OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION,
TECHNOLOGY,
AND LOGISTICS

SEP 2 1 2017

MEMORANDUM FOR COMMANDER, UNITED STATES SPECIAL OPERATIONS COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES TRANSPORTATION COMMAND (ATTN: ACQUISITION EXECUTIVE)
DEPUTY ASSISTANT SECRETARY OF THE ARMY (PROCUREMENT)
DEPUTY ASSISTANT SECRETARY OF THE NAVY (ACQUISITION AND PROCUREMENT)
DEPUTY ASSISTANT SECRETARY OF THE AIR FORCE (CONTRACTING)
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

The Department amended the Defense Federal Acquisition Regulation Supplement (DFARS) in 2016 to provide for the safeguarding of controlled unclassified information when residing on or transiting through a contractor's internal information system or network. DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires contractors to implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" to safeguard covered defense information that is processed or stored on their internal information system or network. Contractors, who self-attest to meeting these requirements, have until December 31, 2017, to implement NIST SP 800-171.

The Director, Defense Pricing/Defense Procurement and Acquisition Policy, in collaboration with the DoD Chief Information Officer and the Deputy Assistant Secretary of Defense, Systems Engineering, has developed the enclosed guidance for acquisition personnel in anticipation of this December 31, 2017 implementation deadline. We are dedicated to ensuring that the requirements of this clause are successfully implemented, and look forward to working with all stakeholders throughout the Department and industry to achieve that objective. If you have any questions related to this issue, please contact Mary Thomas at mary.s.thomas.civ@mail.mil, or (703) 693-7895.

Shay D. Assad
Director, Defense Pricing/Defense Procurement and Acquisition Policy

Attachment
As stated.

September 19, 2017

Guidance for Selected Elements of DFARS Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting" — Implementing the Security Requirements of NIST SP 800-171

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires contractors to provide "adequate security" for covered defense information that is processed, stored, or transmitted on the contractor's internal information system or network. The Department must mark, or otherwise identify in the contract, any covered defense information that is provided to the contractor, and must ensure that the contract includes the requirement for the contractor to mark covered defense information developed in performance of the contract. To provide adequate security, the contractor must, at a minimum, implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," not later than December 31, 2017.

This guidance is provided for DoD acquisition personnel in anticipation of the December 31, 2017, deadline. It outlines, in general, the manner in which contractors are likely to approach implementing NIST SP 800-171; addresses how a contractor may use a system security plan to document implementation of the NIST SP 800-171 security requirements; and describes examples of how DoD organizations might choose to leverage the contractor's system security plan, and any associated plans of action, in the contract formation, administration, and source selection processes.

Contractor Implementation of NIST SP 800-171, Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations

NIST SP 800-171 was developed for use on contractor and other nonfederal information systems and networks to protect Controlled Unclassified Information (CUI). DFARS Clause 252.204-7012 requires that contractors implement NIST SP 800-171 to protect systems and networks that process, store, or transmit "covered defense information" (as defined in the clause). NIST SP 800-171 provides a single, Government-wide set of performance-based security requirements that significantly reduce unnecessary specificity (e.g., as compared to prescribing detailed security controls), which enables contractors to comply in most cases by using or adapting systems and practices already in place.

There is no single or prescribed manner in which a contractor may choose to implement the requirements of NIST SP 800-171, or to assess their own compliance with those requirements. For companies new to the requirements, a reasonable first step may be for company personnel with knowledge of their information systems security practices to read through the publication, examining each requirement to determine if it may require a change to company policy or processes, a configuration change for existing company information technology (IT), or if it requires an additional software or hardware solution. Most requirements

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

The complexity of the company IT system may determine whether additional software or tools are required. For smaller systems, the company may accomplish many requirements manually, such as configuration management or patch management, while larger and more complex systems may require automated software tools to perform the same task. Having reviewed all of the security requirements, a company may then determine which of the requirements, 1) can be accomplished by their own in-house IT personnel, 2) require additional research in order to be accomplished by company personnel, and 3) require outside assistance.

If unsure of what a requirement means, companies may seek additional guidance in the mapping table in Appendix D of NIST SP 800-171, which maps each of the NIST SP 800-171 requirements to relevant security controls that are specified in NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations." After identifying the corresponding NIST SP 800-53 control, the company may consult the "Supplemental Guidance" section of the description of that control in NIST SP 800-53 to find clarifying guidance and examples of how to implement that control, which the company may choose to utilize for its implementation of the more performance-based 800-171 requirements. When doing this, companies should be aware that not all aspects of a NIST SP 800-53 security control may have been included in NIST SP 800-171 security requirement, and as such, not all of the Supplemental Guidance may apply.

Ultimately, it is the contractor's responsibility to determine whether it is has implemented the NIST SP 800-171 (as well as any other security measures necessary to provide adequate security for covered defense information). Third party assessments or certifications of compliance are not required, authorized, or recognized by DoD, nor will DoD certify that a contractor is compliant with the NIST SP 800-171 security requirements.

Documenting a Contractor's Implementation or Planned Implementation of NIST 800-171

NIST SP 800-171 was revised (Revision 1) in December 2016 to enable nonfederal organizations to demonstrate implementation or planned implementation of the security requirements with a "system security plan" and associated "plans of action."

- Security requirement 3.12.4 (System Security Plan, added by NIST SP 800-171, Revision 1), 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.

- Security Requirement 3.12.2 (Plans of Action), requires the contractor to develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in their systems.

Note that DFARS Clause 252.204-7012 requires the contractor to implement the version of the NIST SP 800-171 that is in effect at the time of the solicitation, or such other version that is authorized by the contracting officer. Thus, if Revision 1 of NIST SP 800-171 was not in effect at the time of the solicitation, the contractor should work with the contracting officer to modify the contract to authorize the use of NIST SP 800-171, Revision 1, dated December 2016. DoD guidance is for contracting officers to work with contractors who request assistance in the consistent implementation of the latest version of DFARS Clause 252.204-7012 and NIST SP 800-171, Revision 1.

To document implementation of the NIST SP 800-171 security requirements by the December 31, 2017, implementation deadline, companies should have a system security plan in place, in addition to any associated plans of action to describe how and when any unimplemented security requirements will be met, how any planned mitigations will be implemented, and how and when they will correct deficiencies and reduce or eliminate vulnerabilities in the systems. Organizations can document the system security plan and plans of action as separate or combined documents in any chosen format.

There are a number of mechanisms by which the contractor can inform the Government of the contractor's implementation of the NIST SP 800-171 requirements. The solicitation provision DFARS 252.204-7008, "Compliance with Safeguarding Covered Defense Information Controls," provides that by submitting the offer the contractor is representing its compliance (and provides a procedure for the contractor to request the DoD Chief Information Officer (CIO) to authorize a variance from any of those requirements as being non-applicable, or because the contractor has a different but equally effective security measure). In addition, paragraph (c)(2)(ii)(A) of DFARS Clause 252.204-7012 requires the contractor that is performing a contract awarded prior to October 1, 2017, to notify the DoD CIO of any requirements of NIST SP 800-171 that are not implemented at the time of contract award.

In addition, the solicitation may require or allow elements of the system security plan, which demonstrates/documents implementation of NIST SP 800-171, to be included with the contractor's technical proposal, and may subsequently be incorporated (usually by reference) as part of the contract (e.g., via a Section H special contract requirement). Contractors have indicated in public forums that system security plans or plans of action will likely contain company sensitive information. Incorporating the plans by reference, and advising the companies to ensure their plans are marked with an appropriate restrictive notice or marking (e.g., to indicate that it contains "proprietary" or other sensitive information) should address those concerns.

DFARS Clause 252.204-7012 does not add any other unique or additional requirements for the Government to monitor contractor implementation of NIST SP 800-171 or to monitor compliance with any other requirement of that clause. As noted previously, third party

assessments or certifications of compliance are not required, authorized, or recognized by DoD, nor will DoD certify that a contractor is compliant with the NIST SP 800-171 security requirements. If the requiring activity/buying activity determines that oversight related to the security requirements is necessary, they may add requirements to the terms of the contract as addressed below.

Role of the System Security Plan and Plans of Action in Contract Formulation, Administration, and Source Selection

Chapter 3 of NIST SP 800-171, Revision 1, states that Federal agencies may consider the contractor's system security plan 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. DFARS Clause 252.204-7012 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 using a company's system security plan and associated plans of action to evaluate the overall risk introduced by the state of the contractor's internal information system/network. To facilitate this process, requiring activities should, when feasible, issue a draft request for proposal (RFP) to communicate their intent with regard to the safeguarding requirements associated with a given procurement, the level of risk the requiring activity is willing to accept, and to solicit industry questions and comments regarding those requirements and the state of the contractor's internal information system/network. DPAP is working in collaboration with DoD CIO to develop criteria for requiring activities to apply when describing safeguarding requirements for a given procurement and the level of risk they are willing to accept as industry transitions to full compliance of the NIST SP 800-171 security requirements.

The requiring activity must state in the solicitation whether and how 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 may utilize the system security plan and associated plans of action include, but are not limited to:

- Using proposal instructions and corresponding evaluation specifics (detailed in sections L and M of the solicitation as well as the Source Selection Plan) regarding how implementation of NIST SP 800-171 (and other applicable security measures) will be used by DoD to determine whether it is an acceptable or unacceptable risk to process, store, or transmit covered defense information on a system hosted by the offeror. The solicitation must notify the offeror whether and how its approach to protecting covered defense information and providing adequate security in accordance with DFARS 252.204-7012 will be evaluated in the solicitation.

- Establishing compliance with DFARS 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.

- Requiring that proposals i) identify any NIST SP 800-171 security requirements not implemented at the time of award and ii) include associated plans of action for implementation. If the implementation date is after the date of award then the contracting officer may choose to incorporate that plan by reference into the contract to ensure the contractor is held accountable to meet the NIST SP 800-171 requirements in accordance with its own plans. It is the responsibility of the program office to determine whether to accept the risk of storing sensitive government data on a contractor system that has not fully met the NIST SP 800-171 requirements.

- Identifying in the solicitation that all security requirements in NIST SP 800-171 must be implemented at the time of award.

The Department will work to encourage industry to adopt corporate/segment/facility system security plans in order to ensure more consistent implementations and to reduce costs. Additionally, the Department is developing a risk model for use by the Department and industry to facilitate the analysis of system security plans and plans of action, and to categorize the risk associated with not implementing specific security requirements in NIST SP 800-171 to enable transition to full compliance.

Additional Resources

The Department is 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 and responded to the most common questions and concerns identified through our communications with industry by documenting the issue 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.

To further facilitate communication with small businesses, the Department is leveraging the Procurement Technical Assistance Program (PTAP) to provide information addressing implementation of DFARS Clause 252.204-7012. 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 partnering with NIST Manufacturing Extension Partnership (MEP) to assist small and mid-sized U.S. manufacturers implement NIST SP 800-171. MEP is a nationwide system with centers located in every state. MEP centers are non-profit organization that partner with the Federal government to offer products and services that meet the specific needs of their local manufacturers.

Finally, the Department posts all related regulations, policy, frequently asked questions, and resources addressing DFARS Clause 252.204-7012, and NIST SP 800-171, at the Cybersecurity tab at http://dodprocurementtoolbox.com/.