Guidance to Stakeholders for Implementing Defense Federal Acquisition Regulation Supplement Clause 252.204-7012 (Safeguarding Unclassified Controlled Technical Information)

Version 2.0

August 2015

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

Washington, D.C.

Guidance to Stakeholders for Implementing Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 (Safeguarding Unclassified Controlled Technical Information)

Deputy Assistant Secretary of Defense
Systems Engineering
3030 Defense Pentagon
3C167
Washington, DC 20301-3030
www.acq.osd.mil/se

Contents

This page intentionally blank.

1.0 Purpose

This guidance is intended for stakeholders charged with protection of unclassified controlled technical information (CTI) resident on or transiting through contractor information system(s) covered by DFARS 252-204-7012 (Safeguarding Unclassified Controlled Technical Information). CTI is technical information with military or space application that is subject to controls on its access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. This guide will assist stakeholders in carrying out their responsibilities should a defense contractor report a compromise on a contract that contains unclassified CTI.

2.0 Background

On November 18, 2013, the Department of Defense (DoD) published the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, "Safeguarding of Unclassified Controlled Technical Information." The clause requires a contractor to report to the Department the possible exfiltration, manipulation, or other loss or compromise of unclassified CTI; or other activities that allow unauthorized access to a contractor's unclassified information system on which unclassified CTI is resident or transiting. The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD(AT&L)) published a Procedures, Guidance, and Information (PGI) document for this DFARS clause[1] on December 16, 2014. Additional information about DFARS and PGIs is located on the Office of the Secretary of Defense (OSD) Defense Procurement and Acquisition Policy (DPAP) website[2]. This supplemental guidance is intended to assist stakeholders to carry out their responsibilities associated with DFARS reporting in the event a DFARS compromise occurs.

For references to this DFARS clause, see 48 CFR Part 252.204.7012 (Appendix C), DFARS PGI 204.73 (Appendix D), Instructions for Submitting Media (Appendix E), and Frequently Asked Questions (Appendix G).

The following stakeholders play important roles throughout the DFARS safeguarding unclassified CTI process:

- Defense Cyber Crime Center (DC3)/DoD/DIB Collaborative Information Sharing Environment Office (DCISE)
- Military Department (MILDEP) Damage Assessment Management Offices (DAMOs)
- OSD DAMO
- Requiring Activity (RA)

[1] 48 CFR Part 252.204.7012 PGI - http://www.acq.osd.mil/dpap/dars/pgi/pgi_pdf/PGI204_73.pdf
[2] DFARS and PGI Information - http://www.acq.osd.mil/dpap/dars/about_dfarspgi.html

3.0 DFARS Incident Reporting and Damage Assessment Process

Summary of contract-related responsibilities for the RA:

- During development of a solicitation, determine whether the relevant DoD technical information to be furnished by the Government and/or developed by the contractor contains unclassified CTI.
- Include DFARS Clause 48 CFR Part 252.204.7012 in all contracts containing unclassified CTI.
- Notify the contracting officer when a potential contractor will be required to develop and/or handle unclassified CTI.
- Review all DoD unclassified CTI to be provided to the contractor to verify that distribution statements and classification markings on the government-furnished information are valid/appropriate prior to submittal to the contractor.
- Include a statement in the solicitation that the contract will contain unclassified CTI. The Contract Data Requirements List (DD Form 1423 Contracts Data Requirement List Block 9) informs the bidder that the contract will contain unclassified CTI and indicates the marking requirements associated with each deliverable.
- Include in the statement of work a requirement that distribution statement(s) be applied to technical data products, in accordance with the distribution statement marking instructions as developed by the controlling DoD office and attached to the contract.
- Validate the contractor's execution of the Government's distribution statement marking instructions before delivery and acceptance of the technical data products.

Summary of stakeholder actions in responding to a reported DFARS cyber incident:

DC3

- Serve as the single point of contact for receiving electronic or hard copy DFARS incident submissions (via Incident Report as described in the Dec 2014 DEPSECDEF memo[3]).
- Analyze the DFARS incident report and provide the report to the government contracting officer point of contact identified in the report submission.
- Upon receipt of the contractor's DFARS incident report, send an unclassified e-mail message containing the submitted incident report as soon as possible to the contracting officer, with a courtesy copy to Director, DC3/DCISE; Director, OSD DAMO; and Director, DIB CS/IA Program Office.
- Post the DFARS incident report as soon as possible to the access-controlled Secret Internet Protocol Router Network (SIPRNet) location.

[3]DEPSECDEF Memo, Subj: (U) Directives in Response to Senate Armed Services Committee Report Highlighting Cyber Intrusions Affecting USTRANSCOM and Information-Sharing Challenges, dated December 20, 2014.

- In response to a RA contracting officer's request for media, receive compromised media from the contractor and transfer to OSD DAMO for subsequent analysis.

MILDEP DAMOs

- Coordinate with the MILDEP PCO and RA to request data from the contractor for damage assessment. Subcontractor data would be requested through the prime contractor.
- Inform OSD DAMO if the DFARS cyber incident reported in the incident report did not affect CTI on the protected information system(s).
- Conduct DFARS cyber incident damage assessments by including MILDEP-specific technical and operational expertise.
- Draft/coordinate final damage assessment reports.
- Distribute classified and unclassified reports as required. At a minimum, the contracting officer must receive an unclassified version of the damage assessment report.

OSD DAMO

- If multiple contracts are listed in one incident report for a single DFARS incident, designate a lead DAMO (MILDEP or OSD).
- Coordinate with the non-MILDEP DoD Component/PCO to request data from the contractor for damage assessment.
- Receive a copy of the contractor media from DC3 and load/index that data into the DAMO Automated Tool Suite (ATS) for assessment.
- Conduct DFARS cyber incident damage assessments for field agencies, similar to the assessments conducted by MILDEP DAMOs.

Requiring Activity

- Ensure the appropriate contracting officer communicates with the contractor for all government requests/interaction regarding the DFARS incident.
- Ensure that any discussions with a subcontractor include the contracting officer and prime contractor.
- Inform your chain of command (to the appropriate level) of a DFARS cyber incident and the resulting damage assessment reported under this DFARS clause.
- Contact the OSD DAMO (phone: 410-694-4380) to receive point of contact information for your DoD MILDEP DAMO, if the DAMO has not already contacted you.
- Coordinate with the respective DAMO on the request for contractor media following any reported compromises of DoD unclassified CTI.
- Notify the contracting officer of the decision regarding whether to request media, and provide the rationale.
- Coordinate with the security manager (i.e., the information systems security engineer who understands how to defend networks, is knowledgeable in National Institute of

Standards and Technology (NIST) requirements implementation, and has an understanding of securing/safeguarding procedures for networks, who will consult with the contracting officer before assessing contractor compliance with the requirements of DFARS 252.204-7012. The contracting officer shall consider such cyber incidents in the context of an overall assessment of the contractor's compliance with the DFARS requirements.

- Assess and implement appropriate programmatic, technical, and/or operational actions to mitigate risks identified in the damage assessment report. As appropriate, update the Program Protection Plan to reflect any changes as a result of the assessment.
- Following media review and impact assessment, provide the contracting officer with an unclassified damage assessment summary.

3.1 DFARS Cyber Incident Reporting Processes

3.1.1 DFARS Cyber Incident Reports

DFARS cyber incidents are reported to the Defense Cyber Crime Center (DC3) via the DIBNet portal[4]. *Note: DIBNet is a web portal for sharing threat information between DoD and DIB companies.* See appendix F for a list of reportable fields.

DC3 is the designated collection point for unclassified DFARS cyber incident reporting by DoD contractors required under DFARS Clause 252.204-7012[5]. Access to the DFARS cyber incident reporting site requires a DoD-approved medium assurance certificate. In the event that a contractor does not have anyone with a DoD-approved medium assurance certificate, the contractor may contact DC3 to make alternate arrangements for submissions.

If the contractor does not have all the information required by the clause within the 72-hour time constraint[6], specified in paragraph (d)(1) of the safeguarding clause, the contractor should report the details available at the time. If more information becomes available at a later date, the contractor should submit updates through the DIBNet portal.

3.1.2 Dissemination of the Incident Report

When DC3 receives a DFARS cyber incident report, DC3 will send an unclassified encrypted e-mail message containing the submitted incident report to the government contracting officer point of contact identified in the submitted report, with a courtesy copy to Director, DC3/DCISE; Director, OSD DAMO; and Director, DIB CS/IA Program Office. In addition, DC3 will post the

[4]DIBNet Portal - http://dibnet.dod.mil/
[5]Confidential DEPSECDEF Memorandum, Subject: (U) Directives in Response to Senate Armed Services Committee Report Highlighting Cyber Intrusions Affecting USTRANSCOM and Information-Sharing Challenges, dated December 20, 2014.
[6] DFARS Subpart 204.73-Safeguarding Unclassified Controlled Technical Information (Revised December 16, 2014).

submitted report to its SIPRNet portal as soon as possible. Authorized points of contact designated by the DoD Components will then have access to the incident report.

Upon receipt of the incident report from DC3, the contracting officer shall provide the incident report to the RA and place it in the contract file to document the action[7].

When the RA is notified by the contracting officer that a report has been submitted, the RA should contact OSD DAMO (phone: 410-694-4380) or the appropriate MILDEP DAMO. If needed, OSD DAMO will put the RA point of contact in touch with the appropriate MILDEP DAMO for further action.

3.1.3 Designating Lead DAMO and Lead Requiring Activity

If multiple contracts are listed in an incident report for a single DFARS incident, OSD DAMO will designate a lead DAMO (MILDEP or OSD) and lead requiring activity to coordinate damage assessment activities. The lead DAMO will work with the lead RA to interface with the contractor. In order to be designated as the lead, the RA must have a contract vehicle containing DFARS Clause 252.204-7012 with CTI identified in the contract. If all the affected contracts belong to one MILDEP, then the MILDEP DAMO will choose the lead RA. If an RA is from a defense agency or other non-MILDEP DoD entity, OSD DAMO will act as the lead DAMO.

3.1.4 Transfer of Lead DAMO

The lead DAMO shall coordinate the necessary damage assessment activities to include: identifying the lead RA who will request the media; ensuring the request for media includes input identifying affected media from the other DAMOs, review of the media, and development of the damage assessment report. The lead RA shall communicate the request for media, and all subsequent communications, through a single government contracting officer to ensure there is only one request for media. If, during the course of communications with the contractor, it is determined that a different Component (other than the initial Component) has the preponderance of information/equity in a case, the lead MILDEP DAMO may be transferred to the appropriate Component, subject to the requirement that the new lead must have a contract vehicle containing DFARS Clause 252.204-7012 with CTI identified in the contract. This transfer must be communicated to the RA and contracting officer as part of the hand-off process. Each MILDEP will retain the authority and responsibility to conduct a damage assessment of its affected contracts.

3.2 Incident Report Analysis and Request for Media

3.2.1 Incident Report Analysis

The relevant DAMO(s) will initiate an incident report review with the applicable RA(s) to determine whether or not the media (i.e., copies of the compromised data) need to be analyzed to

[7]DFARS Procedures, Guidance, and Information (PGI) 204.7303-4 DoD damage assessment activities (Added December 16, 2014)

assess the reported loss of unclassified CTI. If the media are required for analysis, the RA(s) and relevant DAMO(s) must request the data within 90 days, through the contracting officer, from the date the DFARS cyber incident was reported. The contracting officer must notify the contractor within this 90-day period, as the clause requires the contractor to preserve and maintain the media for 90 days.

3.2.2 Media Not Required from the Contractor

If media are not required, the RA will advise the contracting officer. The contracting officer will notify the contractor that media are not required, referencing the reported incident and including a courtesy copy to DC3, the appropriate DAMO, and the RA. The contracting officer will place this documented action in the contract files. The relevant DAMO should then submit a closure memo to OSD DAMO, closing the case.

3.2.3 Media Required from the Contractor

In cases in which the contractor media are required, the RA shall notify the contracting officer, who will then e-mail the contractor (referencing the incident report, with copy to DC3, the appropriate DAMO, and the RA) providing the following instructions to submit the compromised unclassified CTI:

1) The preferred method for submitting compromised unclassified CTI to the Government is to submit, on a clean hard drive (or other similar device), a copy of unclassified CTI file(s) associated with contracted DoD program(s), system(s), and technologies.

2) If the contractor is unable, or it is impractical, to submit the specific files, the contractor may submit system drive images. System drive images are bit-for-bit images of the compromised system(s) containing DoD information associated with the contract for which the incident was reported. When creating a bit-for-bit image of a hard drive, the image file(s) must be saved to a separate, clean hard drive or a hard drive that is overwritten with an approved application to erase any bits that could contaminate the image.

Detailed data submission instructions (e.g., contents of an accompanying cover letter, mailing address) can be found in the PGI and in appendix E of this document.

3.3 Dissemination of Reports

Nothing in the DFARS clause limits the Government's ability to conduct law enforcement, counterintelligence activities, or cybersecurity activities in the interest of national security. The results of the activities described in the DFARS clause may be used to support an investigation and prosecution of any person or entity, including attempts to infiltrate or compromise information on a contractor information system.

3.4 Information Handling

The Government shall protect information reported or otherwise provided to DoD under this clause in accordance with applicable statutes, regulations, and policies. Under DFARS, the Government may use attribution information and disclose it only to authorized persons for purposes and activities consistent with this clause[8].

4.0 Cyber Incident Damage Assessment and Response

Upon receipt of media, the affected DAMO(s) will conduct an assessment of the media to determine the impact of the unclassified CTI compromise. This assessment will involve analysis by subject matter experts, as appropriate, who have detailed knowledge of the unclassified CTI submitted by the contractor. Subject matter experts may include systems engineers, program management office personnel, scientists, intelligence community personnel, and military operations personnel. As the DAMOs assess the media, they should review the findings with the applicable RAs.

When all pertinent Component stakeholders complete their reviews, each relevant DAMO should write an unclassified summary and an appropriately classified damage assessment report detailing the impact of the compromise of the unclassified CTI. The relevant DAMO will share appropriate reports with its RA. The RA will provide the unclassified summary to the contracting officer, who will place the report in the contract file to document the contract action. In turn, the contracting officer will notify the contractor that the damage assessment process is complete. The lead DAMO should also submit a closure memo and full report to OSD DAMO once the damage assessment is complete. A MILDEP DAMO that has no equity in a DFARS case is not expected to submit a closure memo/e-mail to OSD. If more than one MILDEP DAMO has equities in a particular case, OSD DAMO will combine the separate assessments into one damage assessment report.

[8] DFARS Subpart 204.73-Safeguarding Unclassified Controlled Technical Information (Revised December 16, 2014).

Appendix A. Abbreviations and Acronyms

CTI	Controlled Technical Information
DAMO	Damage Assessment Management Office
DC3	Defense Cyber Crime Center
DCISE	Defense Industrial Base Collaborative Information Sharing Environment
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DIBNET	Defense Industrial Base Cyber Security/Information Assurance (DIB CS/IA) Program Network
DoD	Department of Defense
DPAP	Defense Procurement and Acquisition Policy
ICF	Incident Collection Format
MILDEP	Military Department
NIST	National Institute of Standards and Technology
OUSD(AT&L)	Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
PCO	Procuring Contracting Officer
PGI	Procedures, Guidance, and Instructions
RA	Requiring Activity
SIPRNet	Secret Internet Protocol Router Network

Appendix B. Definitions

Access. The ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. Committee on National Security Systems Instruction (CNSSI) – 4009

Compromise. Disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media, may have occurred. Committee on National Security Systems Instruction (CNSSI) – 4009

Cyber Incident. Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. Committee on National Security Systems Instruction (CNSSI) – 4009

Cyber Incident Damage Assessment. A managed, coordinated, and standardized process conducted to determine the impact on defense programs, defense scientific and research projects, or defense warfighting capabilities resulting from an intrusion into a DIB unclassified computer system or network.

Damage Assessment Management Office (DAMO). An OSD or Military Department organization that manages the analysis of compromised technical information from Defense Industrial Base (DIB) unclassified computer networks to determine the impact that compromised information has on programs, defense scientific and research projects, or defense warfighting capabilities.

DAMO Automated Tool Suite (ATS). A suite of tools located at the Defense Cyber Crime Center's DAMO Laboratory, that are used by the DAMOs to conduct damage assessment.

Media. Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, thumb drives, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system. Committee on National Security Systems Instruction (CNSSI) – 4009

Requiring Activity. The entity that has a requirement for supplies or services and requests the initiation of the acquisition. The requiring activity has personnel responsible for developing command resource requirements, identifying sources of funding, determining costs, acquiring funds, distributing and controlling funds, and tracking costs and obligations. DoD COR Handbook, dated March 22, 2012, http://www.acq.osd.mil/dpap/cpic/cp/docs/USA001390-12_DoD_COR_Handbook_Signed.pdf

Technical Information. Technical data or computer software as defined in DFARS Clause 252.227-7013, Rights in Technical Data-Non Commercial Items, regardless of whether or not the clause is incorporated in the solicitation or contract. Examples of technical information include

research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

- The data may be in tangible form, such as a blueprint, photograph, plan, instruction, or an operating manual, or may be intangible, such as a technical service or oral, auditory, or visual descriptions.
- Examples of technical data include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software.

Appendix C. 48 CFR Part 252.204.7012

SAFEGUARDING OF UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION (NOV 2013)

(a) *Definitions*. As used in this clause—

"Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

"Attribution information" means information that identifies the Contractor, whether directly or indirectly, by the grouping of information that can be traced back to the Contractor (e.g., program description or facility locations).

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

"Contractor information system" means an information system belonging to, or operated by or for, the Contractor.

"Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B-through-F, in accordance with DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

"Cyber incident" means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

"Exfiltration" means any unauthorized release of data from within an information system. This includes copying the data through covert network channels or the copying of data to unauthorized media.

"Media" means physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system.

"Technical information" means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Non Commercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract.

Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) *Safeguarding requirements and procedures for unclassified controlled technical information*. The Contractor shall provide adequate security to safeguard unclassified controlled technical information from compromise. To provide adequate security, the Contractor shall—

(1) Implement information systems security in its project, enterprise, or company-wide unclassified information technology system(s) that may have unclassified controlled technical information resident on or transiting through them. The information systems security program shall implement, at a minimum—

(i) The specified National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security controls identified in the following table; or

(ii) If a NIST control is not implemented, the Contractor shall submit to the Contracting Officer a written explanation of how—

(A) The required security control identified in the following table is not applicable; or

(B) An alternative control or protective measure is used to achieve equivalent protection.

(2) Apply other information systems security requirements when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

Table 1. Minimum Security Controls for Safeguarding

Minimum required security controls for unclassified controlled technical information requiring safeguarding in accordance with paragraph (d) of this clause. (A description of the security controls is in the NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations" (http://csrc.nist.gov/publications/PubsSPs.html).)

Access Control AC-2 AC-3(4) AC-4 AC-6 AC-7 AC-11(1) AC-17(2) AC-18(1) AC-19 AC-20(1) AC-20(2) AC-22	Audit & Accountability AU-2 AU-3 AU-6(1) AU-7 AU-8 AU-9 Configuration Management CM-2 CM-6 CM-7 CM-8	Identification & Authentication IA-2 IA-4 IA-5(1) Incident Response IR-2 IR-4 IR-5 IR-6 Maintenance MA-4(6) MA-5 MA-6	Media Protection MP-4 MP-6 Physical & Environmental Protection PE-2 PE-3 PE-5 Program Management PM-10 Risk Assessment RA-5	System & Comm Protection SC-2 SC-4 SC-7 SC-8(1) SC-13 SC-15 SC-28 System & Information Integrity SI-2 SI-3 SI-4
Awareness & Training AT-2	Contingency Planning CP-9			

Legend:

AC: Access Control	MA: Maintenance
AT: Awareness and Training	MP: Media Protection
AU: Auditing and Accountability	PE: Physical & Environmental Protection
CM: Configuration Management	PM: Program Management
CP: Contingency Planning	RA: Risk Assessment
IA: Identification and Authentication	SC: System & Communications Protection
IR: Incident Response	SI: System & Information Integrity

(c) *Other requirements*. This clause does not relieve the Contractor of the requirements specified by applicable statutes or other Federal and DoD safeguarding requirements for Controlled Unclassified Information (CUI) as established by Executive Order 13556, as well as regulations and guidance established pursuant thereto.

(d) *Cyber incident and compromise reporting.*

(1) *Reporting requirement*. The Contractor shall report as much of the following information as can be obtained to the Department of Defense via (http://dibnet.dod.mil/) within 72 hours of discovery of any cyber incident, as described in paragraph (d)(2) of this clause, that affects unclassified controlled technical information resident on or transiting through the Contractor's unclassified information systems:

(i) Data Universal Numbering System (DUNS).

(ii) Contract numbers affected unless all contracts by the company are affected.

(iii) Facility CAGE code if the location of the event is different than the prime Contractor location.

(iv) Point of contact if different than the point of contact recorded in the System for Award
Management (address, position, telephone, e-mail).

(v) Contracting Officer point of contact (address, position, telephone, e-mail).

(vi) Contract clearance level.

(vii) Name of subcontractor and CAGE code if this was an incident on a Sub-contractor network.

(viii) DoD programs, platforms or systems involved.

(ix) Location(s) of compromise.

(x) Date incident discovered.

(xi) Type of compromise (e.g., unauthorized access, inadvertent release, other).

(xii) Description of technical information compromised.

(xiii) Any additional information relevant to the information compromise.

(2) *Reportable cyber incidents*. Reportable cyber incidents include the following:

(i) A cyber incident involving possible exfiltration, manipulation, or other loss or compromise of any unclassified controlled technical information resident on or transiting through Contractor's, or its subcontractors', unclassified information systems.

(ii) Any other activities not included in paragraph (d)(2)(i) of this clause that allow unauthorized access to the Contractor's unclassified information system on which unclassified controlled technical information is resident on or transiting.

(3) *Other reporting requirements*. This reporting in no way abrogates the Contractor's responsibility for additional safeguarding and cyber incident reporting requirements pertaining to its unclassified information systems under other clauses that may apply to its contract, or as a result of other U.S. Government legislative and regulatory requirements that may apply (e.g., as cited in paragraph (c) of this clause).

(4) *Contractor actions to support DoD damage assessment.* In response to the reported cyber incident, the Contractor shall—

(i) Conduct further review of its unclassified network for evidence of compromise resulting from a cyber-incident to include, but is not limited to, identifying compromised computers, servers, specific data and users accounts. This includes analyzing information systems that were part of the compromise, as well as other information systems on the network that were accessed as a result of the compromise;

(ii) Review the data accessed during the cyber incident to identify specific unclassified controlled technical information associated with DoD programs, systems or contracts, including military programs, systems and technology; and

(iii) Preserve and protect images of known affected information systems and all relevant monitoring/packet capture data for at least 90 days from the cyber incident to allow DoD to request information or decline interest.

(5) *DoD damage assessment activities*. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor point of contact identified in the incident report at (d)(1) of this clause provide all of the damage assessment information gathered in accordance with paragraph (d)(4) of this clause. The Contractor shall comply with damage assessment information requests. The requirement to share files and images exists unless there are legal restrictions that limit a company's ability to share digital media. The Contractor shall inform the Contracting Officer of the source, nature, and prescription of such limitations and the authority responsible.

(e) *Protection of reported information*. Except to the extent that such information is lawfully publicly available without restrictions, the Government will protect information reported or otherwise provided to DoD under this clause in accordance with applicable statutes, regulations, and policies. The Contractor shall identify and mark attribution information reported or otherwise provided to the DoD. The Government may use information, including attribution information and disclose it only to authorized persons for purposes and activities consistent with this clause.

(f) Nothing in this clause limits the Government's ability to conduct law enforcement or counterintelligence activities, or other lawful activities in the interest of homeland security and national security. The results of the activities described in this clause may be used to support an investigation and prosecution of any person or entity, including those attempting to infiltrate or compromise information on a contractor information system in violation of any statute.

(g) *Subcontracts*. The Contractor shall include the substance of this clause, including this paragraph (g), in all subcontracts, including subcontracts for commercial items.

Appendix D. DFARS Procedures, Guidance, and Instructions (PGI) 204.73

DFARS Procedures, Guidance and Instructions (PGI) 204.73—SAFEGUARDING UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION

PGI 204.7303 Procedures.

PGI 204.7303-1 General.

(a) The contracting officer will be notified by the requiring activity when a solicitation is expected to result in a contract that will require unclassified controlled technical information (CTI) to be furnished by the Government and/or developed by the contractor.

(b) The contracting officer shall—

(1) Notify the requiring activity that all DoD unclassified CTI provided to the contractor shall be marked with the appropriate distribution statement B-F (see DoDI 5230.2, Distribution Statements on Technical Documents);

(2) Ensure that the contract, task order, or delivery order includes a requirement (such as a contract data requirements list) for the contractor to apply the appropriate distribution statement(s) on any unclassified CTI developed by the contractor; and

(3) Coordinate with the requiring activity for instruction regarding the disposition of unclassified CTI associated with the contract. In cases where contract administration has been delegated to an administrative contracting officer (ACO), the ACO shall request the cognizant procuring contracting officer (PCO) to coordinate with the requiring activity.

(c) The safeguarding requirements and procedures apply to the unclassified CTI until such time as the distribution statement identifying information as unclassified CTI (distribution statement B-F) is changed or removed by the controlling DoD office.

PGI 204.7303-2 Safeguarding controls.

(a) The DoD Chief Information Officer (CIO) is responsible to ensure contractor information systems are assessed in a standard way. When a contractor provides a written explanation that either DFARS 252.204-7012(b)(1)(ii)(A) or (B) apply, the contracting officer shall send the written explanation to the requiring activity and the DoD CIO at osd.dibcsia@mail.mil for adjudication and response.

(b) Table 1 of DFARS clause 252.204-7012 requires that contracting officers not specify the values that contractors may assign to the controls; they are applied to the contractor's internal information technology system, and cannot be subject to change from contract to contract.

(c) For additional information on the safeguarding controls, see the Frequently Asked Questions document at:
http://www.acq.osd.mil/dpap/pdi/docs/ControlledTechnicalInformation_FAQ.pdf

PGI 204.7303-3 Cyber incident and compromise reporting.

(a) When a cyber incident is reported by a contractor, the Defense Cyber Crime Center (DC3) will send an unclassified encrypted e-mail containing the DIBNet-generated Incident Collection Form (ICF) to the contracting officer(s) identified on the ICF. The Defense Cyber Crime Center may request the contracting officer to send a digitally signed e-mail to DC3 in order to enable the contracting officer to read the ICF.

(1) The PCO shall notify the requiring activities that have contracts identified in the ICF. In cases where an ACO receives the ICF, in lieu of the PCO, the ACO shall notify the PCO for each affected contract, who will then notify the requiring activity.

(2) The requiring activity may request that the contracting officer assess contractor compliance with the requirements of DFARS 252.204-7012, in accordance with DFARS 204.7302(b)(2). In cases of cyber incidents involving multiple contracts, a single contracting officer will be designated and notified by a requiring activity. If requested to assess compliance, the contracting officer shall—

(i) Consult with the security manager, as identified by the requiring activity. The security manager 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 ensure 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; and

(ii) Consider the following options, if additional information is necessary to assess contractor compliance:

(A) Request a description of the implementation of the controls in DFARS 252.204-7012, *Table 1 – Minimum Security Controls for Safeguarding*, including requesting specific values (if not already requested prior to award), in order to support evaluation of whether any of the controls were inadequate, or if any of the controls were not implemented at the time of the incident.

(B) Request the contractor's assessment of the cause of the cyber incident, e.g., what, if any, security control was inadequate or circumvented. As indicated in DFARS 204.7302(b)(2), a cyber incident does not imply that the contractor has failed to provide adequate information safeguards for unclassified CTI, or has otherwise failed to meet the requirements of DFARS 252.204-7012.

(iii) Provide a copy of the assessment of contractor compliance to the requiring activity and to the DoD CIO, osd.dibcsia@mail.mil. A copy of the assessment will be provided to other contracting officers listed on the ICF by their respective requiring activity.

PGI 204.7303-4 DoD damage assessment activities.

(a) In cases of cyber incidents involving multiple contracts, a single contracting officer will be designated to coordinate with the contractor regarding media submission.

(1) If the requiring activity requests the contracting officer to obtain media, as defined in DFARS 252.204-7012, from the contractor, the contracting officer shall—

(i) Provide a written request for the media;

(ii) Provide the contractor with the "Instructions for Media Submission" document available here; and

(iii) Provide a copy of the request to DC3 (dcise@dc3.mil) and the requiring activity.

(2) If the contracting officer is notified by the requiring activity that media are not required, the contracting officer shall notify the contractor and simultaneously provide a copy of the notice to DC3 and the requiring activity.

(3) The contracting officer shall document the action taken as required by paragraph (a)(1) or (2) of this section, in the contract file.

(b) Upon receipt of the contractor media, DC3 will confirm receipt in writing to the contractor and the requesting contracting officer.

(c) The requiring activity will provide the contracting officer with a report documenting the findings from the damage assessment activities affecting unclassified CTI.

(d) The contracting officer shall include the report documenting the findings in the contract file(s) and provide a copy to the contractor.

PGI 204.7303-5 Subcontracts.

(a) The incident reporting required at DFARS 252.204-7012(d)(1) will be submitted by the prime contractor to the DoD via http://dibnet.dod.mil within 72 hours of notification from the subcontractor of any cyber incident.

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

Appendix E. Instructions for Submitting Media

1) For those instances when the contractor can identify all the files containing unclassified controlled technical information (CTI) that are part of the compromise, submit a copy of each file containing unclassified CTI associated with the compromise.

2) If the contractor cannot identify all the files containing unclassified CTI associated with the compromise, then the contractor can submit a bit for bit image. In these cases, the preparation of the drive image(s) should be as follows for submission: create the image on a separate wiped hard drive, where the hard drive is overwritten using a suitable application or hardware that overwrites previous data with a pattern of binary data. The hard drive can be wiped with utilities such as Unix 'dd' application or other commercially available hard drive duplicators with a drive wiping feature. Suitable applications for creating drive images include, but are not limited to, the following:

(A) Guidance Software's EnCase (software)

(B) Access Software's FTK Imager (software)

(C) Open source dd application (software)

(D) Hard Drive Duplicator (hardware)

3) Submission of Media (as described in (1) and (2) above)

(A) Create a cover letter that includes the following information:

(i) Incident collection form report number.

(ii) Description of the type and number of media being submitted, along with make, model, and serial numbers and/or other identifying information as appropriate.

(iii) Explanation of how the media relate to the cyber incident. This description should provide context to the media submission, not simply repeat the incident summary reported in the incident report.

(iv) MD5 hash results for each item submitted.

(B) Send the cover letter and media via registered USPS mail, FedEx, UPS, or agency drop to:

DIBCERT (DCISE MAC)

911 Elkridge Landing Rd

Linthicum, MD 21090-2993

(C) Send a digitally signed e-mail to dcise@dc3.mil indicating media have been shipped. The subject line should read, "Media submission for [Incident Number]". If the image files are password-protected, include the password in this e-mail.

(D) For more information, please contact DIBCERT: 410-981-0104, dcise@dc3.mil.

4) Upon receipt of the contractor media, DC3 will e-mail the contractor and the contracting officer(s) for each affected contract to confirm the media have been received.

Appendix F. Incident Collection Format (ICF) Template

1.) UNCLASSIFIED//FOR OFFICIAL USE ONLY (when filled in)

2.) FOR INTERNAL USE ONLY

3.) Report ID: xxx-xxxxx

4.) Company Name: xxxxx

5.) DUNS Number: xxxxx

6.) Contract Number Affected (Additional contract numbers can be added on a subsequent page):
xxxxxx-xx-x-xxxx

7.) Contract Clearance Level: xxxxxx

8.) Facility CAGE Code: xxxxx

9.) Does this incident affect cloud services provided to DoD?: xx

10.) Does this incident impact unclassified controlled technical information as defined in DFARS
clause 252.204-7012?: xxx

11.) Last Name: Xxxxxxx

12.) First Name: Xxxxxx

13.) Position/Title: xxxxxxxxxx

14.) Location: xxxxxxxxxxxxxxx

15.) City: xxxxxxxxxx

16.) State: xxxxxxxxxxxxx

17.) Postal Code: xxxxx

18.) Telephone: xxx-xxx-xxxx

19.) E-mail Address: xxxxxx.xxxxx@xxxxxx.xxxx

20.) Subcontractor Name [if incident was on a subcontractor network]: xxxxx

21.) Subcontractor CAGE Code: xxxxxx

22.) DoD Programs, Platforms, or Systems Involved: xxxxxxxxxxxxxxxxxxxxx

23.) Location(s) of Compromise:
xxxxxxxxxxxxxxx
1234 Main St
Anywhere, USA xxxxxx

24.) Date Incident Discovered: xx Xxxx xxxx

25.) Description of Technical Information Compromised: xxxxxxxxxxxxxxxxxxx

26.) Additional Information Relevant to the Information Compromised: xxxxxxxxxxxxxxxxx

27.) Add additional contract numbers: xxxxxx

28.) Add additional Point of Contact: xxxxxx

29.) Last Name: Xxxxxxx

30.) First Name: Xxxxxxxx

31.) Location: Xxxxxxxxxx

32.) City: Xxxxxxxxx

33.) State: Xxxxxxx

34.) Postal Code: xxxxx

35.) Telephone: xxx-xx-xxxx

36.) E-mail Address: xxxxxxxxxxxxxxx@xxx.xxx

37.) Add additional contract numbers: xxxxxxxxxx

38.) Add additional Point of Contact: xxxxxx

39.) NOTICE: DFARS Rule 252.204-7012 requires the preservation of all media associated with all identified targeted systems, for a minimum period of 90 days. Agree / Disagree? xxxx

40.) UNCLASSIFIED//FOR OFFICIAL USE ONLY (when filled in)

Appendix G. Frequently Asked Questions (FAQs)

Following are 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 Federal Acquisition Regulation (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 controlled technical information (CTI) resident on or transiting through a 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 interchangeably. 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 ultimately will 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), U.S. Army Network Enterprise Technology

Command (NETCOM), Defense Information Systems Agency Field Security Operations (FSO), or elements performing similar functions within a Component. In PMOs, security managers typically ensure 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 and 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 Chief Information Officer 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.

Q: What is a reportable incident?

A: Any possible exfiltration, manipulation, or other loss or compromise of unclassified CTI; or other activities that allow unauthorized access to a contractor's unclassified information system on which unclassified CTI is resident or transiting. Loss or compromise of CTI in this context could include loss of a laptop or any other media that contains unclassified CTI.

DFARS CYBER INCIDENT REPORTING: The contractor reports a DFARS cyber incident by filling out and submitting an Incident Collection Format (ICF) via the DIBNet portal (http://dibnet.dod.mil). On the main page, there is a link to the ICF for DIB reporting. Access to this format requires a DoD approved medium assurance public key infrastructure (PKI) certificate. In the event a contractor 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 format. 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 a cyber incident?

A: When the contractor does not have all the information required by the clause within that time constraint, the contractor 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 e-mail 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 the prime's 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 the contractor have to submit multiple reports?

A: The Incident Collection Format (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 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 if a contractor is also a member of the DIB CS/IA program? How should a contractor report an incident?

A: A contractor should fulfill all obligations in the contract with the Government first. The DFARS clause is a contractual requirement that must be fulfilled. It is at the discretion of the contractor whether also to submit information regarding the incident under the DIB CS/IA program. Nothing precludes a contractor, who is also a member of the DIB CS/IA program, from submitting under both DFARS and the voluntary DIB CS/IA program.

CONTRACTOR ACTIONS TO SUPPORT DAMAGE ASSESSMENT

Q: If the contractor is required to submit media, what is the correct format and procedure?

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

Guidance to Stakeholders for Implementing Defense Federal Acquisition Regulation Supplement Clause 252.204-7012 (Safeguarding Unclassified Controlled Technical Information)

Deputy Assistant Secretary of Defense
Systems Engineering
3030 Defense Pentagon
3C167
Washington, DC 20301-3030
www.acq.osd.mil/se