DFARS 252.204.7012 Safeguarding Covered Defense Information
The Interim Rule: Cause for Confusion and Request for Questions

By Jonathan Hard, CEO
And Carol Claflin, Director of Business Development

H2L Solutions, Inc.
2227 Drake Ave, Building 3 Suite C
Huntsville, AL 35805

Executive Summary
On August 26th 2015, the DoD issued an interim ruling which revises DFARS 252.204.7012. At the same time, three new clauses were released and referred to within 252.204.7012: DFARS 252.204.7008, 252.204.7009, 252.204.2010 and 239.76 for cloud computing services. The original text can be read here: http://www.gpo.gov/fdsys/pkg/FR-2015-08-26/pdf/2015-20870.pdf. This interim rule is effective immediately, and indeed we are seeing it in solicitations, especially out of Missile Defense Agency (MDA). There has been much discussion, confusion and even alarm in the DoD contracting community in response to the changes and additions, especially as we move into proposal season.

H2L Solutions has taken the time to break down the changes and revisions to clarify them when possible. We also attended UAH’s Cybersecurity Summit on Thursday, September 24, 2015 where David S. Lane, Assistant Director Ballistic Missile Defense System (BMDS) Acquisition System Protection, and Major Clark, Assistant Chief Counsel, Office for Advocacy, Small Business Administration, led a session on business issues. We went hoping to hear the government’s perspective on the interim rule, and how it should be responded to in solicitations. Our purpose in this paper is to provide some clarity to the interim rulings, relay the information gathered at the Cybersecurity Summit, describe the trends in the marketplace, and gather and encourage questions.

Basic Differences

What is protected:
DFAR 252.204.7012 is now called “Safeguarding Covered Defense Information and Cyber Incident Reporting.” The government has greatly expanded the scope of the regulation to cover company information in addition to DoD information. Contractors are now required to protect any DoD information provided to the contractor or collected, developed, received, transmitted, used,
or stored by or on behalf of the contractor in support of performance of a government contract and that falls into one of the following categories:

1) Controlled Technical Information.
2) Critical Information: specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities that are needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.
3) Export Controlled Information.
4) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies (e.g., privacy, proprietary business information).
5) Included now are contracts for commercial goods.

**How it is protected:**

In June 2015 U.S. Department of Commerce released National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. The interim rules call this publication out. While this may seem confusing, the NIST 800-171 calls out controls directly from NIST SP 800-53. In order to simplify the changes, we have included the old and new controls in a chart below. As you can see, there are approximately 30 new controls that contractors are responsible for.

*H2L* finds it interesting that an entirely new family of controls has been added: Security Assessment and Authorization. CA controls listed in NIST SP 800-171 ask that the contractor conduct a Security Assessment, create and track a Plan of Action and Milestones (POAM), and create a continuous monitoring program. Compliance now requires that contractors demonstrate that they have a security plan in place that is comprehensive and being monitored.

There are also additional Risk Assessment and Awareness Training requirements. RA 3 requires the company to provide documentation that shows it has conducted a risk assessment on the unauthorized access, use, disclosure, disruption, modification, or destruction of the information processed, stored or transmitted and keeps that risk assessment current when there is a significant change to the operating environment or information systems. The DoD wants to know that contractors are looking for the vulnerabilities on their systems and are ensuring that they do a risk assessment to see what damage could be done if those systems were compromised. AT 2 (2) specifies that the contractor must provide documentation that their training program includes recognizing and reporting potential insider threats. This is becoming more and more of a focus point within the DoD.
The NIST SP 800-53 controls called out by NIST SP 800-171. New controls are green, controls no longer required are red and controls remaining the same are black.

252.204.7008 “Compliance with Safeguarding Covered Defense Information Controls” allows for contractors to implement their own controls if those above do not fit. The purpose is to provide contractors some flexibility. However, the new language also specifies that contractors must provide written justification to the government’s contracting officer. The contracting officer will submit the justification and alternate plan to the DoD Chief Information Officer (CIO) and will receive approval from the DoD CIO as to whether the alternative controls may be used in the specified solicitation and ensuing contract. This pre-approval process has many contractors wondering if the process is worth it, or may be more risky during the proposal process than attempting to address the NIST controls as listed.
Who, How and What of Reporting:
The Cyber Incident Reporting requirement is now called the “Rapid Reporting Requirement” and contains several updates:

1) A reportable cyber incident is one that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor’s ability to perform the requirements of the contract that are designated as operationally critical.
   Two important things to note:
   a. The scope is expanded to include Covered Defense Systems and Information.
   b. The scope is narrowed in that a system or information must be affected rather than “potentially affected.”
2) Subcontractors must report directly to the government in addition to reporting to primes.
3) Greater emphasis is placed on Malware collection.
4) The Government makes an effort to protect contractors in the reporting process by including the following: The Government acknowledges that information shared by the contractor under these procedures may include contractor attributional/proprietary information that is not customarily shared outside of the company, and that the unauthorized use or disclosure of such information could cause substantial competitive harm to the contractor that reported the information. The Government shall protect against the unauthorized use or release of information that includes contractor attributional/proprietary information.

Driving Factors

Prime Contractors
The requirement for prime contractors to pass this clause along in all subcontractors remains the same in the interim ruling. H2L Solutions has seen an uptick of subcontractors reaching out for help in drafting a DFARS compliance plan in relationship to several of the large prime contractors implementing subcontractor management plans.

The DoD’s point of view as of September 24, 2015
At the UAH Cybersecurity event on September 24, 2015, David S. Lane, Assistant Director BMDS, fielded a multitude of questions from local DoD contractors who are currently responding to solicitations which contain DFARS 252.204.7012. Among the concerns:
1) What does compliance look like?
2) What is the best way to demonstrate a contractor’s steps towards compliance with the new ruling in solicitations that are due within the next 60 days? Is it better to submit an alternate
set of controls or a POA&M to the new controls since we really have not had the time to implement them?
3) What instructions are being given to the contracting officers who are supposed to be fielding the submissions regarding the clause and regarding the potential for receiving alternate plans?
4) When can we expect guidance on the ruling?

Attendees were not provided any clear guidance points or specific answers to the questions listed above, but there were some general takeaways from Assistant Director Lane and the other panelists:

1) Risk Management is still the goal.
2) Look at whether you are meeting the spirit and intent of the law.
3) The government is still working out guidelines and further definitions. MDA will have a meeting on Tuesday, September 29, 2015, and, at a date still TBD, will release the guidelines.
4) The DoD may outline some of their requests during the source selection phase.

Take Away Points

1. **Address Risk** – At the most basic level, this means asking yourself, “What would be the most detrimental thing for your company to lose?” Ask yourself, “How you are protecting it?”

2. **Address the controls** – The majority of the original 51 NIST SP 800-53 controls remain in effect. Continue to implement them. Create a gap analysis of what you are implementing, and what still needs to be implemented. Then, look at the additional 30 controls. Document what policies and practices you are already using. Create a list and POA&M of what still needs to be addressed.

3. **Submit your questions to us** - Many parts of the regulation are unclear either in statement or in execution, and the workload for small businesses has increased.

There are 3 ways to do this:
- Submit them to **H2L Solutions**: carol.claflin@h2lsolutions.com and jonathan.hard@h2lsolutions.com

This rule is in effect now, do not wait to start your compliance process as you may run into a deadline for submission where you will be unable to verify compliance. It has been our pleasure to provide assistance to companies across the United States from micro sized to mid-level to large primes with their DFARS Safeguarding needs. If we can be of service, please do not hesitate to reach out.