# *Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011-D039):*

## *The Challenges of New DFARS Requirements and Recommendations for Compliance*

***Version 1***


## *Authors:*

**Justin Gercken, TSCP**
**E.K. Koh, NextLabs**
**Dennis Andrie, NextLabs**



## *Published:*

**January 23, 2015**


TSCP
Transglobal Secure Collaboration Participation

NEXTLABS®

# *Table of Contents*

# 1. Introduction

The Department of Defense (DoD) issued a final rule on November 18, 2013, to amend the Defense Federal Acquisition Regulation Supplement (DFARS) with the addition of Subpart 204.73[1], Safeguarding Unclassified Controlled Technical Information, and an associated contract clause, DFARS 252.204-7012[2]. The rule applies to all new DoD solicitations, contracts, and newly modified existing contracts which involve Unclassified Controlled Technical Information (UCTI) resident on, or transiting through, contractor unclassified information systems. The rule affects all DoD contractors and subcontractors, including vendors of commercial goods, as well as DoD personnel carrying out activities involved with the Federal Acquisition Regulation (FAR) system. The primary objectives of the rule are to 1) strengthen DoD's data security requirements for controls that govern access to UCTI on DoD contractor information systems, and 2) impose new reporting and damage assessment requirements in the event of cyber incidents which involve possible unauthorized access, disclosure, manipulation, or any loss or compromise of UCTI on contractor systems.

Controlled Technical Information (CTI) is technical information with military or space application that is subject to controls on its access and use. CTI does not include information lawfully available to the public. UCTI is information which is not classified under Executive Order 13526 or the Atomic Energy Act, but still requires safeguarding and controls due to its potential to threaten national security, adversely affect government function, and/or negatively impact the public were the information to be made available to the wrong parties.

For DoD contractors, both domestic and abroad, the new DFARS requirements may pose significant challenges, especially for smaller organizations that lack the resources to comply with the requirements in a sustainable and cost-effective manner. This paper provides a brief background of DFARS, outlines key requirements of the final rule addressing the safeguarding of UCTI, examines the resulting challenges for affected parties, provides a recommended set of best practices for achieving compliance, and discusses how the freely available Information Labeling and Handling Framework, produced by the Transglobal Secure Collaboration Program (TSCP), can help address data security requirements mandated by the new rule.

---

[1] To view DFARS 204.73 online, visit http://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm

[2] To view DFARS 252.204-7012 online, visit http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012

## 2. Background

The Federal Acquisition Regulation (FAR)[3] manages the process the U.S. government uses to acquire goods and services. The Defense Federal Acquisition Regulation Supplement (DFARS) provides further requirements and regulations specific to the Department of Defense (DoD) and DoD contracts. DFARS contains legal requirements, delegations of FAR authorities, deviations from FAR requirements, and DoD-wide policies. The DFARS both abides by and supplements the FAR, and is intended to be read in combination with the primary set of rules in the FAR. As DoD's primary mission is national security, DFARS is important because it includes policies and procedures that have the potential to significantly impact the public.

DoD published a proposed rule in the Federal Register on June 29, 2011, to increase the strength of security measures and access controls guarding unclassified DoD information within contractor information systems, and set forth reporting requirements in the event of certain cyber intrusion incidents that may affect unclassified DoD information within these systems. The proposed rule was made open to comment, and after comments were received, the decision was made to reduce the scope of information covered under the proposed rule to only UCTI. The rule was finalized in November 2013 and became effective immediately.

## 3. Key Requirements for Contractors

The contract clause, DFARS 252.204-7012, introduces a number of key requirements that significantly affect DoD contractors:

1) The clause must be included on all new DoD contracts and includes a mandatory flow down the supply chain to all tiers of subcontractors.

2) The clause requires contractors to "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." At minimum, a contractor must implement NIST system security controls across 14 control vectors as described in NIST SP 800-53[4]. A contractor may present an option equivalent to NIST standards, or explain why the standards aren't applicable to the specific contract, but any deviation from this requirement necessitates approval from the contracting officer.

[3] For more information, visit the FAR website at http://www.acquisition.gov/far/

[4] To view NIST SP 800-53 online, visit http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

3) The clause also requires adherence to DoD Instruction 5230.24[5], which discusses distribution statements on technical documents. Distribution statements denote the scope of authorized distribution for a document. According to Instruction 5230.24, all UCTI governed by a DoD contract must be marked with one of the distribution statements from B through F, seen in Figure 1 below. Additionally, these distribution statements may be determined by DoD as part of a contract.

| |
|---|
| DISTRIBUTION A. Approved for public release: distribution unlimited. |
| DISTRIBUTION B. Distribution authorized to U.S. Government agencies (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office). |
| DISTRIBUTION C. Distribution authorized to U.S. Government agencies and their contractors (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office). |
| DISTRIBUTION D. Distribution authorized to Department of Defense and U.S. DoD contractors only (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office). |
| DISTRIBUTION E. Distribution authorized to DoD Components only (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office). |
| DISTRIBUTION F. Further dissemination only as directed by (controlling office) (date of determination) or higher DoD authority. |

**Figure 1. Distribution statements defined by DoD Instruction 5320.24.**

4) In the event of certain cyber incidents, the clause requires contractors to communicate specific information relating to the incident, or as much of said information that can be obtained by the contractor, within 72 hours. A reportable incident includes any incident involving possible exfiltration, manipulation, or any loss, compromise, or unauthorized access to UCTI within a contractor system.

5) If a cyber incident is reported, the clause stipulates that a contractor must conduct a damage assessment requiring the contractor to review its unclassified network for evidence of compromise and identify all compromised elements. The contractor must also review all data accessed to identify UCTI associated with DoD programs, systems, or contracts. Furthermore, the contractor is required to preserve and protect images of known affected systems and all relevant monitoring/packet capture data for at least 90 days from the event of a cyber incident. DoD may also choose to conduct its own damage assessment, in which case the contractor must comply with DoD information requests, provided no other legal restrictions govern the contractor's ability to share media.

6) Additionally, contractors may be subject to penalties for violations of DFARS requirements. These penalties are governed by the individual DoD contracts.

[5] To view DoD instruction 5230.24, visit http://www.dtic.mil/dtic/pdf/customer/STINFOdata/DoDD_523024.pdf

# *4. Challenges for Contractors*

The effort to maintain compliance with new DFARS requirements presents a number of challenges for DoD contractors. Contractors must ensure their technological infrastructure meets new standards, as well as address their business processes to ensure compliance.[6]

## 4.1. Technology Challenges

DoD contractors face the following technology challenges:

1) Contractors must identify all of their systems that potentially house or process UCTI.

2) Contractors must develop and implement system security controls for the applicable systems across 14 control vectors, depicted in table 1 below, as described in NIST SP 800-53. Note that not all of the controls in Table 1 are applicable[7] and alternative controls can be provided.

**Table 1. Security control identifiers and family names**

| ID | FAMILY | ID | FAMILY |
|---|---|---|---|
| AC | Access Control | MP | Media Protection |
| AT | Awareness and Training | PE | Physical and Environmental Protection |
| AU | Audit and Accountability | PL | Planning |
| CA | Security Assessment and Authorization | PS | Personnel Security |
| CM | Configuration Management | RA | Risk Assessment |
| CP | Contingency Planning | SA | System and Services Acquisition |
| IA | Identification and Authentication | SC | System and Communications Protection |
| IR | Incident Response | SI | System and Information Integrity |
| MA | Maintenance | PM | Program Management |

3) System controls alone are insufficient to remain compliant with DFARS, and contractors require data controls to ensure the proper classification of data, proper protection of data access and use, and to provide sufficient logging of data use. Figure 2 below lists data controls that address these requirements.

[6] Additionally, contractors have expressed difficulty with interpreting DFARS requirements. Primarily, due to the vast and varied amounts of data in complex systems, there is a need for further clarification regarding what types of data specifically constitute UCTI in order for contractors to correctly begin implementing solutions for DFARS requirements.

[7] CA, PL, PS, SA are not mandated in DFARS 252.204-7012.


**Figure 2. Data level controls.**

4) Contractors need to develop automation that turns the application of solutions for DFARS compliance into efficiently repeatable, cost-effective processes. For example, to meet the 72 hour incident report timeline, as well as the damage assessment requirements, an automated process would be necessary to continuously capture all information that would be required by DoD in the event of a cyber incident.

## 4.2. Business Process Challenges

In addition to technology challenges, contractors are also faced with a number of key business process challenges which must be addressed in order to comply with new DFARS requirements:

1) Contractors must develop new strategies and corporate policies in a timely manner in order to govern, and remain compliant with, DFARS requirements.

2) Contractors must develop a process to ensure that all newly created UCTI involved with a contract is identified, and appropriately labeled and controlled, as early as possible in its lifecycle.

3) Contractors must also develop a process to properly identify and implement DFARS requirements for all legacy UCTI involved with new contracts or newly modified, existing contracts within their systems.

4) Contractors face the task of training legal, compliance, engineering, operations, and IT departments in a complete set of new DFARS compliance processes.

5) Contractors also face the challenge of vetting and/or managing all subcontractors in the supply chain to ensure they are compliant with DFARS.

# 5. Best Practices

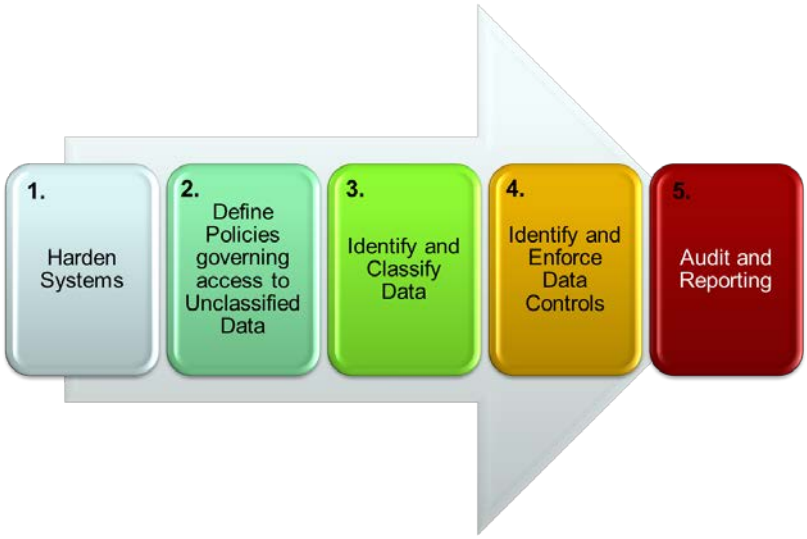


**Figure 3. Flow of recommended best practices.**

The authors of this paper recommend that DoD contracting organizations perform the following practices in the order outlined in Figure 3 above to meet DFARS compliance.

**1) Harden Systems** – Contractors should first implement system security controls and strengthen their systems' security. To implement system controls that are compliant with DFARS, contractors must ensure the appropriate system controls, specified in NIST SP 800-53, are implemented on all of their systems that store or transit UCTI.[8]

**2) Define Policies** – Once contractors have hardened their systems, DFARS compliant policies should be developed to govern access to UCTI. In order to define polices that will govern access to this data, contractors should implement corporate policies and training programs to govern the DFARS process. To enable policies which are practical in use, contractors should develop policies that are systemic rather than manual. The policies should also be enforceable across multiple systems.

**3) Classify Data** – Next, the authors recommend contractors develop policies to identify where their UCTI resides, and what classifications will be applied to what types of data. In order for contractors to properly classify data according to DFARS, they must develop detailed knowledge about the UCTI that must be protected.

[8] To view the best practices for implementing NIST SP 800-53, visit http://csrc.nist.gov/publications/drafts/800-171/sp800_171_draft.pdf.

**4) Enforce Controls** – Once UCTI is identified, contractors must put system and data controls in place across all of their systems where UCTI may reside to govern the access and use of UCTI to ensure only authorized users may access and download data.

**5) Automated Tracking** – In order to remain compliant with DFARS requirements mandating contractors to provide access logs within 72 hours of a cyber incident, contractors should implement automated log collection to record all access to UCTI on their systems. To meet damage assessment requirements, contractors should also implement automated log collection to support a forensic analysis that can quickly assess the extent of potential damage following a cyber incident.

# *6. The TSCP Information Labeling and Handling Framework*

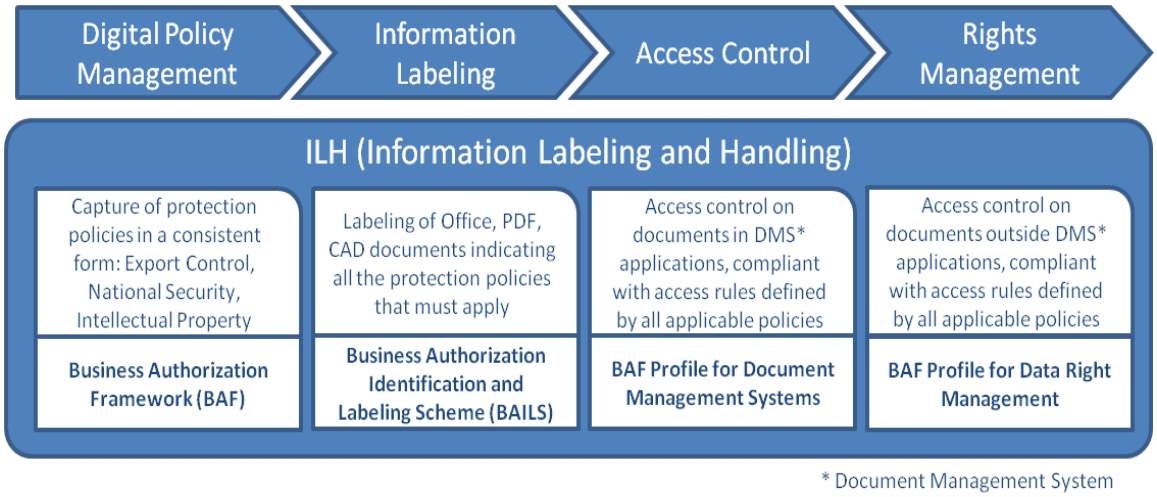


**Figure 4. The TSCP Information Labeling and Handling Framework**

The TSCP Information Labeling and Handling (ILH) Framework is comprised of freely available specifications and guidance documents which provide a methodology to use commercial off-the-shelf products to define policies, classify data, enforce controls, and track access. Of the recommended best practices for DFARS compliance in this paper, ILH provides a framework to consistently identify and mark data across multiple contracting organizations, as well as enforce consistent access control rules. The ILH framework can flow down from prime contractors to subcontractors to ensure consistent policy-based access control to data as it transitions through the supply chain. ILH supports many of the stated controls explicitly required by new DFARS requirements, such as those under AC-Access Control and IA-Identification and Authentication (as mentioned in Section 4.1).

More specifically, the ILH Framework is comprised of two specifications: 1) The Business Authorization Framework (BAF) and 2) The Business Authorization Identification and Labeling Scheme (BAILS).

TSCP's Business Authorization Framework (BAF)[9] specification provides a framework to consistently manage policies governing access to data using an expression of policy requirements that are specifically targeted for automated system processing.

TSCP's Business Authorization Identification and Labeling Scheme (BAILS)[10] provides organizations with a specification of metadata elements that can be applied to an information object, or piece of data, enabling the automation of identifying the protection policies applicable to each piece of data, as well as enabling applications to produce visual markings on the data in accordance with its identified policy. BAILS can be used to identify specific types of data in a contractor's system, as well as to label data with the appropriate distribution statement.

## 6.1. Additional Information on ILH

Recommended Viewing:

To view an online demonstration of how ILH works, visit:

https://www.tscp.org/wp-content/uploads/2013/11/secure_collaboration_proof_of_concept_demo.mp4

Recommended Reading:

To read the ILH white paper, Secure Global Collaboration with Information Labeling and Handling, visit:

https://www.tscp.org/wp-content/uploads/2013/08/tscp_wp_ilh_02272012.pdf

[9] BAF is available online at https://www.tscp.org/wp-content/uploads/2013/08/TSCP_BAFv1.pdf

[10] BAILS is available online at https://www.tscp.org/wp-content/uploads/2013/08/TSCP_BAILSv1.pdf

# *7. Conclusion*

The final rule on safeguarding UCTI imposes challenging requirements for DoD contractors. TSCP's freely available ILH Framework provides solutions for a number of the challenges presented by new DoD requirements, and a means of executing many of the best practices recommended in this paper. Following these recommended practices and implementing the ILH Framework can greatly aid DoD contracting organizations in overcoming DFARS challenges, thus freeing organizations to focus on delivering customer value, while ensuring DFARS compliance.