Dynetics, Inc.

DFARS Compliance - a Moving Target

Whitepaper

Technical POC

Greg Jackson

Phone: 256.964.4692

greg.jackson@dynetics.com

The Department of Defense (DoD) released interim rules on Aug. 26, 2015, that significantly impact the implementation of provisions of the 2013 and 2015 National Defense Authorization Acts.

1 BACKGROUND

The Defense Federal Acquisition Regulation Supplement 252.204-7012, commonly known as DFARS, was amended in November 2013 to implement adequate security measures to safeguard unclassified DoD controlled technical information within contractor information systems. Additionally, it prescribed reporting to DoD certain cyber intrusion events that affect DoD information resident on, or transiting through, contractor unclassified information systems. Each contractor must implement information systems security in its project, enterprise, or company-wide unclassified information technology systems that have access to unclassified controlled technical information. As a result of the 26 August release, the following rules are effective immediately and establish the following:

- Information system security requirements
- Mandatory cyber incident reporting
- Cloud computing standards and procedures

2 INFORMATION SYSTEM SECURITY REQUIREMENTS

Contractor information systems that support a covered DoD contract must meet the standards contained in National Institute of Standards and Technology (NIST) Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

3 MANDATORY CYBER INCIDENT REPORTING

As previously required, contractors must report any cyber incidents within 72 hours of discovery and must conduct an investigation to gather evidence of the scope of the incursion. However, a cyber incident now covers circumstances that affect the contractor's ability to perform the requirements of a contract that is designated as operationally critical support. Additionally, reporting now requires contractors to have or acquire a "DoD-approved medium assurance certificate" for reporting cyber incidents. In addition, they must do the following:

- Submit to DoD any malicious software they are able to isolate
- Preserve and protect images of all known affected information systems and relevant monitoring/packet capture data for at least 90 days from the submission of the incident report
- Permit DoD access in order to perform its own forensic investigation or damage analysis

Although DoD commits to protect against unauthorized use or release of contractor incident report information, it warns contractors to remove, to the extent possible, attributional/proprietary information from the reports. The new regulation authorizes DoD to share information concerning the breach that is not created by or for DoD with the following groups:

- Entities whose missions may be affected by the information
- Organizations assisting with diagnosis, detection, or mitigation of the incident
- Counterintelligence or law enforcement personnel

- Entities with national security purposes, including the Defense Industrial Base participants
- Support services contractors with appropriate protections

Prime contractors must flow down the cyber protection and reporting clause to their subcontractors. Subcontractors are required to submit cyber incident reports to both their prime contractor and DoD, and lower-tier subcontractors must submit them to their upper-tier subcontractors until they reach DoD.

4 CLOUD COMPUTING STANDARDS AND PROCEDURES

Cloud computing is now addressed in the new release and requires contractors to meet the security requirements specified in the clause 252.239-7010. In this clause, the contractor must declare their intent to use cloud computing. If the contractor indicates that it will not use cloud computing, but later decides to make use of cloud services, the contractor must obtain the contracting officer's approval prior to utilizing such services on the contract.

Contractor cloud computing safeguards and controls must meet those set forth in the Cloud Computing Security Requirements Guide. Unless the government grants an exception, all government data that is not physically located on DoD premises must be maintained within the United States or outlying areas. In addition, contractors must report cloud computing security breaches in accordance with the breach notification and protocols described above.

5 TOP 10 INDICATORS OF COMPLIANCE:

1. The organization performs regularly scheduled vulnerability scans of information systems and hosted applications.
2. The organization implements an organization-wide risk management process, a risk management framework, and associated security standards and guidelines.
3. The organization maintains strict access control over information systems through documented policies and procedures.
4. The organization provides security awareness training to information system users as part of initial training, when required by information system changes, and periodically thereafter.
5. The organization actively monitors, audits, reviews, analyzes, and reports on a minimum of 6 specific information system events, generates audit records, and protects audit information.
6. The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.
7. The organization protects the confidentiality, integrity, and availability of and conducts backups of user-level information, system-level information, and information system documentation including security-related documentation.
8. The information system uniquely identifies and authenticates organizational users, manages information system identifiers and authenticators.
9. The organization provides incident response training to information system users that is consistent with assigned roles and responsibilities and follows organizationally documented policies and procedures.
10. The organization physically controls, protects, and securely stores media within controlled areas until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

In light of all the changes impacting contractors who process (collect, develop, receive, transmit, use, or store) defense information, it may be necessary to segment your network. Network segmentation that's designed to isolate defense information from the rest of your enterprise will not only reduce the attack vector to that information but it will also enable you to limit your scope for meeting the new security requirements.

Dynetics is available to assist with any number of implementation strategies going forward. With over 15 years of experience supporting compliance efforts for organizations of all sizes, Dynetics can provide gap assessments, policy and procedure development, IT solutions, and continuous monitoring.