NDA), authorizing DoD support contractors to access and use covered defense information "only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to clause 252.204-7012" (e.g., providing support for cyber incident report analysis and damage assessment processes). That quoted language in DFARS clause 252.204-7009 is not about compliance with the security requirements required by DFARS clause 252.204-7012, but about support contractors' misuse of third-party information they receive in supporting DoD cyber incident analysis and damage assessment processes.

- **Basic Safeguarding of Contractor Information Systems (FAR Clause 52.204.21)**

Q51: Will FAR clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, and DFARS clause 252.204-7012 be used in the same solicitation/contract?

Q51: Yes. The prescribed use of each of these clauses is not reliant on the inclusion of the other clause. Most solicitations/contracts that include covered defense information will also include information that is not covered defense information, but is Federal contract information that requires protection in accordance with the Basic Safeguarding FAR clause. In addition, it is likely that Federal contract information that is not covered defense information will be flowed down to a subcontractor even when covered defense information is not, and as such, the FAR clause will flow down, as well.

NIST SP 800-171

- **General Implementation Issues**

Q52: What is the difference between the Basic and Derived Requirements in NIST SP 800-171? Do all the requirements have to be met (i.e., if the Basic Requirement is met, does that mean the 'Derived' Requirements are met, since they are 'derived' from the Basic Requirement)?

A52: All the requirements, both Basic and Derived, must be separately met. As explained in Section 2.2 of NIST SP 800-171, the Basic Requirements come from FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, and the Derived Requirements come from NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. Since the FIPS 200 requirements are the most fundamental requirements, NIST refers to them as Basic Requirements. However, because FIPS 200 is a set of 'minimum' requirements, these are often insufficient to provide protection at the required "Moderate" impact level for covered defense information.

Accordingly, when the Basic Requirement does not fully meet the "Moderate" requirement, related controls from the "Moderate" baseline in NIST SP 800-53 are specified, and identified in NIST SP 800-171 as Derived Requirements (i.e., derived from NIST SP 800-53).

Q53: Is it appropriate for a program office or requiring activity to add to the NIST SP 800-171 security requirements, or to specify how a contractor should implement the various requirements in NIST SP 800-171 (e.g., specify password length or complexity, use of specific monitoring equipment, etc.)?

A53: No. The Department's intent of a single standard is undermined when individual elements in the DoD unnecessarily add to the NIST SP 800-171 requirements, establish separate cyber incident reporting requirements, or in other ways interfere with the contractor's management of its internal information system. It is problematic when DoD personnel impose requirements on the contractor's internal information systems that are meant to apply to DoD IT systems, or systems operated on DoD's behalf, and not to a contractor's internal IT system. This includes requirements placed on the contractor that can only be applied to government systems, adding unique cyber incident reporting, specifying security requirement parameters, requiring the RMF or DoD IT system governance and governance documentation, and reporting on the internal operations and maintenance of the contractor's system (including requesting details on the number and type of workstations, servers, applications/operating systems, firewalls, IDS/IPS in use).

DoD Components should restrict their security requirements to DFARS clause 252.204-7012 and NIST SP 800-171 unless there is a specific need to increase security above the "Moderate" impact level. Components can request a contractor describe, as part of the solicitation, how the requirements of NIST SP 800-171 are met, or have the contractor demonstrate compliance prior to or upon contract award. After contract award, it is reasonable to require the contractor to advise when there is a deficiency that affects DoD covered defense information and to periodically review how the requirements are being met and any deficiencies are being resolved. Components should not intrude into the operations or management of the contractor's internal IT system by specifying the content and format of the system security plan and plans of action that address deficiencies, requiring any specific method for validating and assessing the system, or specifying the parameters of security requirements.

Q53.1: Are there minimum standards for password length or complexity?

A53.1: Typically, specific requirement parameter values are left to the discretion of the nonfederal organization. NIST SP 800-63B, Digital Identity Guidelines - Authentication and Lifecycle Management, indicates that the minimum length for a password or PIN is to be at least 8 characters in length if chosen by the user. However, in cases where the DoD or a

DoD Component determines that the loss of confidentiality, integrity, or availability of DoD information could be expected to have a serious adverse effect on organizational assets or individuals on their systems or networks, more stringent password requirements may be necessary. For password-based authentication (i.e., when multifactor authentication is not yet implemented): the minimum password complexity, as supported by the device, is a minimum of 15 characters, 1 of each of the following character sets: Upper case, lower case, Numeric, Special characters [e.g., ~ ! @ # $ % ^ & * ( ) _ + = - ‘ [ ] / ? > <]). Additional guidelines are provided for devices that are unable to support the password requirements such as for Microsoft Windows 10 Mobile devices, the device must enforce a minimum password length of six characters and must not allow passwords that include more than two repeating or sequential characters. For Apple iOS 12, the device must be configured to enforce a minimum password length of six characters and be configured to not allow passwords that include more than two repeating or sequential characters.

Q53.2: Are there minimum requirements to configure session lock on systems and networks after periods of inactivity and unsuccessful logon attempts?

A53.2: Typically, specific requirement parameter values are left to the discretion of the nonfederal organization. In cases where the DoD or a DoD Component determines that the loss of confidentiality, integrity, or availability of DoD information could be expected to have a serious adverse effect on organizational assets or individuals on their systems and networks, more stringent security requirements may be necessary. These include requiring session locks after 15 minutes of inactivity and limiting unsuccessful logon attempts to three attempts.

Q54: What is the significance of the change in Revision 1 to NIST SP 800-171 from ‘information systems’ to ‘system.’

A54: DFARS clause 252.204-7012 requires the contractor implement NIST SP 800-171 on “covered contractor information systems.” The change in Revision 1 of NIST SP 800-171 from ‘information system’ to ‘system’ has no effect on how the clause is applied. The definition for ‘system’ in the NIST SP 800-171 Revision 1 glossary points to the definition of ‘information system’ which has not changed. As noted in the ‘gray box’ on page vi of Revision 1, the security requirements apply to more than just general-purpose information systems, but also, where possible, to special purpose information systems (e.g., industrial control systems, medical systems, manufacturing systems). This is not a change - these

special purpose systems were also addressed in the initial version of NIST SP 800-171 (in footnote 18 in chapter 3, page 8).

NIST SP 800-171 Revision 2, published on February 21, 2020, provides minor editorial changes in Chapters One and Two, and in the Glossary, Acronyms, and References appendices. There are no changes to the basic and derived security requirements in

Q55: Does the change from 'Information System' to 'System' mean that NIST SP 800-171 applies to individual devices, such as stand-alone test equipment?

A55: No, NIST SP 800-171 should not be applied to individual devices, even though they may have an IP address, unless such a device (e.g., a computer workstation) meets the definition of a covered contractor information system or is a component of such a system.

Q56: Why was the requirement for a system security plan added to Revision 1 of NIST SP 800-171?

A56: The system security plan was added to address several issues. While not explicitly included in the original version of NIST SP 800-171, the system security plan was identified in the tailoring table (Table E-12, PL-2) as "expected to be routinely satisfied by nonfederal organizations without specification." In other words, the government expected that every company had something that could be considered equivalent to a system security plan. Questions remained, however, about how certain things should be documented, demonstrated or managed - in particular, any enduring exceptions to the requirements to accommodate special circumstances (e.g., medical devices), or any individual, isolated or temporary deficiencies. This drove the need to add the system security plan as an explicit security requirement.

The system security plan also provides a mechanism to address, as part of the requiring activities overall risk management decision, situations in which all of the NIST SP 800-171 security requirements are not fully implemented on the covered contractor information system. If the requiring activity expects full implementation of all NIST SP 800-171 security requirements at time of contract award, this requirement should be specifically identified in the solicitation.

Specific examples of situations that can be addressed in the system security plan follow:

- New entrants to DoD or federal contracting who are working to implement some of the NIST SP 800-171 requirements, can be considered as having 'implemented NIST SP 800-171' if they identify in a system security plan the requirements that are yet to be implemented; develop associated plans of action to describe how unimplemented security requirements will be met, and any mitigations that are in place. It is the

responsibility of the requiring activity to determine the level of acceptable risk for requirements that are not yet implemented.

- Similarly, for companies with contracts that require implementation of NIST SP 800-171 by Dec 31, 2017 and unexpectedly discover they may not meet the deadline, the Rev 1 change provides an opportunity to address the unimplemented requirements through a system security plan and plan of action. This may require negotiations with the Contracting Officer, depending on the provisions of the contract, particularly if Rev 1 was not "in effect" when the contract was solicited.
- A question frequently asked by companies is 'how do I know what I've done meets the NIST SP 800-171 requirement? One of the requirements of the system security plan is that it describe how security requirements are implemented. So, if there is any concern, a company can include that portion of the System Security Plan with its technical proposal (and may subsequently be incorporated as part of the contract). These also may inform a discussion of risk between the contractor and requiring activity/program office.
- The System Security Plan should also be used to identify situations where elements of the NIST SP 800-171 requirements cannot practically be applied, or when events result in short- or long -term issues that have to be addressed by assessing risk and applying mitigations. As also provided in the DFARS clause at 252.204-7012 (b)(3), under Rev 1 the System Security Plan is used to describe any enduring exceptions to the requirements to accommodate special circumstances (e.g., medical devices, equipment or systems required to replicate the configuration of 'fielded' systems), any individual, isolated or temporary deficiencies based on an assessed risk or vulnerability per NIST SP 800-171 security requirements 3.11.1 and 3.12.1, and plans of action as provided by security requirement 3.12.2, to correct deficiencies and reduce or eliminate vulnerabilities.

Contracting Officers should insure that if the requiring activity expects compliance/ implementation of all NIST 800-171 security requirements at time of contract award [or perhaps at time of proposal] that this be identified as an additional, specific requirement in the solicitation (this is not explicitly required by the -7012 clause).

Q57: How can the DoD consider an offeror's implementation of NIST SP 800-171 in the source selection process?

A57: The intent of DFARS clause 252.204-7012 is to ensure that the security requirements in NIST SP 800-171 are applied to information systems that are owned by, or operated by or for contractors, and process, store, or transmit covered defense information. The clause is

not structured to require contractor implementation of NIST SP 800-171 as a mandatory evaluation factor in the source selection process, but the requiring activity is not precluded from stating in the solicitation that it will consider the contractor's implementation of NIST SP 800-171, as documented in the system security plan or otherwise, as part of the source selection process. Examples of how a requiring activity might proceed include:

- Notifying the offeror that its approach to protecting covered defense information and providing adequate security in accordance with DFARS clause 252.204-7012 will be evaluated in the solicitation on an acceptable or unacceptable basis. Proposal instructions and corresponding evaluation specifics of how implementation of NIST SP 800-171 will be used by the DoD to determine whether or not it is acceptable or unacceptable to process, store, or transmit covered defense information on a system hosted by the offeror must be detailed in sections L and M of the solicitation as well as the Source Selection Plan.
- Establishing compliance with DFARS clause 252.204-7012 as a separate technical evaluation factor and notifying the offeror that its approach to providing adequate security will be evaluated in the source selection process. The specifics of how the offeror's implementation of NIST SP 800-171 will be evaluated must be detailed in Sections L and M of the solicitation as well as the Source Selection Plan.

OUSD(A&S) memorandum, Guidance for Assessing Compliance and Enhancing Protections Required by DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, available at https://www.acq.osd.mil/dpap/pdi/cyber/guidance_for_assessing_compliance_and_enhancing_protections.html, provides guidance to assist acquisition personnel in the development of effective cybersecurity strategies to enhance existing protection requirements provided by DFARS clause 252.204-7012 and NIST SP 800-171, and encourages DoD Components to implement the guidance to address individual program needs and requirements.

Q58: If a contractor meets the requirements of NIST SP 800-171, can a DoD requiring activity use the evaluation/source selection process to define the acceptability of 'how' a contractor meets those requirements?

A58: No. NIST SP 800-171 was designed to provide a single set of government-wide security requirements for protection of CUI that can be applied to the wide variety of nonfederal organizations' information systems which may contain CUI. The intent of the DFARS clause 252.204-7012 is to have a DoD security standard for protecting covered defense information (i.e., CUI provided by or developed for DoD) and a single mechanism for reporting cyber incidents. Once a DoD contractor implements the NIST SP 800-171

security requirements, the contractor's system should meet the cybersecurity requirements of any DoD component, program office, or requiring activity.

Q59: How will the DoD account for the fact that compliance with NIST SP 800-171 is an iterative and ongoing process? The DFARS clause imposing NIST SP 800-171 requires that the entire system be in 100% compliance all the time, a condition that in practice (in industry or Government) is almost never the case.

For example:

- **It is not possible to apply session lock or termination (Requirements 3.1.10/11) to certain computers (e.g., in a production line or medical life-support machines).**
- **Applying a necessary security patch can "invalidate" FIPS validated encryption (Requirement 3.13.11) since the encryption module "with the patch" has not been validated by NIST.**
- **Segments of an information system may be incapable of meeting certain requirements, such as correcting flaws/patching vulnerabilities (Requirement 3.14.1) without disrupting production/operations that may be critical to the customer.**
- **How should a contractor deal with situations such as these?**

A59: The requirement at DFARS clause 252.204-7012 (b)(2)(i) to implement, at a minimum, the security requirements in NIST SP 800-171, is not intended to imply that there will not be situations where elements of the NIST SP 800-171 requirements cannot practically be applied, or when events result in short- or long-term issues that have to be addressed by assessing risk and applying mitigations. The rule allows a contractor to identify situations in which a required control might not be necessary or an alternative but equally effective control can be used, and the DoD CIO will determine whether the identified variance is permitted, in accordance with DFARS provision 252.204-7008(c)(2)(i) and (ii) and DFARS clause 252.204-7012(b)(2)(ii).

In addition, the dynamic nature of cybersecurity threats and vulnerabilities is recognized within the NIST SP 800-171. The contractor should address situations such as those listed above in accordance with the NIST SP 800-171 security requirements that follow:

- 3.11.1, Risk Assessment: Requires the contractor to periodically assess the risk associated with operating information systems processing CUI;
- 3.12.1, Security Assessment: Requires the contractor to periodically assess the effectiveness of organizational information systems security controls;

- 3.12.2, Security Assessment: Requires the contractor to "develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems;"
- 3.12.3, Security Assessment: Monitor security controls in an ongoing basis to ensure the continued effectiveness of the controls;" and
- 3.12.4, System security plan: Requires the contractor to "develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems."

The contractor should address issues, security requirement implementations in progress, special circumstances/enduring exceptions, and any individual, isolated or temporary deficiencies through "plans of action" (as described in security requirement 3.12.2) and in the system security plan (as described in security requirement 3.12.4). As provided at 252.204-7012 (b)(3), a system security plan may be used to describe how the system security protections are implemented, any exceptions to the requirements to accommodate special circumstances (e.g., medical devices), any individual, isolated or temporary deficiencies based on an assessed risk or vulnerability per NIST SP 800-171 security requirements 3.11.1, 3.12.1, and 3.12.3, and plans of action as provided by security requirement 3.12.2, to correct deficiencies and reduce or eliminate vulnerabilities identified through the assessment process.

Elements of the security plan may be included with the contractor's technical proposal (and may subsequently be incorporated as part of the contract). These also may inform a discussion of risk between the contractor and requiring activity/program office.

Q60: How might a small business with limited information technology (IT) or cybersecurity expertise approach meeting the requirements of NIST SP 800-171?

A60: NIST SP 800-171 was written using performance-based requirements, with the intent to not require the development or acquisition of new systems to process, store, or transmit controlled unclassified information (CUI), but enable contractors to comply using systems and practices they already have in place. It eliminates unnecessary specificity and includes only those security requirements necessary to provide adequate protection for the impact level of CUI (e.g., covered defense information).

Most requirements in NIST SP 800-171 are about policy, process, and configuring IT securely, while others require security-related software (such as anti-virus) or additional hardware (e.g., firewall).

For companies that were compliant with the 2013 Safeguarding of Unclassified Controlled Technical Information DFARS clause with the table of NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, controls, almost all the additional NIST SP 800-171 requirements can be accomplished by policy/process changes or adjusting the configuration of existing IT. With the exception of the multifactor authentication requirement (3.5.3), no additional software or hardware is typically required.

For companies new to the requirements, a reasonable approach would be to:

- Examine each of the requirements to determine
  - Policy or process requirements
  - Policy/process requirements that require an implementation in IT (typically by either configuring the IT in a certain way or through use of specific software)
  - IT configuration requirements
  - Any additional software required
  - Any additional hardware required.
- If unsure of what a requirement means, companies should refer to the mapping table in Appendix D to NIST SP 800-171, identify the corresponding NIST SP 800-53 control, and consult the Supplemental Guidance related to that control in NIST SP 800-53 [Note: not all aspects of a NIST SP 800-53 control requirement may have been included in NIST SP 800-171 requirement, so not all of the Supplemental Guidance may apply].
  - Typically, most requirements entail determining what the company policy should be (e.g., what should be the interval between required password changes) and then configuring the IT system to implement the policy.
  - Note that when the term “control” or “manage” is used, it does not necessarily imply a technical implementation – often a process or policy (with an ability to check periodically to insure the policy/process is being followed) is sufficient.
  - The complexity of the company IT system may determine whether additional software or tools are required. Small systems can manually accomplish many requirements, such as configuration management or patch management, while more complex systems may require automated software tools to perform the same task.
- Based on the above, determine which of the requirements can be readily accomplished by in-house IT personnel and which require additional research in order to be accomplished by company personnel or may require outside assistance.

- Develop a plan of action and milestones to implement the requirements.

In addition, NIST Handbook 162, Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements, available at https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf, provides guidance on implementing NIST SP 800-171 in response to the DFARS clause 202.204-7012. The Handbook provides a step-by-step guide to assessing a small manufacturer's information systems against the security requirements in NIST SP 800-171.

Q61: Will DoD provide additional guidance or training to smaller companies that may initially find these requirements overwhelming?

A61: To assist small businesses, the Department is engaging with the Procurement Technical Assistance Program (PTAP) to provide additional clarifying information addressing implementation of the cybersecurity regulations. Administered by the Defense Logistics Agency, the PTAP provides matching funds through cooperative agreements with state and local governments and non-profit organizations for the establishment of Procurement Technical Assistance Centers (PTACs). These centers, many of which are affiliated with Small Business Development Centers and other small business programs, form a nationwide network of counselors who are experienced in government contracting. The Department has provided the PTACs with information for small businesses who seek their assistance on the implementation of its cybersecurity regulations.

The Department is also working to assist the defense industrial base in executing its responsibility for ensuring that its supply chain, including small and mid-sized businesses, meets the requirements of the cybersecurity regulations. The Department routinely provides information and assistance to our defense industrial base partners at industry association meetings, joint government and industry meetings, small business training events, and quarterly meetings of the Defense Industrial Base Cybersecurity (DIB CS) Program.

The Department has captured concerns identified through our communications with industry by documenting and posting answers to these frequently asked questions (FAQs). Specific areas of interest to small businesses include guidance on how a small business with limited information technology or cybersecurity expertise might approach meeting the cybersecurity requirements.

The Defense Contract Management Agency's (DCMA's) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) is working to provide training to the Office of Small Business Development Centers, which assist small companies doing business with the federal government. Training is being provided to the Center's staff in the form of boot camps and webinars to prepare them to support small to medium sized companies with company preparations for NIST SP 800- 171 DoD Assessments.

Q62: What if the contractor thinks a required security control is not applicable, or that an alternative control or protective measure will achieve equivalent protection?

A62: The rule allows for the contractor to identify situations in which a required control might not be necessary or for an alternative to a required control. In such cases, the contractor should provide a written explanation in their proposal describing the reasons why a control is not required or adequate security is provided by an alternative control and protective measure. The contracting officer will refer the proposed variance to the DoD CIO for resolution. The DoD Chief Information Officer (CIO) is responsible for ensuring consistent adjudication of proposed non-applicable or alternative security measures.

When covered defense information is used in performance of a subcontract, the requirement is for the subcontractor to request the contracting officer to seek CIO adjudication on variances from NIST SP 800-171 requirements.

Q63: What is the process used by the DoD CIO to adjudicate alternative/non-applicable controls?

A63: DFARS provision 252.204-7008 and DFARS clause 252.204-7012 provide a process for the contractor to identify situations in which a security requirement from NIST SP 800-171 might not be necessary, or the contractor proposes an alternative to a security requirement from NIST SP 800-171. In such cases, the contractor must provide a written explanation describing the reasons why a security requirement is not applicable, or how alternative, but equally effective, security measures can compensate for the inability to satisfy a particular requirement. There is no prescribed format. The contracting officer will refer the proposed variance to the DoD CIO for adjudication. The DoD CIO is responsible for ensuring consistent adjudication of proposed non-applicable or alternative security measures. If the DoD CIO needs additional information, a request is made to the contracting officer. The resultant DoD CIO adjudication is provided to the contracting officer, who in turn advises the contractor of the decision. The timeframe for response by the DoD CIO is typically within five business days.

DFARS clause 252.204-7012 (b)(2)(ii)(B) clarifies that, should the status of the contractor's covered information system change after contract award, the contractor may submit a request to vary from the security requirements in NIST SP 800-171 after contract award.

Q64: What are the criteria used by the DoD CIO in adjudicating alternative/non-applicable controls?

A64: The basis for judging acceptability of an alternative is whether it is equally effective; the acceptability of "not applicable" is if the basis/condition for the requirement is absent.

Q65: Are there circumstances when DoD CIO adjudication of 'Alternative' or 'Not Applicable' solutions is not required?

A65: Yes, when the contractor's policy, process, etc., does not allow the circumstances addressed in the NIST SP 800-171, the contractor need only document the details surrounding the situation in the system security plan per NIST SP 800-171 (Chapter 3) and DFARS clause 252.204-7012 (b)(3). For example:

- Remote access must be monitored and controlled per requirement 3.1.12, but if the organization does not allow (and positively prevents by technical or procedural means) remote access, there is no need to request a 'not applicable' approval – indeed, the policy, procedure or technology that are used to prohibit remote access are considered an implementation of the requirement.
- Similarly, requirement 3.1.18 requires controlling the connection of mobile devices. If an organization does not allow such connections and ensures such connections are not provisioned, the organization is actually meeting the requirement, and adjudication of an alternative is not required.
- If the functionality addressed by the requirement is not permitted (e.g., 3.1.14, Route remote access via managed access control points), and the organization has a policy and procedure in place (and documented in the system security plan required by 3.12.4) to enforce the prohibition, then no approval of 'non-applicability' is required as the requirement is considered to have been implemented.

In addition, in situations where specialized systems, such as medical devices, CNC or other shop floor equipment, cannot by their nature meet the NIST SP 800-171 requirements, there is no need to request approval for an alternative or not applicable solution. These situations should be addressed in the contractor's system security plan.

Q66: Are contractors required to submit previously approved DOD CIO assessments of "not applicable" requirements or "alternative security measures" for any deficiency not being remediated? For example: Once a contracting officer accepts a request from a contractor for

a NIST SP 800-171 requirement to be deemed "not applicable" or an "alternative security measure," is the contractor required to submit that documentation for every current contract with DFARS clause 252.204-7012?

A66: Once DoD CIO assessments approving "not applicable" requirements or "alternative security measures" are included in the Contractor's system security plan, the contractor does not need to submit that documentation for every current contract with DFARS clause 252.204-7012 unless specifically requested to do so by the Contracting Officer. When completing the Basic (Contractor Self-Assessment) *NIST SP 800-171 DoD Assessment* Results Format, the contractor shall annotate any security requirements for which an assessment of "not applicable" or "alternative security measures" was previously approved by DoD CIO as 'met,' with no deduction.

Q67: Why does the DoD CIO require notification of the security requirements not implemented at the time of award? What is required for the notification requirement if the contract in question ends prior to the 31 December 2017 compliance date? Will the DoD allow for a single corporate-wide notification, such that the notification requirement could be accomplished at annual or semi-annual intervals, and not on every single transaction within 30 days? [Note: Not required for contracts awarded after October 1, 2017]

A67: The 30-day notification requirement contained in DFARS clause 252.204-7012 requires the contractor to provide DoD CIO with a list of the security requirements that the contractor is not implementing at the time of award. These lists will enable the DoD to monitor implementation progress across the Defense Industrial Base, identify trends, and identify issues with the industry implementation of specific requirements that may require clarification or adjustment. The list need only identify the security requirement(s) (e.g., NIST SP 800-171 security requirement 3.1.1) that is/are not implemented. No additional information is required. If the contract in question ends prior to October 1, 2017, the contractor must still provide the DoD CIO, within 30 days of contract award, with a list of the security requirements that are not implemented at the time of award. Nothing precludes the contractor from providing a corporate-wide update to the status of requirements not implemented on a periodic basis, assuming it meets the requirements of the clause.

Notification of NIST SP 800-171 requirements not implemented is NOT required for contracts awarded on October 1, 2017 or thereafter. As of January 1, 2018, all NIST SP 800-171 requirements are presumed to have been implemented OR identified as not implemented in your system security plan with a plan of action describing how and when they will be implemented per NIST SP 800-171 requirements 3.12.4 and 3.12.2, respectively.

Q68: Is post-award notification of the security requirements not implemented at the time of award also required within 30 days of award of subcontracts?

A68: Contractors are required to flow down DFARS clause 252.204-7012 to subcontractors without alteration when performance will involve operationally critical support or covered defense information. As such, the requirement is for the subcontractor to provide the DoD CIO, within 30 days of award to the subcontractor, with a list of the security requirements that the subcontractor has not implemented at the time of subcontract award.

Q69: Can contractors and subcontractors negotiate the provisions for providing notifications to higher tiered contractors when submitting the required statements of NIST non-compliance, non-applicability, and/or equally effective and alternate controls to the contracting officer for adjudication by the DOD CIO?

A69: Contractors are required to flow down DFARS clause 252.204-7012 to subcontractors without alteration (except to identify the parties) when performance will involve operationally critical support or covered defense information.

The clause also states that contractors must require their subcontractors to notify them (the prime Contractor (or next higher-tier subcontractor)) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer.

As such, with regard to the requirement at 252.204-7012(b)(2)(ii)(B) for the Contractor to "submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO", the subcontractor must notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171.

Q70: How does NIST SP 800-171 relate to the NIST Cybersecurity Framework?

A70: As noted in NIST SP 800-171 Revision 1, page vii (and page 29): "Organizations that have implemented or plan to implement the NIST Framework for Improving Critical Infrastructure Cybersecurity can find in Appendix D of this publication, a direct mapping of the Controlled Unclassified Information (CUI) security requirements to the security controls in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, and ISO/IEC 27001. Once identified, those controls can be located in the specific categories and subcategories associated with Cybersecurity Framework core functions: Identify, Protect, Detect, Respond, and Recover. The security control mapping information can be useful to organizations that wish to demonstrate compliance to the security requirements in the context of their established information security programs, when such programs have been built around the NIST or ISO/IEC security controls. See http://www.nist.gov/cyberframework." In addition, the "Defense Industrial Base (DIB)

Guide to Implementing the Cybersecurity Framework", published on October 4, 2019, is available at https://dibnet.dod.mil/.

Q71: NIST SP 800-171 is focused on confidentiality of information. In a manufacturing environment, there may also be the need for availability and integrity controls. How will operational environments influence the selection and/or implementation of additional security controls? Will the DoD develop implementation guides or case scenarios to demonstrate implementation of security controls in a manufacturing environment?

A71: The stated purpose of the security requirements in NIST SP 800-171 is to protect the confidentiality of controlled unclassified information (CUI) for protection of CUI in nonfederal systems. However, as noted in the question, the manufacturing environment may require controls for integrity of the data and the availability of the system which may be significantly different than that provided to protect the confidentiality via implementation of the security requirements in NIST SP 800-171. NIST SP 800-171 was structured such that the contractor's operations would dictate the selection of the integrity and availability controls appropriate for their internal system - i.e., the contractor decides what is required for integrity and availability based on the company's business needs.

Because of the variation in equipment and environments represented by the manufacturing sector, it is not practical for the DoD to develop implementation guides or case scenarios to demonstrate implementation of security controls in a manufacturing environment. Industry associations representing the defense industrial base may develop such implementation guides and/or case scenarios.

- **Specific NIST SP 800-171 Security Requirements**

Q72: Security Requirements 3.1.13, 3.1.17, 3.1.19, 3.13.8, and 3.13.11 – Do all of the 171 security requirements for cryptography have to be FIPS validated, and if so, what does that mean? If the algorithm is FIPS approved, is that sufficient?

A72: Yes, all the NIST SP 800-171 requirements for cryptography used to protect the confidentiality of CUI (or in this case covered defense information) must use FIPS-validated cryptography, which means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or-2 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient – the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non-FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at

http://csrc.nist.gov/groups/STM/cmvp/ and
http://csrc.nist.gov/groups/STM/cmvp/validation.html.

When NIST SP 800-171 requires cryptography, it is to protect the confidentiality of CUI (or in this case covered defense information). Accordingly, FIPS-validated cryptography is required to protect CUI, typically when transmitted or stored outside the protected environment of the covered contractor information system (including wireless/remote access) if not separately protected (e.g., by a protected distribution system). FIPS validated cryptography is required whenever the encryption is required to protect covered defense information in accordance with NIST SP 800-171 or by another contract provision. Encryption used for other purposes, such as within applications or devices within the protected environment of the covered contractor information system, would not need to be FIPS-validated. Note that any separate contract requirement (not currently in NIST SP 800-171) to encrypt data at rest (e.g., PII) within the information system would require use of FIPS validated cryptography.

Q73: Security Requirement 3.1.7 and 3.5.3 - If regular users' computer accounts are "administrator accounts" or have 'limited administrative rights" only on their computers, are they considered a "privileged account" requiring audit for privileged functions (3.1.7) or requiring multifactor authentication (3.5.3) at the "local access level"?

A73: No. NIST SP 800-171 defines a "privileged user" as "a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform." Since, in this case, the 'ordinary users' are authorized to perform the function, they are not considered privileged users.

Q74: Security Requirement 3.1.9 – 3.1.9 requires "privacy and security notices consistent with applicable CUI rules." Which CUI rules are being referenced?

A74: This requirement references the National Archives and Records Administration's (NARA) Federal rule (32 CFR 2002) implementing its CUI program. It would apply if a specific type of CUI (i.e., information that requires safeguarding or dissemination controls pursuant to law, regulation or Government-wide policy) requires such notices (e.g., before accessing or entering the data). This is not common.

Q75: Security Requirement 3.1.20 – 3.1.20 requires that an organization "verify and control/limit connections to and use of external systems." What is meant by 'external systems' and how are they controlled/limited?

A75: The discussion paragraph in NIST SP 800-171r2 (Feb 2020) at 3.1.20 provides a comprehensive explanation. Typically, these are systems over which the organization has no direct supervision or authority and include personally owned systems, components, or

devices, and privately-owned computing and communications devices resident in commercial or public facilities. This can range from personally owned computers used to work from home, external systems used to store data, external service providers (e.g., cloud service providers) as well as business-to-business connections, which may also permit external partners access to the organization's system.

Organizations establish terms and conditions for the use of such systems with the owners, imposing restrictions on their use if terms and conditions cannot be established. Control is established through the terms and conditions/limits for use, implemented by service level agreements with external parties and the organization's security practices and procedures, including, for example, boundary protections established per Security Requirement 3.13.1.

The System Security Plan, per Security Requirement 3.12.4, should describe how these limits/controls on external connections are implemented and verified, referencing supporting policies, procedures and agreements as appropriate.

Q76: Security Requirement 3.1.21 – 3.1.21 requires limiting the use of organizational portable storage devices on external information systems. Is this expected to be done using technical means or by policy? If there are technical options, can you provide any examples?

A76: This is generally implemented by policy, though some devices can be configured to work only when connected to a system to which they can authenticate (this is, however, not a requirement).

Q77: Security Requirement 3.1.21 – Can you provide a definition of "portable device", as that is not defined in NIST guidance?

A77: A 'portable storage device' (the term used by NIST) is an information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory). References: NIST SP 800-171, Appendix B, Glossary; NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Appendix B, Glossary.

Q78: Security Requirement 3.2.1, 3.2.2, and 3.2.3 – The requirement to ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems (3.2.1), the requirement to ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities (3.2.2), and the requirement to provide

security awareness training on recognizing and reporting potential indicators of insider threat (3.2.3) address the training required to be compliant with NIST SP 800-171. Where can we find training materials to address these requirements?

A78: Specific topics/course content is up to the nonfederal organization. However, there are substantial training materials available from federal sources that you can use. These often contain reference to specific federal (or DoD) procedures that may not apply to your particular situation, so make note of those if used for your workforce. There are two 'cyber security awareness' courses (the DoD 'cybersecurity challenge' course is the more complex) and one 'insider threat awareness course' that would apply to 3.2.1 and 3.2.3:

https://iatraining.disa.mil/eta/disa_cac2018/launchPage.htm

https://securityawareness.usalearning.gov/cybersecurity/index.htm

https://securityawareness.usalearning.gov/itawareness/index.htm

These materials plus more are available in the links shown below. The DISA IASE online catalog offers courses that are useful in meeting 3.2.2 security specific training requirements. Some of the IASE training materials will require a DoD PKI certificate to access, but generally these will not be applicable to security requirements 3.2.1 - 3.2.3.

Links to training resources:

https://iase.disa.mil/eta/Pages/index.aspx - DoD cybersecurity training. Some courses require a DoD approved PKI certificate, but most do not.

https://iase.disa.mil/eta/Pages/online-catalog.aspx - Provides a full catalog of training, to include security specific/role-based training (e.g., privileged user training).

https://securityawareness.usalearning.gov/ - Provides general security awareness training, such as cyber security awareness and 'insider threat awareness' training required by 3.2.3.

https://securityawareness.usalearning.gov/itawareness/index.htm - Link to the insider threat awareness training.

https://www.us-cert.gov/ncas/tips - Link to the DHS US CERT site. Tips/articles are useful in general user training and training for specific security roles.

https://fedvte.usalearning.gov/ - Link to federal 'virtual training environment' open to government contractors.

Q79: Security Requirement 3.4.9 and 3.13.13 – The requirement to control and monitor user-installed software (3.4.9) and the requirement to control and monitor the use of mobile code (3.13.13) seem outside the scope of protecting CUI. Shouldn't the requirement be to control CUI processing to authorized software?

A79: These requirements are necessary to protect the overall system processing CUI. They are not about software used to actually process CUI.

Q80: Security Requirement 3.5.3 – Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. What is meant by "multifactor authentication?"

A80: Multifactor authentication (MFA) to an information system uses two or more methods of authentication involving something you know (e.g., password); something you have (e.g., a One-Time Password (OTP) generating device like a fob, smart-card, or a mobile app on a smart-phone); and something you are (e.g., a biometric like a fingerprint or iris). The traditional authentication method uses a single factor, typically a password, while multifactor authentication requires that a second factor also be used such as PIN sent via a text message (using something you have – the cell phone) or something you are (fingerprint).

Local Access means access to an organizational system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

Network Access means access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

For a NON-PRIVILEGED user, if it's a standalone computer (e.g., a laptop computer), with no network access, the access can be via single factor authentication (SFA) - MFA is not required. However, if used to connect to a LAN, the network access has to be MFA. Typically, organizational desktops are used for network access and so the user has to use MFA to access their network account. For a PRIVILEGED user, even local access (e.g., to the standalone) requires MFA.

MFA is not required to access a mobile device (e.g., smart phones) even if they contain covered defense information, as there is a separate requirement (3.1.19) to encrypt CUI on mobile devices and mobile computing platforms, and typically mobile devices do not support MFA in order to access the device. However, if the mobile device is used to access a Covered Contractor Information System, then the system has to provide the capability for MFA for access by the device, and which would be entered via the device (e.g., use of a OTP device and a password).

Q81: Security Requirement 3.5.3 – Can one of the factors in multifactor authentication be where you are (e.g., within a controlled access facility)?

A81: No. Multifactor requires at least two of the following three factors: what you know (e.g., secret password), what you are (e.g., fingerprint), and what you have (e.g., PKI certificate on smartcard, OTP device). Each of these factors is unique to the individual being authenticated. Where you are, even in a controlled access facility is not one of these factors and, generally, would be a condition that applied to many and not unique to the individual being authenticated.

Q82: Security Requirement 3.5.3 – Native 2-factor authentication support for network access on all platforms is problematic; how is the multifactor requirement met?

A82: The multifactor authentication system is a requirement for local or network access to the information system, which is different from authentication to a specific information system component (e.g., a router) or an application (e.g., database). While many system components and applications now support (and expect) multifactor authentication, it is not a requirement to implement two-factor authentication on specific devices.

Q83: Security Requirement 3.5.3 – Do I need to use "multifactor authentication" for a smartphone or tablet?

A83: Multifactor authentication is not required for access to mobile devices such as smartphones or tablets – which are not considered to be network devices or information systems. Multifactor authentication to the device itself (e.g., to open the device) is not required as (1) no current devices appear to support more than a single factor; (2) there is a separate security requirement (3.1.19) to encrypt any CUI on the mobile device; and (3) multifactor authentication is not required to decrypt the CUI. If the device is used as a mechanism to access the organization's information system (e.g., via a web interface), then the information system itself must require the multifactor authentication, which would be entered by means of the mobile device. The DoD does not consider e-mail or text messages "pushed" from an organization's information system as "accessing" the information system, and requiring multifactor authentication.

Q84: Security Requirement 3.5.3 – What if I have covered defense information on my smartphone or tablet (e.g., in company e-mail) – do I need to use multifactor authentication in that case?

A84: No, that is covered under a separate security requirement, 3.1.19 - Encrypt CUI on mobile devices. As noted above, the multifactor authentication requirement applies to an information system, and a mobile device in not considered an "information system." But, if there will be covered defense information on a mobile device, it must be encrypted. This

can be done by encrypting all the data on the device (as is typically done on a laptop, and is available with recent iOS devices and some Android/Windows devices) or via a container (like the Good app, which is available for iOS (iPhone, iPad), Android, Windows; Blackberry's Secure Work Space for iOS and Android; etc.) to separate the covered defense information from the other information on the phone (or company information from personal information if employing a bring your own device (BYOD) approach). Care should be taken to ensure the encryption module is FIPS-validated for either the whole device or container. Information that is independently and appropriately encrypted (e.g., an e-mail encrypted with a PKI certificate) is self-protecting and need not be double-encrypted.

Q85: Security Requirement 3.5.3 – If a systems administrator has already been authenticated as a normal user using multifactor authentication, does using his administrative password to install software on the system violate the multifactor requirement?

A85: A privileged user (e.g., systems administrator) should always be in the "privileged" role to administer – e.g., he should use multifactor authentication in his privileged role (not as a normal user) to logon to the system to perform administrative functions.

Q86: Security Requirement 3.5.4 – The requirement to employ replay resistant authentication mechanisms for network access to privileged and non-privileged accounts. What defines replay resistant?

A86: Per NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, upon which NIST SP 800-171 is based (and references if additional information is required), "authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators." Reference: NIST SP 800-53, IA-2(8, 9), Identification and Authentication | Network Access to Privileged Accounts - Replay Resistant, Identification and Authentication Network Access to Non-Privileged Accounts - Replay.

Q87: Security Requirement 3.5.5 and 3.12.1 – Are there minimum acceptable values for "periodic" or "conditional" in requirements such as 3.5.5 "Prevent reuse of identifiers for a defined period" and 3.12.1, "Periodically assess the security controls in organizational systems…"?

A87: No – the values are left to the DoD contractor to determine.

Q88: Security Requirement 3.5.10 – Store and transmit only encrypted representations of passwords (in Revision 1, "encrypted representations of passwords" is changed to

"cryptographically-protected password)." Is a HASH considered an "encrypted representation" of a password or a cryptographically-protected password?

A88: Yes, the Supplemental Guidance in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, for the related security control IA-5(1) notes that "Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords." Best practice would add a unique "salt" to the password before hashing. This description applies to the use of "encrypted representations of passwords" in NIST SP 800-171 as well.

Q89: Security Requirement 3.7.5 – Can the requirement for multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete be met using other authentication and access control combinations such as remote IP address restrictions, session monitoring, and "One-Time-Pads"?

A89: The multifactor authentication for non-local maintenance is intended for recurring non-local maintenance by organizational personnel rather than episodic non-local maintenance by outside vendors where issuance of such credentials for one-time activities is not efficient and may not be advisable. Nevertheless, presuming the individual performing the repair is known and trusted, it is possible to provide for "one-time" multifactor authentication through the use of a password and a separately provided token (e.g., PIN via text message to a cell phone).

Q90: Security Requirement 3.8.2 – Can digital rights management protections or discretionary access control lists meet the intent of the requirement to "limit access to CUI on information system media to authorized users?"

A90: This requirement is meant to be applied by using physical controls to access physical media, but other mechanisms for logical access, such as those mentioned, are acceptable.

Q91: Security Requirement 3.8.4 – Mark media with necessary CUI markings and distribution limitations. Is this for all media, to include cell phones, for example, or just for removable media?

A91: This applies to information system media, which includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. It would not include cell phones.

Q92: Security Requirement 3.8.4 – Mark media with necessary CUI markings and distribution limitations. Can DoD provide further guidance on DoD's covered defense information

marking requirements? In the NIST SP 800-171 Revision 1 document, this control contains a footnote that indicates, "The implementation of this requirement is per marking guidance in 32, Part 2002, and the CUI Registry." In light of this, is DoD's position that contractors must mark all CUI processed through covered contractor information systems, or only covered defense information processed through covered contractor information systems? Also, is DoD's position that contractors must use the National Archives and Records Administration ("NARA") CUI marking handbook?

A92: The requirements of the clause only apply to covered defense information, i.e., information provided or developed by the contractor for DoD which is Controlled Technical Information or other information requiring protection by law, regulation or government-wide policy. It does not apply to information provided by or developed for non-DoD organizations. Guidance on marking media, along with other materials, should be addressed separately in the contract and is derived from DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI).

Q93: Security Requirement 3.10.1 – Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. This requirement has a feel of handling classified data and treating the data as need to know within the organization. Is this the case? Does covered defense information need to be handled as need to know? Can covered defense information-authorized and non-covered defense information-authorized personnel use the same set of cubicles?

A93: No, this is not the case. The purpose is simply to protect the information system/equipment by limiting physical access to the information system equipment to authorized organizational personnel (e.g., employees).

Q94: Security Requirement 3.10.6 – Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites). Is this expected to be done using technical means or by policy? If there are technical options, can you provide any examples?

A94: This simply means that if you have alternate work sites that will be used to store, process or transmit covered defense information, that the same requirements apply (i.e., there is no difference in requirements between the primary and alternate work sites), although different methods may be used to meet the requirements at the alternate site.

Q95: Security Requirement 3.11.1 – Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. Is there a minimum requirement for risk assessment

methodology (including risk calculation methodology) and reporting format and a defined minimum period?

A95: No, there is no defined requirement, methodology or period for the assessments, nor is a report required. All of these are dependent on the organization, its mission, changes to its systems and environment – this is a periodic assessment of how you operate to insure you understand your risk, which can change over time. Any changes resulting from the assessment would be reflected in implementing plans of action and in the system security plan per 3.12.2 and 3.12.4.

Q96: Security Requirements 3.12.1 and 3.12.3 – Periodically assess the security controls in organizational systems to determine if the controls are effective in their application; Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. Is there a defined period for assessment; what content is required in a DFARS clause 252.204-7012 compliant 'security controls assessment' report?

A96: There is no defined period for security control assessments, nor is there a report required. The organization should define for itself when controls are assessed, which may be based on a time period determined by its needs and/or events, such as a change to the system or its environment. (See also FAQ 20)

Q97: Security Requirements 3.12.2 and 3.12.4 - System security plans are being interpreted differently by various federal departments and agencies. Can you clarify the role of the system security plan and plans of action in contract formation and contract administration? Can full compliance with SP 800-171 be achieved after December 31, 2017, with a company specific system security plan and plans of action?

A97: DFARS clause 252.204-7012 requires the contractor to implement NIST SP 800-171 not later than December 31, 2017. Revision 1 of the NIST SP 800-171 states that when requested by the requiring activity and submitted by contractor, the system security plan and any associated plans of action demonstrate implementation or planned implementation of the security requirements. Additionally, Revision 1 notes that "Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether or not it is advisable to pursue an agreement or contract with the nonfederal organization."

Accordingly, requiring activities may utilize the system security plan and associated plans of action in a variety of ways in the contract formation/administration process in order to obtain the level of security that they require. These include, but are not limited to, the following:

- Require that proposals identify any NIST SP 800-171 security requirements not implemented at the time of award and include associated plans of action for implementation. Implementation of NIST SP 800-171, as documented in the system security plan or otherwise, would be considered as part of the source selection process. Proposal instructions and corresponding evaluation specifics of how implementation of NIST SP 800-171 will be used by the DoD to determine whether or not it is acceptable or unacceptable to process, store, or transmit covered defense information on a system hosted by the offeror must be detailed in sections L and M of the solicitation as well as the Source Selection Plan. This scenario is outside of the scope of DFARS clause 252.204-7012.
- Identify in the solicitation that all security requirements in NIST SP 800-171 must be implemented at the time of award. Planned or partial implementations would generally not be allowed, with the exception of any enduring exceptions to the requirements to accommodate special circumstances (e.g., medical devices), or any individual, isolated or temporary deficiencies. This scenario is outside of the scope of DFARS clause 252.204-7012.
- The contractor will self-attest to be compliant with DFARS clause 252.204-7012, to include implementation of NIST SP 800-171 (which allows for planned implementation of some requirements if documented in the system security plan and associated plans of action), by signing the contract at the time of award. No additional conditions beyond DFARS clause 252.204-7012 are imposed.

Unless the solicitation and/or contract specifically requires submission of system security plan or an extract thereof, there is NO requirement to submit this information to the government.

Q98: Security Requirement 3.12.4 – Is there a prescribed format/level of specificity for a system security plan?

A98: No. Footnote 26 to NIST SP 800-171 Security Requirement 3.12.4 states that, "There is no prescribed format or specified level of detail for system security plans. However, organizations must ensure that the required information in 3.12.4 is appropriately conveyed in those plans." Additionally, Chapter 3 of NIST SP 800-171, Revision 1 states that, "Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format."

Q99: What are the minimum requirements for a system security plan to be 'compliant'?

A99: NIST SP 800-171 security requirement 3.12.4 states that system security plans must describe system boundaries, system environments of operation, how security requirements are

implemented, and the relationships with or connections to other systems. There is no prescribed format or specified level of detail for system security plans, but organizations must ensure that the required information is conveyed. NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information, identifies the following areas to assess the effectiveness of a system security plan:

a) A system security plan is developed
b) The system boundary is described and documented
c) The system environment of operation is described and documented
d) The security requirements identified and approved by the designated authority as non-applicable are identified
e) The method of security requirement implementation is described and documented
f) The systems is described and documented in the system security plan
g) The frequency to update the system security plan is defined
h) The system security plan is updated with the defined frequency

Note that the description of the system environment of operation (c) should include a description and/or listing of the IT system hardware and software, to include versions and types of software and operating systems. It should also include a listing and description of any cloud services being utilized for the processing or storage of DoD CUI.

NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, provides further guidance on developing security plans, and a template for system security plans is available for free at the NIST website. The system security plan should not be a 'copy and paste' of the NIST SP 800-171 requirements, but should explain how your company implements each of the NIST SP 800-171 requirements. For Medium NIST SP 800-171 DoD Assessments, the majority of the information for the scoring is gleaned from the details of the system security plan. Poorly constructed system security plans will have a negative impact on the results of these assessments.

Q100: Security requirement 3.13.6 – The requirement to "deny network communications traffic by default and allow network communications traffic by exception" (i.e., deny all, permit by exception) is unrealistic if it must be implemented on all systems that host or transit CUI information. Can this requirement be met if there is a mechanism to implement "deny all, permit by exception" rule within the path between the external network and the CUI information?

A100: Yes, but if there are internal elements/segments of the information system that do not have the protections in place to process/store CUI, then they would also fall under this provision.

Q101: Security Requirement 3.13.8 – When implementing the requirement to "Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards," is encryption required for a Multiprotocol Label Switching (MPLS) private network (thus an extension of a local network) but it is multi-tenant protected by VLANs?

A101: Encryption, though preferred, is not required if using common-carrier provided MPLS, as the MPLS separation provides sufficient protection without encryption.

Q102: Security Requirement 3.13.8 – Can Transport Layer Security (TLS) protocol be used to protect CUI during transmission over the Internet?

A102: Yes, TLS can be used. The current version of TLS (TLS 1.2) is preferred. If earlier versions must be used to interact with certain organizations, the servers shall not support Secure Sockets Layer (SSL) version 3.0 or earlier. The cryptographic module used by the server and client must be a FIPS 140-validated cryptographic module. All cryptographic algorithms that are included in the configured cipher suites must be within the scope of the validation, as well as the random number generator. For further information see NIST SP 800-52, Rev 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, April 2014.

Q103: Regarding security requirement 3.13.8– How is CUI to be protected when transmitted over Common Carrier telecommunications lines/Plain Old Telephone Service (POTS)?

A103: Common Carrier telecommunications circuits or Plain Old Telephone Service (POTS) would not normally be considered part of the information system processing CUI. Data traversing Common Carrier systems should be separately encrypted per 3.13.8. Contracts with Common Carriers to provide telecommunications services may include DFARS clause 252.204-7012, but should not be interpreted to imply the Common Carrier telecommunications systems themselves have to meet the DFARS requirements. Data transmission of CUI transmitted over standard telephone dial-up service (POTS) similarly should be separately encrypted as no protection is expected to be provided by the telephone system. Voice communication of CUI over the telephone is not addressed by NIST SP 800-171 or by DFARS clause 252.204-7012.

Q104: Security Requirement 3.13.14 – The description for the security requirement in Section 3 (3.13.14) "control and monitor the use of Voice over Internet Protocol (VoIP) technologies"

is different from the corresponding Appendix D entry, "Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies and monitor/control use of VoIP." Which is correct? How should this be handled for 3rd party VoIP service offerings where control is outsourced. (i.e., Vonage)? Does this security requirement only apply when the VoIP service is shared on a network that transits CUI?

A104: Section 3 is correct, and this has been corrected in the current posted version of NIST SP 800-171. Even if outsourced, the internal IT system should have protections in place to control (albeit limited) and monitor VoIP within the system. If physically or cryptographically isolated from an information system processing CUI, this control would not apply (but it would be prudent to apply the requirement).

Q105: Security Requirement 3.13.16 – Protect the Confidentiality of CUI at rest. Can CUI be stored at rest in any non-mobile device or data center, unencrypted, as long as it is protected by other approved logical or physical methods?

A105: Yes, the mapped NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, control (SC-8), notes that this requirement is to protect the confidentiality of CUI information at rest when it is located on storage devices as specific components of information systems and that "organizations may employ different mechanisms to achieve confidentiality protection, including the use of cryptographic mechanisms and file share scanning." Thus, encryption is an option, not a requirement.

Cloud Computing

- ### General

Q106: Can you clarify when DFARS clause 252.239-7010 applies to cloud computing services and when DFARS clause 252.204-7012 applies?

A106: DFARS clause 252.239-7010, Cloud Computing Services, applies for the acquisition of commercial products and commercial services, for information technology services. Information Technology is defined at FAR Part 2 as:

Information technology means any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

(1) For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires-

(i) Its use; or

(ii) To a significant extent, its use in the performance of a service or the furnishing of a product.

(2) The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

(3) The term "information technology" does not include any equipment that-

(i) Is acquired by a contractor incidental to a contract; or

(ii) Contains imbedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment, such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology.

DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, applies when a contractor intends to use an external cloud service provider to store, process, or transmit covered defense information in the performance of a contract and the requirements in DFARS 252.204-7010 are not already applicable. DFARS clause 252.204-7012 requires the cloud service provider to meet security requirements equivalent to those established for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.

Q107: Why is DFARS clause 252.239-7010 addressed in DFARS clause 252.204-7012?

A107: DFARS clause 252.204-7012(b)(1)(i) states that to provide adequate security for covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, “(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.” This is included to ensure the proper clause is used when DoD is contracting for an IT service or system that will be operated on behalf of the

Government. Because DFARS clause 252.204-7012 is required in all contracts (except for COTS), and DFARS clause 252.239-7010 is required in all contracts for IT services, contracts for IT services will include both clauses – DFARS clause 252.204-7012 requiring the use of NIST SP 800-171, and DFARS clause 252.239-7010 requiring the use of the DoD Cloud Computing Security Requirements Guide. To avoid a potential conflict regarding which requirements apply when, DFARS clause 252.204-7012 states that DFARS clause 252.239-7010 applies to contracts for IT services involving cloud computing services.

Q108: Will the DoD require physical access to cloud computing data centers in order to conduct forensic analysis under DFARS clause 252.204-7012(f) or 252.239-7010(g) and (i)?

A108: DFARS clause 252.239-7010 is included in contracts for information technology services and applies when a contractor is using cloud computing to provide information technology services to DoD in the performance of the contract. It does not apply to cloud computing data centers operated as an extension of a contractor's internal IT system. DFARS clause 252.204-7012 is included in all DoD contracts (except those solely for COTS items) and a reference to DFARS clause 252.239-7010 is provided at paragraph (b)(1)(i) to notify contractors of the security requirements that must be followed when DoD is contracting for cloud services (i.e., DoD Cloud SRG vice NIST SP 800-171) .

Paragraph (f) of DFARS clause 252.204-7012 implements a statutory requirement from section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013 and states that, "Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis." This statement applies to cloud computing data centers operated as an extension of a contractor's internal IT system. DoD normally will not require physical access if the cloud services provider captures, preserves, and protects images and the state of all systems known to be affected by a cyber incident as separately required by paragraph (e) of DFARS clause 252.204-7012. However, in highly unusual circumstances, there may still be some cases when DoD may require physical access to equipment. Because the need for access is driven by the circumstances surrounding the cyber incident, DoD is not able to waive this requirement.

- **Cloud solution being used to store data on DoD's behalf (DFARS provision 252.239-7009 and DFARS clause 252.204-7010, Cloud Computing Services, apply)**

Q109: How is the requirement for a provisional authorization waived by the DoD CIO, allowing a contracting officer to award a contract to acquire cloud services from a cloud service provider (CSP) that has not been granted a provisional authorization by the Defense Information System Agency (DISA)?

A109: All DoD CIO and other DoD cybersecurity issuances apply to DoD information systems, assets, or networks owned or operated by or on the behalf of DoD Components, whether interconnected, isolated, or stand-alone. This includes owned and leased communications and systems and services, software (including applications), data, security services, and other associated services. Exceptions to DoD Cloud Computing policies can be requested through DISA's Systems/Network Approval Process (SNAP) system at https://snap.dod.mil using the latest request for exception to policy template posted on the website. If you need assistance, please contact the DoD CIO exception processing team at osd.pentagon.dod-cio.mbx.dcio-cs-ae@mail.mil.

- **Contractor using cloud solution to store covered defense information (DFARS provision 252.204-7008 and DFARS clause 252.204-7012 apply)**

Q110: How can a contractor ensure that the cloud service provider can comply with requirements 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 (i.e., paragraphs (c) through (g) of DFARS clause 252.204-7012?

A110: While the (c)-(g) requirements are contractual requirements you must meet (e.g., reporting of cyber incidents), if you are using a cloud service, you'll need to insure the cloud service provides you the necessary information/support to meet those requirements (e.g., report a cyber incident affecting your DoD CUI to you in a timely manner, so you can report the cyber incident to DoD within 72 hours of discovery). Each provider approaches these differently, with some providers explicitly stating they support the requirements (or not) while others may note that the customer can supplement their services to meet the requirements.

Q111: Do cloud service providers (CSP) have to follow DFARS clause 252.204-7012 (c)-(g) if there is a breach inside a hosted customer Virtual Machine (VM)?

A111: Per DFARS clause 252.204-7012 (b)(2)(ii)(D), the contractor "shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this 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.

The contractor does not normally 'flow down' the DFARS clause to the CSP but must ensure, when using a CSP as part of his covered contractor information system, that he can continue to meet the DFARS clause requirements, including the requirements in DFARS clause 252.204-7012 (c)-(g). Accordingly, what the CSP is required to do depends on the cloud services provided (IaaS, PaaS, or SaaS), and on what the CSP is actually responsible for and is capable of observing (e.g., if the CSP observes a cyber incident, it should report the incident to the contractor). Generally, the CSP will provide the contractor the required information, when that is possible, and the contractor will provide that information to DoD.

Q112: What security requirements apply when using a cloud solution to process/store covered defense information?

A112: When the cloud requirements prescribed at DFARS 252.239-7010 do not already apply to the use of cloud services in performance of the contract for the transmittal of covered defense information, then the cloud security requirements at DFARS 252.204-7012 (b)(2)(ii)(D) apply. DFARS clause 252.204-7012 (b)(2)(ii)(D) requires the Contractor to ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline and that the cloud service provider complies with requirements 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.

Q113: Can you clarify what is meant by 'equivalent' to FedRAMP, so that companies will know what cloud services they can use and the relationship to NIST 800-171 in order to assess what the cloud service provides and what the company may need to furnish to meet the required cybersecurity controls.

A113: The DFARS clause 252.204-7012 (b)(2)(ii)(D) states that "the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/)." This does not preclude nor require the contractor use a CSP service authorized/approved by the FedRAMP program – since in some instances such FedRAMP approved services may only allow use by government agencies – but simply requires that the contractor ensure that the cloud services contracted to process and store covered defense information meet the same set of requirements.

Q114: Why 'equivalent to FedRAMP moderate'? Why is NIST SP 800-171 not sufficient in the case of a cloud service provider?

A114: FedRAMP "Moderate" requirements (rather than NIST SP 800-171) are specified for the following reasons:

- NIST SP 800-171 was not developed to accommodate the additional security requirements necessary to protect information when using an external Cloud Service Provider. The FedRAMP Moderate baseline was developed to include these additional requirements.
- Many of the modifications made to the NIST "Moderate" baseline confidentiality controls in developing NIST SP 800-171 - such as removing automation requirements - to accommodate the broad range in the size/complexity of nonfederal organizations internal IT systems, as well as the elimination of availability requirements, do not apply to external CSPs.
- The FedRAMP Moderate baseline cloud service is well established and offered by multiple CSPs

Q115: The DFARS states "the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline". If the cloud provider is not FedRAMP certified, how can a contractor ensure that the cloud provider meets security requirements equivalent to FedRAMP Moderate?

A115: The contractor can ensure that the cloud provider meets security requirements equivalent to FedRAMP "Moderate" in the same way the contractor would normally ensure any services or product being contracted for will meet his requirements. For example, a cloud service provider (CSP) may choose to provide evidence that it meets the security requirements equivalent to FedRAMP "Moderate" by providing a body of evidence (BOE) that attests to and describes how the CSP meets the FedRAMP Moderate baseline security requirements (https://www.fedramp.gov/assets/resources/documents/FedRAMP_Moderate_Security_Controls.xlsx). Examples of items that could be included in such a BOE are a System Security Plan (SSP) (https://www.fedramp.gov/assets/resources/templates/FedRAMP-SSP-Moderate-Baseline-Template.docx) that describes the system environment, system responsibilities, and the current status of the Moderate baseline controls required for the system, and a Customer Implementation Summary/Customer Responsibility Matrix (CIS/CRM) (https://www.fedramp.gov/updated-customer-implementation-summary-cis-and-customer-responsibility-matrix-crm-templates/) that summarizes how each control is met and which party is responsible for maintaining that control. Although non-FedRAMP providers may use different formats, the FedRAMP templates available at the provided links are representative of the kind of information/evidence that could be provided.

Additionally, per DFARS clause 252.204-7012(b)(3), companies need to apply other information security measures, if required. When using external cloud services, FedRAMP moderate generally addresses the security requirements of information categorized as CUI Basic and most CUI Specified. However, some types of CUI/covered defense information have additional requirements that have to be addressed. For example, some data such as export control/ITAR information may require the data be processed and stored in the US and be administered by US persons. This may dictate what type of FedRAMP moderate cloud service can be used, as most FedRAMP 'commercial' services do not insure data is stored/processed in the US and by US persons. For this reason, a vendor may say a 'Government' version or service is required - it depends on whether the CUI/covered defense information has specific processing/storage requirements.

Note that some cloud providers will only ensure **complete** US sovereignty (e.g., all services are US-based and administered, even if the user is operating outside the US) with their FedRAMP 'High' offerings. Since FedRAMP High is not required to protect CUI in accordance with DFARS 252.204-7012 (such offerings are a by-product of DoD Cloud Security Requirements Guide Security Level 4 services made available to non-DoD users), companies should determine whether their particular situation requires use of a providers FedRAMP 'High' services to meet any US data sovereignty requirements.

Q116: If a company is using an external Cloud Service Provider (CSP) to provide processing and storage of covered defense information, (i.e., DFARS clause 252.204-7012 requires that the CSP meet requirements equivalent of to the FedRAMP Moderate baseline), depending on the service provided (i.e., IaaS, PaaS or SaaS), some of these FedRAMP requirements are allocated to the client. In this case, does the client (the company contracting with the CSP) have to meet FedRAMP "Moderate" requirements that are NOT mapped to the NIST SP 800-171 requirements per Appendix D of NIST SP 800-171?

A116: No. The CSP has to meet all of the requirements equivalent to the FedRAMP Moderate Baseline, but if some of these (as is typical) are allocated to the client, the client does not need to meet FedRAMP requirements that are unrelated to the NIST SP 800-171 requirements. If the particular FedRAMP requirement (a control from NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations) is not mapped to a NIST SP 800-171 requirement in Appendix D of NIST SP 800-171, it need not be applied by the client. When the FedRAMP control is mapped to a NIST SP 800-171 requirement, only the actual NIST SP 800-171 requirement need be implemented, which may be somewhat different than its mapped NIST 800-53 control. Note that in some circumstance controls that must be implemented by the CSP may require a reciprocal implementation by the client for the CSP's control to be effective.

Q117: Is the contractor required to flow down DFARS clause 252.704-7012 when utilizing a cloud service provider? Is the contractor responsible for ensuring that cloud service providers comply with DFARS clause 252.204-7012?

A117: When a contractor uses an external cloud service provider to store, process or transmit any covered defense information for the contract, DFARS clause 252.204-7012 (b)(2)(ii)(D) applies. If the cloud service provider is considered a subcontractor for this contract effort and will be handling covered defense information, then DFARS clause 252.204-7012 would flow down, but this would not be typical. While the flow-down provision in 252.204-7012 does not apply if the CSP is not considered a subcontractor, the prime contractor is responsible to ensure that the CSP meets the requirements at 252.204-7012 (b)(2)(ii)(D).

Assessing Contractor Implementation of NIST SP 800-171 Security Requirements

Q118: What is the *NIST SP 800-171 DoD Assessment Methodology*?

A118: The *NIST SP 800-171 DoD Assessment Methodology*, available at https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.1%20%203.13.2020.pdf, is a standard methodology that enables DoD to strategically assess a contractor's implementation of NIST SP 800-171, and to provide DoD Components with visibility to the summary level scores of strategic assessments completed by DoD, thus providing an alternative to the contract-by-contract approach. The *NIST SP 800-171 DoD Assessment* consists of three levels of assessments - Basic, Medium, and High. These three levels of assessments (described in detail in the *NIST SP 800-171 DoD Assessment Methodology*) reflect the depth of the assessment, and the associated level of confidence in the assessment results. Conduct of the *NIST SP 800-171 DoD Assessment* will result in a score reflecting the net effect of security requirements not yet implemented. 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. This scoring methodology is designed to provide an objective assessment of a contractor's NIST SP 800-171 implementation status.

DCMA's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) is partnering with DIB companies to strategically assess contractor implementation of NIST SP 800-171 using the *NIST SP 800-171 DoD Assessment Methodology*. The Department is pursuing implementation of the *NIST SP 800-171 DoD Assessment Methodology* via DFARS Case 2019-D041, Strategic Assessment and Cybersecurity Certification Requirements.

Q119: What is meant by a 'strategic' or 'corporate' assessment?

A119: When a contractor conducts a Basic *NIST SP 800-171 DoD Assessment*, or DoD conducts a Medium or High *NIST SP 800-171 DOD Assessment*, the results reflect the contractor's NIST SP 800-171 implementation status for the covered contractor information system that was assessed. The results are relevant to every contract supported by the assessed covered contractor information system – thus referred to as a 'strategic' assessment. Summary level scores for Basic assessments completed by the Contractor, and for Medium and High assessments conducted by DoD, will be posted in the Supplier Performance Risk System (SPRS) to provide DoD Components with visibility to the results of strategic assessments (see FAQs 128-132). DoD Components may then rely on assessment results posted in SPRS, to include information identifying the specific industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed in the assessment, in lieu of including requirements to assess implementation of NIST SP 800-171 on a contract-by-contract basis.

Q120: Will NIST SP 800-171 DoD Assessments be completed for a given facility at a specific location, as identified by the Commercial and Government Entity (CAGE) code, or by contractor?

A120: The scope of each *NIST SP 800-171 DoD Assessment* will be defined by the system security plan(s), and associated system(s)/network(s), that is(are) assessed. Each system security plan assessed will be mapped to the specific industry CAGE code(s) associated with the information system(s) addressed by the plan.

Q121: How is the *NIST SP 800-171 DoD Assessment Methodology* different than *NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information*? Why is the DoD methodology needed?

A121: The NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information" uses 320 objectives to assess contractor implementation of the security requirements in NIST Special Publication 800-171 and sets a repeatable standard for assessment procedures. The procedures are guided and informed by the individual system security plans for the covered contractor information systems processing, storing, or transmitting CUI, and focus on the implementation and effectiveness of the safeguards intended to meet the security requirements defined in NIST Special Publication 800-171.

The *NIST SP 800-171 DoD Assessment Methodology* was developed to complement and build off of the NIST SP 800-171A by providing a scoring methodology and scoring template based on which, if any, NIST SP 800-171 security requirements are not yet implemented. The Methodology recognizes that the risk associated with an unimplemented security

requirement is not equally weighted across the 110 requirements contained in the NIST SP 800-171.

Q122: What is the difference between a Basic, Medium, and High *NIST SP 800-171 DoD Assessment*?

A122: The Basic Assessment is the Contractor's self- assessment of NIST SP 800-171 implementation status, based on a review of the system security plan(s) associated with covered contractor information system(s), and conducted in accordance with NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information" and Section 5 and Annex A of this document. The Basic Assessment results in a confidence level of 'Low' in the resulting score because it is a self-generated score.

The Medium Assessment is conducted by DoD personnel who have been trained in accordance with DoD policy and procedures to conduct the assessment. It is anticipated that Medium Assessments will be conducted primarily by Program Management Office cybersecurity personnel, as part of a separately scheduled visit (e.g., for a Critical Design Review). The assessment, also conducted in accordance with NIST SP 800-171A, will consist of a review of the system security plan description of how each requirement is met to identify any descriptions which may not properly address the security requirements. The Medium Assessment results in a confidence level of 'Medium' in the resulting score.

The High Assessment, conducted by DoD personnel who have been trained in accordance with DoD policy and procedures to conduct the assessment, requires a thorough on-site or virtual verification/examination/demonstration or test of the Contractor's system security plan and implementation of the NIST SP 800-171 security requirements. Also conducted in accordance with NIST SP 800-171A, the High Assessment, will determine if implementation meets the requirements by reviewing appropriate evidence and/or demonstration (e.g., recent scanning results, system inventories, configuration baselines, demonstration of multifactor authentication).

An on-site High NIST SP 800-171 DoD Assessment is the preferred methodology for a full evaluation of the risk to DoD CUI because of the ability to verify and validate the effectiveness of the safeguards that implement security requirements defined in NIST Special Publication 800-171. While a High Assessment maybe be conducted virtually in lieu of onsite, a virtual assessment will not cover all the NIST SP 800-171 requirements, resulting in a less than full understanding of overall risk.

A virtual High Assessment utilizes the same methodology as the on-site assessment, with added data protections and processes enacted to protect the DIB data that is shared with the assessment teams. All data is transmitted through DoD Safe, is only reviewed locally on each assessor's computer (screen sharing is conducted utilizing DoD collaboration mediums

that are approved for processing CUI) and contractor data is destroyed post assessment using NSA guidance for data destruction. With concurrence from the DIB companies being assessed, the assessment verifies and examines all documents utilizing the NIST SP 800-171A methodology minus the demonstration or testing of some requirements. In some cases, a follow-up on-site assessment of the items not assessed may be required or requested.

The first step in a High Assessment is for the contractor to conduct a Basic Assessment and submit results to the Department using the procedures in Annex B, Basic (Contractor Self-Assessment) *NIST SP 800-171 DoD Assessment* Results Format, of the *NIST SP 800-171 DoD Assessment Methodology*. The High Assessment consists of a review of the Basic Assessment, a thorough document review and discussion with the contractor regarding the results to obtain additional information or clarification as needed, combined with government validation that the security requirements have been implemented as described in the system security plan. Network access by the assessor(s) is not required. This assessment is conducted using NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information." The assessment will determine if the implementation meets the requirements by reviewing appropriate evidence and/or demonstration (e.g., recent scanning results, system inventories, configuration baselines, demonstration of multifactor authentication). The High Assessment results in a confidence level of 'High' in the resulting score.

Q123: How is a *NIST SP 800-171 DoD Assessment* scored?

A123: The scoring methodology is designed to provide an objective assessment of a contractor's NIST SP 800-171 implementation status. With the exception of requirements for which the scoring of partial implementation is built-in (e.g., multi-factor authentication, security requirement 3.5.3) the methodology is not designed to credit partial implementation. Conduct of the NIST SP 800-171 DoD Assessment will result in a score reflecting the net effect of security requirements not yet implemented. 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. Scores will be posted in the Supplier Performance Risk System (SPRS) (see FAQ 128-132).

Q124: Why are some requirements worth more points than others in the *NIST SP 800-171 DoD Assessment* Scoring Template?

A124: While NIST SP 800-171 does not prioritize security requirements, 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.

Weighted requirements include all of the fundamental NIST SP 800-171 'Basic Security Requirements' - high-level requirements which, if not implemented, render ineffective the more numerous 'Derived Security Requirements'; and a subset of the 'Derived Security Requirements'- requirements that supplement the Basic Security Requirements - which, if not implemented, would allow for exploitation of the network and its information.

For security requirements that, if not implemented, could lead to significant exploitation of the network, or exfiltration of DoD CUI, 5 points are subtracted from the score of 110. For example, failure to limit system access to authorized users (Basic Security Requirement 3.1.1) renders all the other Access Control requirements ineffective, allowing easy exploitation of the network; failure to control the use of removable media on system components (Derived Security Requirement 3.8.7) could result in massive exfiltration of CUI and introduction of malware.

For Basic and Derived Security Requirements that, if not implemented, have a specific and confined effect on the security of the network and its data, 3 points are subtracted from the score of 110. For example, failure to limit access to CUI on system media to authorized users (Security Requirement 3.8.2) or failure to encrypt CUI stored on a mobile device (Security Requirement 3.1.19), put the CUI stored on the system media or mobile device at risk, but not the CUI stored on the network itself.

All remaining Derived Security Requirements, if not implemented, have a limited or indirect effect on the security of the network and its data. For these, 1 point is subtracted from the score of 110. For example, failing to prevent reuse of identifiers for a defined period (Security Requirement 3.5.5) could allow a user access to CUI to which they were not approved.

Q125: How long are the results from a NIST SP 800-171 DoD Assessment valid? How often does the assessment need to be done? Annually?

A125: It is anticipated that contractor information systems/networks supporting contracts containing DFARS clause 252.204-7012 will be assessed once every three years, unless other factors, such as program criticality/risk or a security-relevant change, drive the need for a different assessment frequency.

Q126: Will there be a pass/fail scoring threshold utilized with the *NIST SP 800-171 DoD Assessment* in the future?

A126: Not as it applies to the implementation of DFARS clause 252.204-7012, this is essentially a risk decision. A decision to accept the risk should remain with the Requiring Activity.

Q127: How will Software as a Service solutions be scored with the *NIST SP 800-171 DoD Assessment*? For example: Integration with Office 365, which holds a FedRAMP moderate certificate, may create an issue as the vendor will not share specific details with clients.

A127: For cloud-based solutions (e.g., SaaS, Office 365), if authorized at FedRAMP moderate or equivalent, the solutions are assumed to meet NIST SP 800-171 requirements. However, typically certain configuration settings remain the responsibility of the subscriber/client, and when they are related to specific NIST SP 800-171 requirements, they are subject to assessment and scoring.

Q128: What is the Supplier Performance Risk System (SPRS)? Who can access SPRS?

A128: SPRS is the authoritative source to retrieve supplier and product performance information for the DoD acquisition community to assess and monitor unclassified performance, and to assess corporate business practices related to DoD contracts and the supplier's management of risk. SPRS is defined by DoD Instruction (DoDI) 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information, October 15, 2019 available at https:\\www.esd.whs.mil/DD/. Assessment results posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI), available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500079p.PDF?ver=2019-10-15-115609-957. Authorized representatives of the Contractor for which the assessment was conducted may access SPRS to view their own results in accordance with the SPRS Software User's Guide for Awardees/ Contractors available at https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf.

Q129: Who can post *NIST SP 800-171 DoD Assessment* results to the Supplier Performance Risk System (SPRS)? What will be posted?

A129: A contractor may submit, via encrypted email, summary level scores of Basic Assessments conducted in accordance with Section 5 and Annex B of *NIST SP 800-171 DoD Assessment Methodology*, available at https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.1%20%203.13.2020.pdf, to webptsmh@navy.mil for posting to SPRS.

DoD will post the following Medium and/or High *NIST SP 800-171 DoD Assessment* results to SPRS for each system security plan assessed:

i) The standard assessed (e.g., NIST SP 800-171 Rev 1).

ii) Organization conducting the assessment, e.g., DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC) or Commercial and Government Entity (CAGE) Code).

iii) Each system security plan assessed, mapped to the specific industry CAGE code(s) associated with the information system(s) addressed by the system security plan. All corporate CAGE codes must be mapped to all appropriate system security plan(s) if the contractor has more than one system security plan and CAGE code. Additionally, a brief description of the system security plan architecture may be required if more than one plan exists.

iv) Date and level of the assessment, i.e., basic, medium, or high.

v) Summary level score (e.g., 105 out of 110), but not the individual value assigned for each requirement.

vi) Date a score of 110 is expected to be achieved (i.e., all requirements implemented) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.

Q130: How are Plans of Action (security requirement 3.12.2) addressed in the NIST SP 800-171 Assessment results posted in Supplier Performance Risk System (SPRS)?

A130: When DoD posts *NIST SP 800-171 DoD Assessment* results to SPRS for each information system/system security plan assessed, these results will include the date a score of 110 is expected to be achieved (i.e., all requirements implemented) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171 (see FAQ 129).

Q131: How will DoD use the results posted in to the Supplier Performance Risk System (SPRS)?

A131: DoD Components should consider assessment results posted in SPRS prior to making a risk-based decision to assess implementation of NIST SP 800-171 on a contract-by-contract basis. Acquisition/procurement officials and contractors have been directed/are expected to access SPRS to determine if a strategic assessment has been conducted.

Q132: How do I know if the NIST SP 800-171 DoD Assessment results posted in Supplier Performance Risk System (SPRS) SPRS are for a contractor's Basic self-assessment, or for a Medium or High assessment conducted by DoD?

A132: Summary results posted in SPRS include: the date and level of the assessment, e.g., basic (contractor self-assessment), medium, or high; and the organization conducting the assessment, e.g., DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC) or Commercial and Government Entity (CAGE) Code) (see FAQ 129).

Q133: Is the NIST SP 800-171 DoD Assessment required for contracts with DFARS clause 252.204-7012 and a requirement to protect DOD CUI?

A133: No. This methodology is used for assessment purposes only and does not, and is not intended to, add any substantive requirements to either NIST SP 800-171 or DFARS clause 252.204-7012.

Q134: If a prime contractor chooses to assess a subcontractor using this methodology, on what basis should it decide whether to assess at a 'Basic,' 'Medium' or 'High' level?

A134: Generally similar to the approach DoD is using: Basic to provide 'the most basic' initial information on compliance – scales easily to large number of subcontractors; High requires significant effort and is difficult to scale and so would be used in circumstances where compliance is critical (e.g., involves extremely sensitive information/critical programs and technologies); Medium would be considered as means of providing more fidelity than a Basic Assessment. Note that Medium and High NIST SP 800-171 DoD Assessments can only be conducted by specific DoD personnel who have been trained in accordance with DoD policy and procedures to conduct the assessment.

Q135: What is the maximum acceptable duration for which a "temporary deficiency" may be active?

A135: There is no standard duration. It is what is reasonable, which would take into consideration the availability of the solution, the cost and time to implement, the overall risk and whether any mitigations are applied in the interim. Generally, deficiencies should be resolved as soon as is reasonably possible.

Q136: Is a scheduled change management action sufficient for inclusion in a POAM? For example: Implementation issue identified, the solution is known and the remediation date set.

A136: Yes.