Safeguarding unclassified controlled technical information (UCTI)

An overview

Government Contract Services Bulletin
In June 2011, the DoD proposed to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to add a new subpart and associated contract clauses addressing requirements for safeguarding unclassified DoD information. In November 2013, the rule was finalized and, effective immediately, clause 252.204–7012, *Safeguarding of UCTI*, was mandated to be included in all new solicitations and contracts, including those for commercial items.

**Primary requirements 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 UCTI?**

Controlled technical information has a military or space application or falls under the definition of research and engineering data or engineering drawings, including associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog items, identifications, data sets, studies/analyses and related information, and computer software executable code and source code. The DoD is expected to mark UCTI items requiring protection; however, it is unclear at this time how the requirements for marked data will be defined and applied.
Security and safeguarding

To be compliant with DFARS 252.204-7012, contractors must establish reporting and accountability requirements and flow UCTI requirements to subcontractors. Contractors must also maintain knowledge of the company’s and subcontractors’ current state of compliance, including gaps to the required controls and documented mitigating controls. Finally, contractors must actively monitor all systems that store, manipulate or transmit UCTI for cyber events. The 51 minimum required security controls for UCTI requiring safeguard are specified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.

Cyber incident reporting

In addition to security controls and safeguard requirements, contractors are required to report all cyber “incidents.” DFARS 252.204-7012 defines the information required to be reported and requires that contractors maintain incident evidence for at least 90 days from the date of the cyber incident to support the DoD in the event it conducts a damage assessment.

- Incident reporting is required within 72 hours of discovery of a cyber incident that affects DoD UCTI.

- It includes exfiltration, manipulation, or other loss or compromise of UCTI resident on or transiting through a contractor’s, or its subcontractors’, unclassified information systems.

- Any other activities that allow unauthorized access to the contractor’s unclassified information system on which UCTI is resident on or transiting also apply.

- Contractors found to be noncompliant with DFARS 252.204-7012 may be removed from information technology procurements supporting national security systems and in some cases may be unable to protest their removal.

Compliance challenges

With the expansion of cybersecurity regulations for contractors comes new and compounded compliance challenges, including:

- Interpreting the definition of UCTI and marked data
- Identifying systems considered to be in-scope
- Overseeing and monitoring of subcontractor compliance
- Meeting incident reporting deadlines
UCTI compliance framework considerations

A framework is imperative to help establish and maintain compliance with the DFARS UCTI requirements. The steps below should be considered when developing your framework.

Identify
- Identify confidential information assets and key systems where UCTI resides
- Evaluate security control effectiveness over systems that store, process and transmit UCTI
- Identify regulatory and disclosure requirements
- Identify threat groups, vulnerabilities and evidence to be analyzed
- Evaluate subcontractor risk and required processes

Protect
- Design and implement compliant security controls
- Review cyber-monitoring processes for adequacy
- Review logs to detect access to sensitive information and filter suspicious events
- Remediate third-party contracting processes
- Document and communicate the rationale for excluding any required NIST controls

Detect
- Develop a communications plan for reporting incidents to a contracting officer
- Examine and preserve key log data for hostile activity
- Identify suspicious events and incidents that may have occurred and that may be required to be reported within a 72-hour period
- Evaluate the current data preservation plan for compliance with evidence maintenance criteria

Respond
- Forensically preserve and maintain incident evidence for the required 90 days
- Respond to Defense Contract Audit Agency (DCAA) and contracting officer inquiries and audit results

Recover
- Restore any capabilities or services that were impaired due to a cybersecurity event
- Identify control improvements and develop remediation plans
- Update Government contracting processes to address compliance with key regulations
- Flow provisions to subcontracts and monitor subcontractor compliance and reporting

Monitor
- Establish a plan for ongoing monitoring of DFARS 252.204-7012 UCTI requirements
- Periodically assess related controls and complete corrective action plans for identified deficiencies and control exceptions
About EY's UCTI response team

The combination of distinct skills and integration across EY allows us to offer a seamless end-to-end approach to maintain compliance with government contracting challenges including UCTI regulations.

Ernst & Young LLP
Government Contract Services (GCS)

Our team of experienced professionals has both the depth of knowledge and breadth of experience in applying the procurement rules and regulations of Government agencies.

Contacts:
Robert Malyska
Partner
Government Contract Services Leader
+1 214 969 8628
robert.malyska@ey.com

Todd LaMastres
Partner
+1 214 969 8484
todd.lamastres@ey.com

Deborah Nixon
Partner
+1 703 747 1478
deborah.nixon@ey.com

Darl Rhoades
Executive Director
+1 720 931 4022
darl.rhoades@ey.com

Frank Summers, Jr.
Executive Director
+1 617 375 1285
frank.summersjr@ey.com

Steven Tremblay
Executive Director
+1 617 375 2420
steven.tremblay@ey.com

Ernst & Young LLP
Fraud Investigation and Dispute Services (FIDS)

Our FIDS team has the capabilities to perform incident investigations, collect and preserve evidence, manage the reporting of an incident to the DoD, and manage the continued preservation and maintenance of evidence for the required 90 days.

Contacts:
David Remnitz
Partner
Global & Americas Forensic Technology & Discovery Services Leader
+1 212 773 1311
david.remnitz@ey.com

Kenneth Feinstein
Senior Manager
+1 203 674 3177
kenneth.feinstein@ey.com

Ken Zatyko
Senior Manager
+1 202 327 7185
ken.zatyko@ey.com

Kelly Volz
Senior Manager
+1 202 327 5684
kelly.volz@ey.com

Ernst & Young LLP
Information Technology Risk Assurance (ITRA)

Our ITRA team can assist with the identification of systems where UCTI is stored, assessments against the 51 required controls, documentation of compliance with required controls, identification of gaps and mitigating controls, development of ongoing compliance processes, control remediation, reviews of cyber-monitoring processes for adequacy, post-incident lessons learned, and the design of necessary control improvements.

Contacts:
Mark Johnson
Principal
+1 703 517 3442
mark.johnson@ey.com

Michael Baker
Senior Manager
+1 703 747 0710
michael.baker@ey.com

Safeguarding UCTI An overview | 5
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2014 Ernst & Young LLP.
All Rights Reserved.

SCORE No. WW0339
CSG No. 1402-1206209
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com