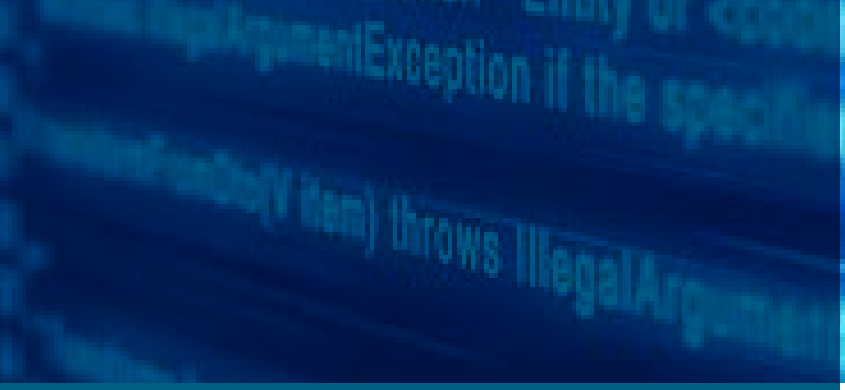
AEROSPACE INDUSTRIES ASSOCIATION

# Safeguarding of Unclassified Controlled Technical Information (UCTI)

## Understanding and Complying with the Defense Federal Acquisition Regulation Supplement Clause 252.204-7012



**Cybersecurity attacks continue to increase in frequency and sophistication for the aerospace and defense industries. A new requirement of contracting with the Department includes a new information security clause: DFARS clause 252.204-7012 to safeguard Unclassified Controlled Technical Information (UCTI), effective November 13, 2013. The clause is required for all new DoD contracts and subcontracts and will affect companies of all sizes.**

## IN THIS PAPER, AIA HELPS YOU UNDERSTAND:

- **The new DFARS clause**
- **How to comply with Security and Incident Reporting Requirements**

### Two Main Compliance Components of DFARS 252.204–7012:

- DoD and its contractors and subcontractors must provide adequate security to safeguard DoD unclassified controlled technical information resident on or transiting through their unclassified information systems from unauthorized access and disclosure.
- Contractors must report to DoD certain cyber incidents that affect the protected information.

### What is the definition of Unclassified Controlled Technical Information (UCTI)?

Controlled technical information is defined as technical data or computer software (as defined in DFARS 252.227-7013) with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. The clause further specifies that 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 at http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf

### Meeting the Adequate Security Requirement

To provide adequate security, the contractor must implement information security that, at a minimum, includes the 51 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security controls defined in the clause.

Contractors that don't have all of the NIST controls implemented must submit a written explanation of how 1) the required security control(s) is not applicable, or 2) an alternative control or protective measure is used to achieve equivalent protection. This means all 51 controls must be addressed, either through implementation or documented explanation of non-applicability.

## HOW TO REPORT CYBER INCIDENTS

A cyber incident is defined as any action taken through the use of computer networks that results in an actual or potentially adverse effect on an information system and/or the information residing therein. As much of the following information from an incident must be reported to DoD within 72 hours of detection:

- DUNS number for location
- Contract numbers affected and clearance level
- Facility CAGE code
- Company point of contact
- Contracting officer point of contact
- Name of subcontractors affected and their CAGE codes (if at the subcontractor level)
- DoD programs, platforms, or systems involved
- Location(s), date, and type of compromise
- Description of the technical information compromised

## TO SUPPORT A POST-INCIDENT DAMAGE ASSESSMENT, CONTRACTORS MUST:

- Conduct a further review of the unclassified network for evidence of a cyber incident;
- Review the data accessed during the incident to identify specific UCTI associated with DoD programs, systems, or contracts;
- Preserve and protect images of affected information systems and all relevant monitoring/packet capture data for at least 90 days from the cyber incident.

When an incident is reported, the contracting officer will consult with a security manager from the DoD customer organization prior to assessing contractor compliance. Just because there is an incident does not necessarily mean the CO will find the contractor failed to comply with the rule if the contractor has met the requirements of the safeguarding portion of the clause.

## WHAT TO DO NOW

**All DoD contractors must rethink the way they view IT security and follow the steps shown below to comply with the requirements of this clause.**

**1. Determine if you have, or expect to win, any DoD contracts that contain this clause**

**2. If yes, determine if there is – or will be – any UCTI residing on or transiting through your IT system**

**3. If there is UCTI, determine if the IT system security complies with the NIST standards per the clause**

**4. If the compliance standards are not met, modify IT security to be in compliance with the NIST standards**

**5. Develop a protocol for documenting responses to any cyber incidents**

**6. Determine the policies and procedures necessary for continuous maintenance and periodic review of compliance**

AEROSPACE INDUSTRIES ASSOCIATION

1000 Wilson Boulevard, Suite 1700
Arlington, Va 22209-3928
703.358.1000
www.aia-aerospace.org