DFARS COMPLIANCE FAQ

DOES THIS REALLY APPLY TO ME?

- **Are you a Department of Defense government Contractor?**
- **Does your company work with Covered Defense Information (CDI) or Confidential Unclassified Information (CUI)?**
- **Is DFARS clause 252.204.7008 in your contract requirements?**

If you answered "yes" to any of these questions then THIS COMPLIANCE REQUIREMENT APPLIES TO YOU. All prime and subcontractors doing business with the Department of Defense must implement the new security regulations or document an exception. Even if you don't think this requirement applies to you, you may still need to comply with portions of NIST SP 800-171.

IS THERE A DEADLINE? HOW MUCH TIME DO I HAVE?

Yes, you have ONLY 30 days to complete your DFARS CDI Assessment and report your findings to the DoD Chief Information Officer (CIO), upon contract award. *This assessment provides the government your current cybersecurity posture. You then have until December 31, 2017 to correct any gaps documented by your assessment.*

WHAT IS DFARS CDI (252.204-7008, 252.204-7009, 252.204-7012)?

Defense Federal Acquisition Regulation Supplement (DFARS) Safeguarding rules and clauses, for the basic safeguarding of contractor information systems that process, store, or transmit Federal contract information. DFARS imposes a set of "basic" security controls for contractor information systems upon which this information resides. These security controls must be implemented at both the contractor and subcontractor levels based on information security standards developed by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, titled "Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations." The most common DFARS safeguarding rule and clauses for which a defense contractor will be expected to demonstrate compliance are as follows:

- *DFARS 252.204.7008 – Compliance with Safeguarding Covered Defense Information Controls*
- *DFARS 252.204.7009 – Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information*
- *DFARS 252.204.7012 – Safeguarding Covered Defense Information and Cyber Incident Reporting*

I'M NOT SURE I HAVE CUI…WHAT IS IT?

CUI is any unclassified information that is provided to the contractor by or on behalf of DoD in connection with 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. CUI has a broad definition and can be technical, administrative, or operational in nature. CUI applies to any information identified in 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)

DOES THE GOVERNMENT INTEND TO MONITOR CONTRACTORS TO ENSURE IMPLEMENTATION OF THE REQUIRED SECURITY REQUIREMENTS?

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.

WHAT IF THE CONTRACTOR THINKS A REQUIRED SECURITY CONTROL IS NOT APPLICABLE, OR THAT AN ALTERNATIVE CONTROL OR PROTECTIVE MEASURE WILL ACHIEVE EQUIVALENT PROTECTION?

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.

Subcontractors must notify 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, in accordance with paragraph (b)(2)(ii)(B) of the DFARS 252.204-7012 clause.

HOWEVER, it is the belief of Subject Matter Experts that the effort involved in obtaining an approved alternative to a required control rarely will be successful.

HOW DOES THE CONTRACTOR REPORT A CYBER INCIDENT?

The contractor will access the DIBNet portal 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.

Subcontractors must provide the incident report number, automatically assigned by DoD, to the prime contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of the DFARS 252.204-7012 clause.

NOTE: It can take up to FOUR weeks to obtain your Incident Reporting Login credentials. It is highly recommended you begin the effort without delay.

HOW CAN THE CONTRACTOR OBTAIN DOD-APPROVED MEDIUM ASSURANCE EXTERNAL CERTIFICATE AUTHORITY (ECA) CERTIFICATE IN ORDER TO REPORT?

For information on obtaining a DoD-approved ECA certificate, please visit the ECA website: iase.disa.mil/pki/eca/Pages/index.aspx.

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?

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.

WHAT IF A SUBCONTRACTOR DISCOVERS A REPORTABLE CYBER INCIDENT?

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.

WHAT HAPPENS WHEN THE CONTRACTOR SUBMITS AN ICF TO THE DIBNET PORTAL?

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.

WHAT ROLE DOES THE DOD CYBER CRIME CENTER (DC3) PLAY IN THE DFARS REPORTING PROGRAM?

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.

WHAT IF THE CONTRACTOR IS REQUIRED TO SUBMIT MEDIA, HOW DO THEY DO THAT?

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

HOW WILL THE DOD ACCOUNT FOR THE FACT THAT COMPLIANCE WITH NIST SP 800-171 IS AN ITERATIVE AND ONGOING PROCESS?

Additional background behind this question:

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?

The DFARS requirement is not intended to imply there will not be situations where elements of the NIST SP800-171 requirements cannot be practically 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 addition, the dynamic nature of cybersecurity threats and vulnerabilities is recognized within the NIST SP800-171. The contractor should address situations such as those listed above in accordance with the NIST SP800-171 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.”

WHAT SECURITY REQUIREMENTS APPLY WHEN USING A CLOUD SOLUTION TO PROCESS/STORE COVERED DEFENSE INFORMATION?

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, cloud computing services shall be subject to the security requirements specified in DFARS 252.239-7010, Cloud Computing Services, and subsequently, 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 their data in a cloud*
- *A cloud solution is being used for processing that the DoD would normally do themselves but have decided to outsource*

If the contractor intends to use an external cloud service provider to do their own processing related to meeting a DoD contract requirement to develop/deliver a product, i.e., as part of the solution for their internal contractor system (Example - contractor is developing the next generation tanker, and uses cloud for the engineering design,) 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 and that the cloud service provider complies with requirements in paragraphs (c) through (g) of the DFARS 252.204-7012 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.

HOW LONG DOES IT TAKE TO COMPLETE A DFARS CDI ASSESSMENT?

Larger companies can take several months. Certain factors determine where a company fits within the small to large categories. Traditional aspects such as number of employees and their computing devices, number of sites that must be visited during the assessment, number of DoD contracts that must be reviewed for various unique requirements and definitions of systems, and the overall number of computing systems in place.

One particular impact is the number of unique "Information Systems" that must be assessed as defined here:

An information system is a collected group of information system components (workstations, servers, VoIP phones, routers, switches, firewalls) in a connected infrastructure, under a single management authority. A separate information system would be segregated by a firewall or even air gapped, or under a separate management authority. Companies may choose to segregate information systems for multiple reasons. In some cases, they may have non-US citizens who only have access to an information system that doesn’t contain export controlled information. The relevant DFARS clause states that any information system that stores or transmits CDI is subject to the NIST SP800-171 controls. If an organization has multiple information systems, and only one stores or transmits CDI, then it is the only one that requires an assessment.

I JUST HEARD SOMETHING ABOUT NARA MAKING THIS A REQUIREMENT FOR ALL FEDERAL CONTRACTORS. IS THIS TRUE?

Yes, it's true. The National Archives and Records Administration (NARA), which is the organization with the authority to define CUI, has announced that they are about a year out from establishing a universal FAR ruling that will eventually replace DFARS 252.204-7012, and expand the scope to all Federal agencies and contractors (such as NASA, DoE, etc.), rather than just the DoD as it was previously. NARA's stated goal is for this change to be in place by November of 2017, and it will still use NIST SP 800-171.

HOWEVER, if you are a DoD contractor with the DFARS 252.204 clause contained in your contract, you still must abide by this current requirement. You cannot wait until the new FAR clause is established, as your contract requires you to implement this requirement earlier than the non-DoD federal contractors, which will almost certainly reference the same CUI requirements in NIST SP 800-171.