AERSTONE

DFARS ASSESSMENT

Presented by: Jason Winder, Frank Schugar

An Aerstone™ White Paper

I. Executive Summary

The Department of Defense recently added a new clause to the Defense Federal Acquisition Regulation Supplement (DFARS). This clause, "Safeguarding Covered Defense Information and Cyber Incident Reporting" (Section 252.204-7012), requires all DoD prime contractors and subcontractors to implement "adequate security" based on a set of security controls referenced in NIST SP 800-171, and to conduct cyber incident analysis and reporting. The seventy-nine (79) security controls identified in this publication map back to a down-selected set of controls defined in NIST SP 800-53. As such, achieving DFARS compliance may be viewed as a slightly simplified FISMA accreditation process, against the FIPS-199 moderate baseline. The wording of the clause is sufficiently broad as to require compliance by virtually any company doing business with the DoD, no later than **31 December 2017**.

II. About DFARS

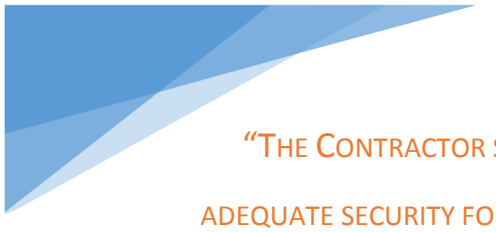
The **Federal Acquisition Regulation**, or "FAR" for short, is a set of rules jointly issued by the GSA, NASA, and the DoD, and followed by the executive branch of the federal government, in acquiring goods and services. It applies to all acquisitions, from the very low-tech (like grounds keeping or food service) to the highest of high-tech (like building stealth aircraft and missiles). The FAR, which is documented in Title 48, Chapter 1 of the Code of Federal Regulations, covers the entire life-cycle of a contract, starting with need recognition and acquisition planning, through contract formation and administration, and ultimately contract close-out. FAR clauses are explicitly included in federal contracts. There are a few federal agencies (like the FAA and the US Mint) that are exempt from the FAR – however they are the exception and not the rule.

Although the FAR was designed to be as comprehensive as possible, many government agencies have developed their own supplements to the FAR. The **Defense Federal Acquisition Regulation Supplement**, or "DFARS" for short, is the set of supplemental guidance to the FAR specific to the DoD, and which applies to companies doing business with the US military and intelligence community. The DFARS is addressed in Title 48, Chapter 1 of the Code of Federal Regulations, and provides specific guidance to government contracting officers for creating and managing military contracts.

III. DFARS 252.204-7012

DFARS Section 252.204-7012, as revised in December 2015, is a relatively new DFARS clause titled "Safeguarding Covered Defense Information and Cyber Incident Reporting." This clause requires all DoD contractors (including their subcontractors) to comply with two core information security requirements:

1. Adequate Security
2. Incident Reporting



> "THE CONTRACTOR SHALL PROVIDE ADEQUATE SECURITY FOR ALL COVERED DEFENSE INFORMATION ON ALL COVERED CONTRACTOR INFORMATION SYSTEMS THAT SUPPORT THE PERFORMANCE OF WORK UNDER THIS CONTRACT."
>
> DFARS 252.204-7012

Adequate Security

The "adequate security" clause is designed to ensure that sensitive government information is properly protected, with an appropriate set of security controls. This requirement applies broadly to any "covered contractor information systems," which includes any network owned or operated by or for the contractor. This could be a company LAN/WAN, or a third party network like Microsoft Azure or AWS.

What's Covered

The scope of this requirement is limited to systems that store "Covered Defense Information," which includes any information related to "the performance of the contract" that the DoD provides to the contractor (like NDAs or contract paperwork), or which the contractor accumulates in support of the contract (e.g., research, deliverables, schedules, resumes, and billing or financial information). This is a massive requirement on its face, and makes a dramatic impact on the number of systems that must be considered in-scope of an assessment.

In general, however, information must fall into one of **four specific categories** in order to be covered by this regulation:

1. Controlled Technical Information, which is defined as "technical information [i.e., technical data or computer software] with military or space application that is subject to controls." This can a wide array of artifacts, such as engineering drawings, manuals, technical reports, data sets, and computer software executables and source code.
2. OpSec information about intentions, capabilities, and activities that an adversary could use to "guarantee failure or unacceptable consequences." This could include things like employee names, work schedules, work locations, and any other information that might affect operational security.
3. Export-controlled information, such as "dual-use" technologies like nuclear or biochemical information.
4. Any additional information specifically identified in the contract.

How to Comply

In order to achieve the standard of adequate security, the contractor is obligated to implement "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information." However, in the achievement of this standard, the regulation further instructs contractors to follow the security guidance specified in **NIST Special Publication 800-171**, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organization," no later than later than **31 December 2017**.

"THE SECURITY REQUIREMENTS [...] IN EFFECT AT THE TIME THE SOLICITATION IS ISSUED OR AS AUTHORIZED BY THE CONTRACTING OFFICER, AS SOON AS PRACTICAL, BUT NOT LATER THAN DECEMBER 31, 2017."

DFARS 252.204-7012

The regulation does provide some room for alternative approaches, other than rigorously following NIST 800-171. Contractors may solicit written approval for "alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement" from the DoD CIO, and contractors may

supplement the controls described in NIST 800-171 with additional controls that they deem prudent. However contractors are also obligated to notify the DoD (osd.dibcsia@mail.mil) of any deficiencies against NIST 800-171 within thirty (30) days of contract award.

Incident Reporting

Incident reporting under this clause is triggered by the discovery of a "cyber incident," which is defined very broadly as a network compromise, an "adverse effect," or even just a "potentially adverse effect," on either the network, the covered contract information (per above), or the ability to execute against "operationally critical" contract requirements. The latter are defined as those activities considered "essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation."

In practice, this means that contractors aren't merely required to disclose network intrusions, but also *attempted* intrusions, regardless of whether systems or data were actually compromised. This is a very low bar, and implies a requirement for intrusion monitoring.

Upon discovery of a cyber incident, the contractor is required to do the following things:

1. Report the incident to the DoD within 72 hours of discovery, through http://dibnet.dod.mil, as well as to the prime contractor (if applicable) "as soon as practicable."
2. Conduct an investigation to determine whether any covered information was compromised. This includes a review of not just systems that are specifically in scope of this regulation (i.e., systems containing covered information), but also any other systems that were attacked or compromised and which either: (a) might help an attacker identify covered information; or (b) could affect the contractor's ability to provide operationally critical support (as defined above).
3. Preserve an image of all affected systems, plus all relevant logging data, for at least 90 days from the submission of the incident report. The DoD may request this information.
4. Submit to the DoD any malware discovered and isolated, per instructions provided by the Contracting Officer.

Note that contractors should proactively acquire a DoD-approved medium assurance certificate, to facilitate the reporting of cyber incidents per above. See the link to DISA's ECA program under References below, for instructions on how to acquire a certificate.

IV. NIST Guidance

About NIST

The National Institute of Standards and Technology (NIST) is the Federal Government's standards laboratory, managed under the U.S. Department of Commerce. NIST publishes standards, guidelines, recommendations and research on computer/cyber/information security and privacy, via several series of technical publications, including:

- Federal Information Processing Standards (FIPS) security standards;
- Special Publications (SPs), including security and privacy guidelines, recommendations, and reference materials;
- NIST Interagency or Internal Reports (NISTIRs), which are reports of research findings and background information for FIPS and SPs; and
- Information Technology Laboratory (ITL) Bulletins, which are monthly overviews of NIST's security and privacy publications, programs and projects.

NIST SP 800-171

NIST Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," is a set of guidelines for protecting Controlled Unclassified Information (CUI) on information systems outside the immediate control of the federal government. These guidelines provide federal agencies with recommended requirements to protect the confidentiality of CUI residing in nonfederal systems and organizations consistent with law, regulation or government-wide policy. The requirements apply to all components of nonfederal information systems and organizations that process, store or transmit CUI, or provide security protection for those components.

The guidelines presented in NIST SP 800-171 are a subset of guidance from other NIST publications, notably FIPS 200 ("Minimum Security Requirements for Federal Information and Information Systems") and NIST SP 800-53 ("Security and Privacy Controls for Federal Information Systems and Organizations"). These latter documents are used by the government to ensure security posture of both classified and unclassified systems, as required by the Federal Information Security Modernization Act (FISMA). The down-selected set of controls that were chosen for NIST SP 800-171 are based on the assumption of a "moderate" impact due to loss of confidentiality, as defined in FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems." Other controls were also eliminated for a variety of reasons, including lack of applicability outside the federal government, or an expectation that certain controls would be "routinely satisfied" by commercial entities.

Achieving Compliance

For ease of use, the security requirements defined in NIST SP 800-171 are organized into fourteen "families" of control. Within each family, a series of **Basic Security Requirements** (from FIPS 200) and **Derived Security Requirements** (from NIST SP 800-53) are defined. The Basic Security Requirements may be thought of as security "goals," which are achieved by the implementation of the Derived Security Requirements, which are testable security controls.

The 14 security control families, with a tally of the number of requirements in each family, are listed in Table 1. NIST SP 800-171 also includes a control mapping table in Appendix D, which defines how the 79 derived security controls map back to their source controls in NIST SP 800-53. In this way, achieving DFARS Section 252.204-7012 compliance is very similar to conducting a scaled-down FISMA assessment, against the moderate baseline of NIST SP 800-53 controls.

NIST SP 800-171		
Control Family	**Basic Requirements**	**Derived Requirements**
1. Access Control	2	20
2. Awareness and Training	2	1
3. Audit and Accountability	2	7
4. Configuration Management	2	7
5. Identification and Authentication	2	9
6. Incident Response	2	1
7. Maintenance	2	4
8. Media Protection	3	6
9. Personnel Security	2	0
10. Physical Protection	2	4
11. Risk Assessment	1	2
12. Security Assessment	3	0
13. System and Communications Protection	2	14
14. System and Information Integrity	3	4
Total:	**30**	**79**

Table 1 -- NIST 800-171 Security Requirement Families

VI. Lessons Learned

Experience has shown that there are a few relatively simple steps that defense contractors (and their subcontractors) can take to efficiently deal with the requirements levied on them by the new DFARS guidance:

Third party confirmation is better than doing it yourself

Auditors understandably prefer assessment results produced by someone *other* than the system owners and implementers.

Style is just as important to the auditors as substance

Although perhaps somewhat trite, repeat experience has confirmed this without room for doubt or compromise. Defense auditors dramatically prefer “paperwork” (security assessment reports, control documentation, and penetration testing reports) that looks and feels familiar. How information is presented is just as important as the information itself.

Perfection isn't the required standard

Most systems have failed controls, particularly in their first assessments or audits. This isn't a problem. Correctly documenting any failures, and showing the intent to mitigate in a plan of actions and milestones (POA&Ms) will cover most sins – at least long enough to resolve any real issues.

Moving into the cloud both helps and hurts

By moving systems into the cloud, defense contractors can inherit many security controls provided by the cloud service provider (CSP). That said, ensuring proper documentation of the CSP provided controls *and* the controls provided by the entity itself is challenging.

Most real problems come from poor configuration management

Regardless of the access control family, most problems have configuration management issues at their root. This includes issues like build control, patching, and change management. After the system security plan, the next most important document is the configuration management plan.

Don't try to be clever!

While there are always work-around options, these paths will invariably prove more cumbersome and time-consuming than implementing the controls as envisioned and intended. The audit exception process exists for a series of good reasons, but it is never the preferred route to compliance.

VII. For More Information

Contact dfars@aerstone.com to schedule a free DFARS compliance consultation – or visit us on the web at www.aerstone.com.

VIII. References

1. Federal Acquisition Regulation (FAR)
   https://www.acquisition.gov/?q=browsefar
2. Defense Federal Acquisition Regulation Supplement (DFARS)
   http://www.acq.osd.mil/dpap/dars/dfarspgi/current
3. DFARS 252.204-7012
   http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012
4. DoD-DIB Cyber Incident Reporting & Cyber Threat Information Sharing Portal
   http://dibnet.dod.mil
5. NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organization"
   http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf
6. FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems"
   http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
7. FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems"
   http://www.nist.gov/customcf/get_pdf.cfm?pub_id=50835
8. NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations"
   http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
9. DISA IASE External Certification Authority Program (ECA)
   http://iase.disa.mil/pki/eca/Pages/index.aspx
10. Federal Information Security Modernization Act (FISMA)
    https://www.congress.gov/bill/113th-congress/senate-bill/2521/text