17 November 2015

Network Penetration Reporting and Contracting for Cloud Services

(DFARS Case 2013-D018)

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

http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

Class Deviation 2016-O0001(OCT 2015)

http://www.acq.osd.mil/dpap/dars/class_deviations.html

The following questions are addressed in this document:

Q: Why was the Network Penetration Reporting and Contracting for Cloud Services rule published as an interim rule?

Q: What are the major difference between DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services and DFARS Case 2011-D039, Safeguarding Unclassified Controlled Technical Information?

Q: When is DFARS Clause 252.204-7012 required in contracts?

Q: What is included in the definition of Covered Defense Information (CDI)? Does this include Controlled Unclassified Information (CUI)?

Q: What is "Operationally Critical Support"?

Q: How will CDI be identified?

Q: What is Unclassified Controlled Technical Information (CTI)?

Q: Who is responsible for identifying/marking unclassified CTI?

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

- A comparison of NIST SP 800-53 and NIST SP 800-171

Q: Why did the security protections required by DFARS clause 252.204-7012 change from a table of selected NIST SP 800-53 security controls to NIST Special Publication (SP) 800-171? This is a significant change from the previous version of this clause.

Q: What drove the need for Class Deviation 2016-O0001 (October 2015)?

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

Q: How does the Contractor report a cyber incident?

Q: 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?

Q: What happens when the contractor submits an ICF to the DIBNet portal?

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

Q: What if a subcontractor discovers a reportable cyber incident?

Q: What role does the DoD Cyber Crime Center (DC3) play in the DFARS reporting program?

Q: 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"?

Q: What if the contractor is required to submit media, how do they do that?

Q: What is the Enhanced Cybersecurity Services (ECS) program and how can it help me?

QUESTIONS SPECIFIC TO THE NIST SP 800-171 SECURITY REQUIREMENTS:

Q: 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.

Q: Do all the 171 requirements for cryptography have to be FIPS validated, and if so, what does that mean? If the algorithm is FIPS approved, is that sufficient?

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

Q: Security requirement 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?

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

Q: Security requirement 3.4.9 - Control and monitor user-installed software: this requirement, and security requirement 3.13.13, Control and monitor the use of mobile code, seem outside the scope of protecting CUI. Shouldn't the requirement be to control CUI processing to authorized software?

Q: 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?"

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

Q: Native 2-factor authentication support for network access on all platforms is problematic; how is the multifactor requirement met?

Q: Do I need to use 'multifactor authentication' for a smartphone or tablet?

Q: What if I have CDI on my smartphone or tablet (e.g., in company e-mail) – do I need to use multifactor authentication in that case?

Q: 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?

Q: 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?

Q: Security requirement 3.5.10 – Store and transmit only encrypted representations of passwords. Is a HASH considered an 'encrypted representation' of a password?

Q: 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'?

Q: 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?"

Q: 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?

Q: 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?

Q: 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?

Q: 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?

Q: Regarding security requirement 3.13.14– how is CUI to be protected when transmitted over Plain Old Telephone Service (POTS)?

CLOUD COMPUTING

Q: What security requirements apply when using a cloud solution to process/store Covered Defense Information?

Q: Why was the Network Penetration Reporting and Contracting for Cloud Services rule published as an interim rule?

A: A determination was made under the authority of the Secretary of Defense that urgent and compelling reasons exist to promulgate the interim rule without prior opportunity for public comment. This action was necessary because of the urgent need to increase the cyber security requirements placed on DoD information in contractor systems, to mitigate the risk of compromise of covered defense information, to ensure uniform application of policies and procedures for the acquisition of cloud computing services across DoD, and to gain awareness of the full scope of cyber incidents being committed against defense contractors. The Network Penetration Reporting and Contracting for Cloud Services rule revises the DFARS to implement section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013 (Pub. L.112-239) and section 1632 of the NDAA for FY 2015. This rule also implements policies and procedures for use when contracting for cloud computing services.

Section 941 of the NDAA for FY 2013 requires cleared defense contractors to report penetrations of networks and information systems and allows DoD personnel access to equipment and information to assess the impact of reported penetrations. Section 1632 of the NDAA for FY 2015 requires that a contractor designated as operationally critical must report each time a cyber incident occurs on that contractor's network or information systems.

Q: What are the major differences between DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services and DFARS Case 2011-D039, Safeguarding Unclassified Controlled Technical Information?

A: DFARS Case 2011-D039, Safeguarding Unclassified Controlled Technical Information, was amended as follows:

- DFARS subpart 204.73 was modified to expand safeguarding and reporting policy to require protection of covered defense information (CDI)
- The clause at 252.204–7012 was renamed ''Safeguarding Covered Defense Information and Cyber Incident Reporting'' and the scope of the clause was expanded to cover the safeguarding of CDI and require contractors to report cyber incidents involving this information as well as any cyber incident that may affect the ability to provide operationally critical support.
- The table of security controls based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800–53 was replaced by NIST SP 800-171, entitled ''Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.''
- A new provision at 252.204–7008, Compliance with Safeguarding Covered Defense Information Controls, was added to ensure that offerors are aware of the requirements of

clause 252.204–7012 and allow for a process to explain; (i) how alternative, but equally effective, security measures can compensate for the inability to satisfy a particular requirement; or (ii) why a particular requirement is not applicable.
- A new clause at 252.204–7009, Limitations on the Use and Disclosure of Third-Party Contractor Reported Cyber Incident Information, was added to protect contractor information submitted to DoD in response to a cyber incident.
- DFARS subpart 239.76 was added to implement policy for the acquisition of cloud computing services.
- A new provision at 252.239–7009, Representation of Use of Cloud Computing, was added to allow the offeror to represent their intention to utilize cloud computing services in performance of the contract or not.
- A new clause at 252.239–7010, Cloud Computing Services, was added to provide standard contract language for the acquisition of cloud computing services.

Q: When is DFARS Clause 252.204-7012 required in contracts?

A: DFARS Clause 252.204-7012 is required in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items. 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 in accordance with the terms of the contract.

Q: When must the contractor implement DFARS Clause 252.204-7012?

A: The PCO shall indicate in the solicitation/contract when performance of the contract will involve, or is expected to involve, covered defense information (CDI) or operationally critical support, and all unclassified CDI documents provided to the contractor by the Government will be marked when appropriate.

Q: What is included in the definition of Covered Defense Information (CDI)? Does this include Controlled Unclassified Information (CUI)?

A: Covered Defense Information is unclassified information that:

- Is provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or
- Is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract;
  and
- Falls in any of the following categories:
  - Controlled technical information

- Critical information (operations security)
- Export control
- Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies (e.g., privacy, proprietary business information)

The last bullet covers information that currently must be protected by law, regulation and policy. This information will most likely continue to be required to be safeguarded under the emerging Federal CUI policy.

Q: What is "Operationally Critical Support"?

A: 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.

The 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); Cl l, 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, such as the F-22 and F-35.
d. The prime contractors and subcontractors for critical weapons systems in development and sustainment that are fielded to the AOR.
e. Contractor Logistics (maintenance and supply) Support. Examples include Unmannned Aerial Systems maintenance, (aviation) training command maintenance support, or performance based logistics/performance based arrangements.
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".

Q: How will CDI and operationally critical support be identified?

A: The contracting officer will be notified by the requiring activity 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, or when the contractor will provide operationally critical support.

The contracting officer shall ensure that notification of CDI or operationally critical support provided is included 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 markings when appropriate on CDI.

Q: What is Unclassified Controlled Technical Information (CTI)?

A: Controlled technical information is defined in the DFARS at 204.7301 as; 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 is to be marked with one of the distribution statements B through F, in accordance with DoDI 5230.24, Distribution Statements on Technical Documents. Classified controlled technical information would be subject to the requirements of the National Industrial Security Program (NISPOM), which has different requirements than DFARS clause 252.204-7012.

Q: Who is responsible for identifying/marking unclassified CTI?

A: The controlling DoD office (defined in DoDI 5230.24), in most cases the requiring activity, is responsible to:

- Determine whether the relevant technical information to be furnished by the Government and/or developed by the contractor contains unclassified CTI. The requiring activity must notify the procuring contracting officer (PCO) when a contractor will be required to develop and/or handle unclassified CTI.
- Review all unclassified CTI to be provided to the contractor to verify that all document distribution statements are valid and that all documents that should be marked are properly marked with the correct statement prior to their being provided to the contractor.
- If the contractor will develop unclassified CTI with Government rights in the performance of the contract, whether or not the unclassified CTI is to be delivered to the Government, the requiring activity should work with the PCO to:
    - Include a statement of work to require the contractor to develop the unclassified CTI technical data products. Include specific requirements for any other type of technical data products, such as test plans and reports.
    - Include in the DD Form 1423, Block 9, specific distribution statement requirements for individual technical data documents, other than specification and engineering drawing documents to be delivered as part of a technical data package.
    - Include a statement of work to require that the distribution statement(s) be applied on the various types of technical data products specified in the statement of work in accordance with the distribution statement marking instructions as developed by the controlling DoD office and attached to the contract.
    - Ensure that the requiring activity validates the contractor's execution of the Government's distribution statement marking instructions prior to delivery and acceptance of the technical data products.

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

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

- **A comparison of NIST SP 800-53 and NIST SP 800-171**

DFARS Rule 2013-D018 amends the security controls required to provide "adequate security" – replacing a table of controls based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, with security requirements found in NIST SP 800-171, Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations. 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, Jun 15**
• 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 Security Categorization of Federal Information and Information Systems • Allows organizations to tailor relevant security control baseline to align with their mission/business environment	• Provides standardized/uniform set of requirements for all CUI security needs • Allows nonfederal organizations to consistently implement safeguards for 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

Q: Why did the security protections required by DFARS clause 252.204-7012 change from a table of selected NIST SP 800-53 security controls to NIST Special Publication (SP) 800-171? This is a significant change from the previous version of this clause.

A: 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 initial version of the DFARS 252.204-7012 clause included only a selected subset of those controls. In contrast, the new NIST SP 800-171 security requirements were developed specifically to be applied to, and by, non-federal organizations. They are performance-based to avoid mandating specific solutions, and to make it easier to apply to existing systems in use by industry. The new NIST 800-171 also provides a standardized and uniform set of requirements for all CUI security needs, allowing nonfederal organizations to be in compliance 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).

Q: What drove the need for Class Deviation 2016-O0001 (October 2015)?

A: While implementation of the new NIST SP 800-171 generally only requires configuration or process changes from what was previously required, one requirement - the use of multi-factor authentication for local and network access to the contractor's information system - may require a significant effort to implement. For this reason, the Department issued an amendment to the interim rule which will allow contractors to request an extended period, of up to nine months after award, to implement the multi-factor authentication requirement. This amendment was issued as class deviation 2016-O0001 on October 8, 2015, available at http://www.acq.osd.mil/dpap/dars/class_deviations.html.

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

A: 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.

Q: How does the Contractor report a cyber incident?

A: The Contractor will access the DIBNet portal (http://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.

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

A: For information on obtaining a DoD-approved ECA certificate, please visit the ECA website (http://iase.disa.mil/pki/eca/certificate.html).

Q: 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?

A: When the contractor does not have all the information required by the clause within that time constraint, they should report what is available. If more information becomes available, the contractor should provide updates to DC3.

Q: What if a subcontractor discovers a reportable cyber incident?

A: DFARS Clause 252.204–7012 (m) (2) requires subcontractors to rapidly report cyber incidents directly to DoD at http:// dibnet.dod.mil and to the prime Contractor. This includes providing the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable.

Q: What happens when the contractor submits an ICF to the DIBNet portal?

A: Upon receipt of the contractor submitted ICF in the DIBNet portal, the DC3 will send an unclassified email containing the submitted ICF to the Contracting Officer identified on the ICF. DC3 is the designated collection point for cyber incident reporting required under DFARS Clause 252.204-7012.

Q: What role does the DoD Cyber Crime Center (DC3) play in the DFARS reporting program?

A: The DoD Cyber Crime Center (DC3) serves as the DoD operational focal point for receiving cyber threat and incident reporting from those Defense contractors who have a contractual requirement to report under DFARS.

Q: 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"?

A: This statement 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 access and use of CDI by contractors supporting DoD activities triggered by the reported cyber incident, 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 CDI "only for the purpose of furnishing advice or technical assistance directly to the Government in support of 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 252.204-7012 clause, but about support contractors' misuse of third party information they receive in supporting DoD cyber incident analysis and damage assessment processes.

Q: What if the contractor is required to submit media, how do they do that?

A: The contracting officer will send instructions for submitting media when a request to submit media is made.

QUESTIONS SPECIFIC TO THE NIST SP 800-171 SECURITY REQUIREMENTS:

Q: **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?

A: The DFARS requirement at 252.204-7012 (b)(1)(ii)(A) to, "implement information systems security protections on all covered contractor information systems including, at a minimum, the security requirements in NIST SP 800-171," is not intended to imply 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) and (d).

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 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; and

- 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."

DoD estimates that a contractor system that was compliant with the previous DFARS clause would be 90-95% compliant with the NIST 800-171 security requirements by implementing policy and procedure requirements which do not involve substantive IT changes. The contractor may then address any residual issues, e.g., security requirement implementations in progress, through 'plans of action' (as described in security requirement 3.12.2 noted above) in the contractor's equivalent of a system security plan.The 'system security plan' is addressed in NIST 800-171 as "expected to be routinely satisfied by non-federal organizations without specification" as part of an overall of a risk-based information security program (see footnote 16, page 6 and Table E-12, PL-2). The system security plan should be used to describe how the system security protections are implemented, any exceptions to the requirements to accommodate issues such as those listed in the question above, and plans of action as provided by security requirement 3.12.2, to correct deficiencies and reduce or eliminate vulnerabilities.

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

Q: Do all the 171 requirements for cryptography have to be FIPS validated, and if so, what does that mean? If the algorithm is FIPS approved, is that sufficient?

A: Yes, the requirement is to 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 is not sufficient – the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. More information is available at http://csrc.nist.gov/groups/STM/cmvp/ and http://csrc.nist.gov/groups/STM/cmvp/validation.html

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

A: This requirement anticipates approval of the National Archives and Records Administration (NARA) proposed 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.

Q: Security requirement 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?

A: 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).

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

A: 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 800-171, Appendix B, Glossary; NIST 800-53, Appendix B, Glossary

Q: Security requirement 3.4.9 - Control and monitor user-installed software: this requirement, and security requirement 3.13.13, Control and monitor the use of mobile code, seem outside the scope of protecting CUI. Shouldn't the requirement be to control CUI processing to authorized software?

A: This requirement, and the requirement for mobile code, are necessary to protect the overall system processing CUI. They are not about software used to actually process CUI.

Q: 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?"

A: Multifactor authentication 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 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)).

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

A: No – multifactor requires at least two of the following three factors: what you know, what you are, and what you have. Where you are is not one of these factors.

Q: Native 2-factor authentication support for network access on all platforms is problematic; how is the multifactor requirement met?

A: 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**.**

Q: Do I need to use 'multifactor authentication' for a smartphone or tablet?

A: 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. 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. 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.

Q: What if I have CDI on my smartphone or tablet (e.g., in company e-mail) – do I need to use multifactor authentication in that case?

A: 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 CDI 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 CDI from the other information on the phone (or company information from personal information if employing a 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.

Q: 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?

A: 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.

Q: 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?

A: Per NIST, "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.

Q: Security requirement 3.5.10 – Store and transmit only encrypted representations of passwords. Is a HASH considered an 'encrypted representation' of a password?

A: Yes. The Supplemental Guidance in NIST SP 800-53 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.

Q: 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'?

A: 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 txt message to a cell phone).

Q: 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?"

A: 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.

Q: 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?

A: 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.

Q: 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?

A: This simply means that if you have alternate work sites that will be used to store, process or transmit CDI, 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.

Q: 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?

A: 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.

Q: 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?

A: Section 3 is correct, and this has been corrected in the current posted version of NIST SP 800-171 (see Errata on page ix). 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).

Q: **Regarding security requirement 3.13.14– how is CUI to be protected when transmitted over Plain Old Telephone Service (POTS)?**

A: POTS would not normally be considered part of the information system processing CUI. Protection of CUI over the telephone is not addressed by NIST SP 800-171 or by this DFARS Clause 252.204-7012.

CLOUD COMPUTING

Q: What security requirements apply when using a cloud solution to process/store Covered Defense Information?

A: In accordance with the Federal Information Security Management Act (FISMA), when an information system is being operated on the DOD's behalf, it is considered a DoD system, and so needs to meet the same requirements as if it were operated by DoD. Accordingly, the DoD Cloud Computing Security Requirements Guide (SRG) applies when:

- A cloud solution is being used to process data on the DoD's behalf
- DoD is contracting with a Cloud Service Provider to host and process our data in a cloud
- A cloud solution is being used for processing that we (the DoD) would normally do ourselves but have decided to outsource

NIST SP 800-171 is designed to be used by nonfederal organizations to protect Controlled Unclassified Information (CUI). Accordingly, The NIST SP 800-171 applies when:

- A cloud solution is used by the contractor to do his own processing related to meeting a DoD contract requirement to develop/deliver a product, i.e., as part of the solution for his internal contractor system. (Example - contractor is developing the next generation tanker, and uses cloud for the engineering design.)