DFARS 252.204-7012 Defense Industrial Base Compliance Information

Protecting Controlled Unclassified Information (CUI)

Executive Order 13556 "Controlled Unclassified Information," November 2010

Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes the method by which the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies.

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

Executive Order 13556, "Controlled Unclassified Information" (the Order) establishes a program for managing CUI across the Executive branch. The Order designates the National Archives and Records Administration (NARA) as Executive Agent to implement the Order and to oversee Federal agency actions to ensure compliance. The Archivist of the United States delegated these responsibilities to the Information Security Oversight Office (ISOO).

32 CFR Part 2002 "Controlled Unclassified Information" was issued by ISOO to establish policy for Federal agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, self-inspection and oversight requirements, and other facets of the Program. The rule affects Federal executive branch agencies that handle CUI and all organizations (sources) that handle, possess, use, share, or receive CUI—or which operate, use, or have access to Federal information and information systems on behalf of an agency. Notably, this coverage includes the U.S. Department of Defense; it's Component agencies and it's Services.

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

The DoD implementation of the EO was issued December 2015 as the "Guidance to Stakeholders for Implementing Defense Federal Acquisition Regulation Supplement Clause 252.204-7012 (Safeguarding Unclassified Controlled Technical Information)." It was subsequently amended, and now states that any, and all, contractors to DoD who will handle CUI must comply with these provisions with, at minimum, a System Security Plan (SSP) that includes a Plan of Action and Milestones (POA&M) before December 31st, 2018.

Penalties for failure to comply with the DFARS 252.205-7012 requirement include contract revocation. If a contractor uses a computer system, connects to the Internet, and handles CUI, this is a DFARS contract clause that requires more than an affirmative check-the-box response.

In the following paragraphs, additional information about these provisions is provided.

What is 'Technical Information' as defined in DFARS?

Technical data or computer software is defined in DFARS Clause 252.227-7013, Rights in Technical Data - Non-Commercial Items. Importantly, this definition applies to technical data used by contractors, 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.

Current Requirement for DoD FRCS / DoD Control Systems Contractors – Compliance standards for the DFARS 7012 regulatory requirement are published by the National Institute of Standards and Technology (NIST) in its Special Publication 800-171. All FRCS projects that will collect, transmit, or store CUI data must have a current System Security Plan (SSP), or Cyber Risk Management Plan (CRMP) IAW with NIST SP 800-171 and the DFARS CUI Guide, with a Plan of Action and Milestones (POA&M) established to introduce, correct, or remediate elements of a contractors' operations that do not comply with the NIST 800-171 framework. It is important to note that due to wide mission-set, the NIST 800-171 framework is intentionally widely scoped. Compliance may be treated in a variety of ways, not all of them technological.

The IE and ESTCP offices wish to assist contractors/vendors completing a CRMP or SSP by providing templates of many frequently used documents. Note the templates can be used for both corporate IT business systems and OT FRCS projects. Typical CUI data on corporate IT systems includes design drawings and site information (CAD, BIM, GIS), specifications, test results, and consumption data (meter, site data). Typical CUI on OT projects includes network traffic (Modbus, BACNet, TCP/IP) between HMI and lower level controllers, configuration files, hardware/software versions and hashes, and consumption data (meter, site data). However, our provision of these documents does not mean that our offices in any way have approved a contractor's SSP/CRMP; nor that we advocate any one particular approach as being the correct way to approach compliance.

The following documents are typically included in the SSP/CRMP (presented in order of recommended completion):

- NIST SP 800-171 Cyber Risk Management Plan Table of Contents – use the NIST SP 800-171 Excel file
- Event/Incident Communications Plan (EICP) – use the modified FedRAMP template and ESTCP EICP Graphics PowerPoint
- Event/Incident Response Plan (EIRP) – use the modified FedRAMP templates
- Information Systems Contingency and CONOPS Plan (ISCP) – use the modified FedRAMP template
- Information Systems Policies and Procedures (ISPP) – use the Word document template
- Security Audit Plan (SAP) – use the modified NIST template
- System Security Plan (SSP) – recommend using the CSET tool/template
- Security Assessment Report (SAR) – Most FRCS projects will not require a SAR, however, many insurance companies or AO's may require a SAR. An organization can use the modified FedRAMP template.
- Plan of Action & Milestones (POAM) – use the modified FedRAMP templates (GSA and DoD provided) (POAM Template)
- DIBNet Incident Reporting Form – use the DFARS CUI Excel file template for a DoD data incident
- US-CERT Incident Response Form – use the Excel file template for a non-DoD data incident
- CJCSM 6510.01B - Cyber Incident Handling Program 2012 – use the procedures outlined in the manual and the Excel file template

The DFARS Guide 2015 Guidance to Stakeholders for Implementing Defense Federal Acquisition Regulation Supplement - This guidance is intended for stakeholders charged with protection of unclassified controlled technical information (CUI or UCTI) 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.

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting – This is the DFARS Contract clause an investigator should look for in their contract/subcontract. If the ESTCP contract does not include this clause, contact the ESTCP office so a modification can be issued.

NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations - The protection of Controlled Unclassified Information (CUI) while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations. The

requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components. The CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

NIST SP 800-171B (Draft) – This Draft addendum is intended to provide context and insight to contracting agencies. It suggests a three-level hierarchy of criticality for evaluating contractor compliance.

CJCSM 6510.01B Cyber Incident Handling Program 2012 - This manual describes the Department of Defense (DoD) Cyber Incident Handling Program and specifies its major processes, implementation requirements, and related U.S. government interactions.

CUI Categories and Subcategories

Twenty-two categories of CUI data are defined by the National Archives and Records Administration (NARA), of which five are pertinent to the Installations and Environment community and related to the Critical Infrastructure Category: Controlled Technical Information, Critical Infrastructure, DoD Critical Infrastructure Security Information, Critical Energy Infrastructure Information, Physical Security, and Protected Critical Infrastructure Information.

Category-Subcategory: Controlled Technical Information

Category Description: 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 Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.2277013). 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.

Subcategory Description: N/A **Marking: CTI**

Category-Subcategory: Critical Infrastructure

Category Description: Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.

Subcategory Description: N/A **Marking:** CRIT

Category-Subcategory: Critical Infrastructure-DoD Critical Infrastructure Security Information

Category Description: Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.

Subcategory Description: Information that, if disclosed, would reveal vulnerabilities in the DoD critical infrastructure and, if exploited, would likely result in the significant disruption, destruction, or damage of or to DoD operations, property, or facilities, including information regarding the securing and safeguarding of explosives, hazardous chemicals, or pipelines, related to critical infrastructure or protected systems owned or operated on behalf of the DoD, including vulnerability assessments prepared by or on behalf of the DoD, explosives safety information (including storage and handling), and other site-specific information on or relating to installation security.

Marking: DCRIT

Category-Subcategory: Critical Infrastructure-Critical Energy Infrastructure Information

Category Description: Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.

Subcategory Description: Critical energy infrastructure information means specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that: (i) Relates details about the production, generation, transportation, transmission, or distribution of energy; (ii) Could be useful to a person in planning an attack on critical infrastructure; and (iii) Does not simply give the general location of the critical infrastructure.

Marking: CEII

Category-Subcategory: Critical Infrastructure-Physical Security

Category Description: Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.

Subcategory Description: Related to protection of federal buildings, grounds or property.

Marking: PHYS

Category-Subcategory: Critical Infrastructure-Protected Critical Infrastructure Information

Category Description: Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.

Subcategory Description: As defined by 6 USC 131-134, and 6 CFR 29, PCII relates to threats, vulnerabilities, or operational experience related to the national infrastructure. PCII offers protection to private sector infrastructure information voluntarily shared with government entities for purposes of homeland security.

Marking: PCII