Safeguarding Unclassified Controlled Technical Information (CTI)

Frequently Asked Questions (FAQs) regarding the implementation of

DFARS Subpart 204.73 and PGI Subpart 204.73

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

SCOPE/GENERAL:

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

A: Upon publication of DFARS Clause 252.204-7012 (November 18, 2013) it 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: What is the purpose of DFARS Clause 252.204-7012?

A: The clause was developed to provide a set of minimum standards to protect DoD unclassified CTI resident on or transiting through contractor's unclassified networks. It also prescribes reporting to DoD certain cyber incidents that affect this information.

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

A: When CTI is present on a contractor's system the controls must be in place.

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: What is the difference between technical information and intellectual property?

A: These two terms are often used to mean the same thing. The government views technical information as any technical data or computer software that can be used in the design, production, manufacture, development, testing, operation, or maintenance process of goods or materiel; or any technology that advances the state of the art in an area of

significant military applicability to the United States. Defense contractors view any such data or software created by them as intellectual property. Defense contractors should be willing to take the steps necessary to protect their own intellectual property which will ultimately mean better protection of technical information.

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:

- 1) 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 potential contractor will be required to develop and/or handle unclassified CTI.
- 2) 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 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:

- 1) 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.
- 2) 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.
- 3) 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.
- 4) 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: Who/Where is the Security Manager?

A: The generic term “Security Manager” was used at 204.7302(b)(2) because there is no standard term for this role in the DoD. The security manager for the purposes of this clause is the person who is knowledgeable in cybersecurity and NIST-SP 800-53. This particular aspect of the security manager’s role is also referred to as an information systems security engineer (ISSE) and may reside in Program Management Offices (PMOs), Program Executive

Offices (PEOs), Air Force Network Integration Center (AFNIC), Space and Naval Warfare Systems Command (SPAWAR), US Army Network Enterprise Technology Command (NETCOM), DISA Field Security Operations (FSO), or elements performing similar functions within a Component. In Program Management Offices, security managers typically insure that the program's information assurance/cybersecurity requirements are incorporated into the design of the system/product and are realized throughout development and production. Elsewhere, security managers are typically those who validate/certify that information systems meet information assurance/cybersecurity requirements prior to (and periodically during) operation.

SAFEGUARDING UNCLASSIFIED CTI: The contractor must comply with the minimum required security controls in DFARS Clause 252.204-7012 for all unclassified CTI resident on or transiting the contractor's unclassified information system(s).

Q: Where do I find the details on the Security Controls in Table 1? How do I read the Security Controls in Table 1?

A: The controls in Table 1 refer to the specific controls found in Appendix F, Security Controls Catalog, in NIST SP 800-53(version in effect at time of award). In Appendix F the controls are listed in security control families (e.g., Access Control, Incident Response), which are identified by a two-character identifier (e.g., AC=Access Control). The security control structure consists of (i) a control section; (ii) a supplemental guidance section; and (iii) a control enhancements section. The basic controls in each family are indicated by a number (e.g., AC-1, AC-2), followed by a description of the control and supplemental guidance that provides additional information. Many controls also include "enhancements" to the basic control. The security control enhancements provide statements of security capability to: (i) add functionality/specificity to a control; and/or (ii) increase the strength of a control, and when cited are indicated by a number in parenthesis following the basic control (e.g., AC-2(3)).

The controls listed in the table that are not followed by "(#)" require only the basic control. Controls listed with a (#) require both the basic control and the "control enhancement" corresponding to the #. The supplemental guidance section provides non-prescriptive, additional information for a specific security control, which may be applied by the contractor as appropriate. For many security controls, a degree of flexibility is provided in the description by allowing organizations (e.g., the contractor) to define values for certain parameters associated with the controls (e.g., password length & complexity; time before screen lock). This flexibility is achieved through the use of assignment and selection statements embedded within the security controls and control enhancements. Under the

clause, these values are to be left to the discretion of the contractor. Contracting Officers are not to specify the values that contractors may assign to the controls; they are applied to the contractor's internal information technology system, and will not be subject to change from contract to contract.

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.

In addition, exchanges of information among all interested parties, from the earliest identification of a requirement through receipt of proposals, are encouraged in accordance with FAR Part 15.201.

It should be noted that the security controls identified in Table 1 are intended to be applied to the contractor's general purpose internal information system transmitting, processing or storing CTI. Some specialized IT systems such as specialized medical IT, CNC machines, or industrial control systems which may have restrictions/limitations on the application of certain controls and would be granted exemption from the controls.

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

A: The DFARS rule did not add any additional requirement for the Government to monitor contractor implementation on the required security controls because this is a decision that should be made at the agency level. Failure to implement the controls to protect CTI that is resident on or transiting through contractor unclassified information systems would be a breach of contract.

CYBER INCIDENT REPORTING: When the Contractor reports a cyber incident, he/she will fill out and submit an Incident Collection Form (ICF) via the DIBNet portal (http://dibnet.dod.mil). On the main page, there is a link to the Incident Collection Form (ICF) for DIB reporting. 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) to obtain a document version of the form. The electronic submission is preferred for timely processing.

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 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: 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 if a subcontractor discovers a reportable cyber incident?

A: The subcontractor will report the incident to the prime and the prime will submit an incident report to DoD via (http://dibnet.dod.mil) within 72 hours of being notified of any cyber incident.

If a contractor is hosting unclassified CTI in the capacity of both a prime contractor and a subcontractor, and if the contractor is unable to determine specifically which contract effort is being impacted by a cyber incident, the contractor should report to both the prime as a subcontractor, and to the DoD via (http://dibnet.dod.mil) as a prime contractor.

Q: If the contractor is a participant in the DIB CS/IA Program will they have to submit multiple reports?

A: The Incident Collection Form (ICF) has been modified to include the 14 fields required under DFARS clause 252.204-7012. At the end of the DFARS fields, you may elect to continue to respond to the DIB CS/IA questions. We encourage you to provide additional information about the incident, along with the malware so that more complete cyber threat analysis can be performed.

Q: 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.

CONTRACTOR ACTIONS TO SUPPORT DAMAGE ASSESSMENT

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.