
This Memo is expired. DFAR Clause 252.204-7012 was updated in August of 2015. The guidance in this memo applies to the November 2013 version of the clause (attached to the memo). Guidance relevant to the updated clause will be posted in REMS

June 18, 2014

To: Contract & Grant Officers

Subject: DFAR 252.204-7012: Safeguarding of Unclassified Controlled Technical Information

Purpose

This memo provides guidance for accepting contracts from the Department of Defense containing Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012: Safeguarding of Unclassified Controlled Technical Information (*see November 2013 version of clause attached to this memo*).

Background

In November 2013, the Department of Defense (DoD) issued a final rule amending the DFARS to add contract clause 252.204-7012, which addresses requirements for safeguarding unclassified controlled technical information resident on or transiting through our systems. The prescription requires insertion of the clause in all DoD contracts.

252.204-7012 defines “Controlled Technical Information” as follows:

“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.

Guidance

Note that the definition contains a carve-out for information that is “lawfully publicly available without restrictions.” Thus, the clause would not apply to information generated by the University under the Fundamental Research Exclusion (FRE) since such information would be “legally publicly available without restrictions.” However, the obligations in the clause could apply to Controlled Technical Information transmitted to us by DoD (or a third party). As per current standard policy, it is important that receipt of such information not compromise our ability to operate under the FRE. That is, consistent with current practice, any Controlled

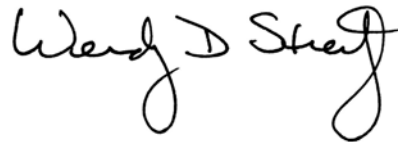
Technical Information provided should be the minimal background information needed to inform the research, and should be transmitted only to one or two individuals legally eligible to receive it and who are properly informed about their responsibilities in receiving the information. In addition, the larger research team should not need access to Controlled Technical Information in order to participate in the research project. Researchers should be informed about the added administrative and financial burdens* of accepting such information under DFARS 252.204-7012. Additionally, prior to the acceptance of any Controlled Technical Information a researcher must ensure that:

- 1) The C&G Office is consulted;
- 2) The transmitter will indicate whether the information they are providing is controlled by DoD Instruction 5230.24 or is otherwise subject to export controls (and if so the ECCN should be provided); and
- 3) The proper safeguards required by 252.204-7012 are in place.

* Note: To establish the burdens of establishing a compliant system, campuses will have to consult with their IT departments

Contact

Lourdes DeMattos
Lourdes.DeMattos@ucop.edu
(510) 987-9850



Wendy D. Streit
Executive Director
Research Policy Analysis & Coordination

Attachments: 252.204-7012: Safeguarding of Unclassified Controlled Technical Information
Sample 252.204-7012 Informed Participation Agreement

The attachment may not be viewable in your web browser. Download this memo, and view it in a PDF viewer, such as Adobe Reader or Acrobat, to ensure your access to the attachment.

252.204-7012 Informed Participation Agreement

This acknowledgment is made by me to The Regents of the University of California, hereinafter called "University," in part consideration of my participation on the Department of Defense funded project entitled, "____", hereinafter called "Project."

By execution of this acknowledgment, I hereby document my understandings with respect to the acceptance of any Controlled Technical Information (**CTI**), as defined in DFAR Clause 252.204-7012 and pasted below. I acknowledge that it is my responsibility to make sure each member of my team understands the requirements associated with acceptance of CTI. I understand that the University has accepted the DoD award for the Project with the understanding that I and my team will be performing open fundamental research and that this precept cannot be compromised.

I understand that if the receipt of CTI is absolutely necessary as *background* in order for me to accomplish the goals of this project, such CTI must be limited, submitted only to me, and I must not share the information further.

Prior to receipt of CTI, I will consult with the C&G Office in order to assure that the University can continue to enjoy exemptions provided under the export control regulations (i.e., the Fundamental Research Exclusion, or FRE)¹ and that all the proper systems safeguards required by 252.204-7012 and any otherwise required control plans are in place.

If CTI is accepted, the IT department must be consulted. I understand that the cost of establishing a compliant system cannot be estimated and that all costs will be borne by my department.

"Controlled technical information" (CTI) 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.

¹ Please refer to the [Export Compliance FAQ](#) for more information about the FRE.

UNIVERSITY
OF
CALIFORNIA

I acknowledge that I am bound to do all things necessary to enable University to perform its obligations under the contract.

Principal Investigator:

Signature

Date

Name

252.204-7012 Safeguarding of Unclassified Controlled Technical Information.
As prescribed in [204.7303](#), use the following clause:

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 is 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>).)

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

Legend:

AC: Access Control

AT: Awareness and Training

AU: Auditing and Accountability

MA: Maintenance

MP: Media Protection

PE: Physical & Environmental Protection

CM: Configuration Management
CP: Contingency Planning
IA: Identification and Authentication
IR: Incident Response

PM: Program Management
RA: Risk Assessment
SC: System & Communications Protection
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 POC recorded in the System for Award Management (address, position, telephone, email).
- (v) Contracting Officer point of contact (address, position, telephone, email).
- (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.

(End of clause)