PART 204—ADMINISTRATIVE MATTERS

*** * * * ***

[SUBPART 204.74—SAFEGUARDING UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION

204.7400 Scope.

(a) This subpart applies to contracts and subcontracts requiring safeguarding of unclassified controlled technical information resident on or transiting through contractor unclassified information systems.

(b) This subpart does not abrogate any existing contractor physical, personnel, or general administrative security operations governing the protection of unclassified DoD information, nor does it impact requirements of the National Industrial Security Program.

204.7401 Definitions.

As used in this subpart—

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

"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.

"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.

204.7402 Policy.

(a) DoD and its contractors and subcontractors will provide adequate security to safeguard unclassified controlled technical information on their unclassified information systems from unauthorized access and disclosure.

(b) When safeguarding is applied to controlled technical information resident on or transiting contractor unclassified information systems—

(1) Contractors must report to DoD certain cyber incidents that affect unclassified controlled technical information resident on or transiting contractor unclassified information systems. Detailed reporting criteria and requirements are set forth in the clause at 252.204-7012, Safeguarding of Unclassified Controlled Technical Information.

(2) A cyber incident that is properly reported by the contractor shall not, by itself, be interpreted under this clause as evidence that the contractor has failed to provide adequate information safeguards for unclassified controlled technical information, or has otherwise failed to meet the requirements of the clause at 252.204-7012. When a cyber incident is reported, the contracting officer shall consult with a security manager of the requiring activity prior to assessing contractor compliance. The contracting officer shall consider such cyber incidents in the context of

an overall assessment of the contractor's compliance with the requirements of the clause at 252.204-7012.

204.7403 Contract clause.

Use the clause at 252.204-7012, Safeguarding of Unclassified Controlled Technical Information, in all solicitations and contracts including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items.]

* * * * *

PART 212—ACQUISITION OF COMMERCIAL ITEMS

* * * * *

SUBPART 212.3—SOLICITATION PROVISIONS AND CONTRACT CLAUSES FOR THE ACQUISITION OF COMMERCIAL ITEMS

212.301 Solicitation provisions and contract clauses for acquisition of commercial items.

(f) * * *

[(vi) Use the clause at 252.204-7012, Safeguarding of Unclassified Controlled Technical Information, as prescribed in 204.7403.]

* * * * *

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

* * * * *

SUBPART 252.2—TEXT OF PROVISIONS AND CLAUSES

* * * * *

[252.204-7012 Safeguarding of Unclassified Controlled Technical Information.
As prescribed in 204.7403, use the following clause:

SAFEGUARDING OF UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION (DATE)

(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: 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	Audit & Accountability	Identification and Authentication	Media Protection	System & Comm Protection
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)		SC-7
			Physical and Environmental Protection	
AC-6	AU-7			SC-8(1)
		Incident Response		
AC-7	AU-8		PE-2	SC-13
AC-11(1)	AU-9	IR-2	PE-3	
AC-17(2)		IR-4	PE-5	SC-15
	Configuration			
AC-18(1)	Management	IR-5		SC-28
			Program Management	
AC-19	CM-2	IR-6		
				System & Information Integrity
AC-20(1)	CM-6		PM-10	

AC-20(2)	**CM-7**	**Maintenance**		**SI-2**
AC-22	**CM-8**	**MA-4(6)**	**Risk Assessment**	**SI-3**
		MA-5	**RA-5**	**SI-4**
Awareness & Training	**Contingency Planning**	**MA-6**		
AT-2	**CP-9**			

Legend:

AC: Access Control
AT: Awareness and Training
AU: Auditing and Accountability
CM: Configuration Management
CP: Contingency Planning
IA: Identification and Authentication
IR: Incident Response
MA: Maintenance
MP: Media Protection
PE: Physical & Environmental Protection
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)]