2017 DFARS Cyber Compliance Deadline: Modified or Not?

By: Michael G. Semmens, President of Imprimis, Inc.

On December 7, 2017, the Honorable Ellen M. Lord, Under Secretary of Defense for Acquisition, Technology and Logistics (AT&L), provided testimony before the Senate Armed Services Committee (SASC) regarding the implementation of the "Cyber DFARS" (Defense Federal Acquisition Regulations Supplement). In her testimony, she said, "We said that clearly the only requirement for this year [2018] is to lay out what your plan is. That can be a very simple plan. We can help you with that plan. We can give you a template for that plan. Then just report your compliance to it."

That testimony has caused several articles to be published with headlines such as " Pentagon Delays Deadline for Military Suppliers to Meet Cybersecurity Rules". In response to such articles, a Pentagon spokesman said that the change should not be considered a delay in the deadline since contractors will still document, by December 31, how they will implement the new rules.

So, is the deadline delayed? Really? Well, in keeping with the crisp clean roll-out and implementation of the Cyber DFARS, the answer is a definite yes and no.

A quick review of the brief history of the Cyber DFARS assists in understanding the current situation. After extensive rumors, the first cyber regulations were published in November of 2013 with a deadline at the end of 2015 for reaching compliance. There was great push-back from contractors large and small. So, the Department of Defense (DoD) delayed the deadline to December 31, 2017 and published an updated DFARS regulation that required compliance with NIST 800-171, a newly designed cybersecurity standard specifically applicable to government contractors – first DoD contractors and then all government contractors.

Efforts to comply with the DFARS cyber requirements have been all over the board. Those who see cybersecurity as a necessity and as a competitive advantage moved out and got to work. They are in good shape to meet the deadlines. Many have continued to push back and this push-back, at least in part, is why Ms. Lord was questioned in the SASC.

Roll forward to September of 2017, just 4 months before the deadline. Mr. Shay D. Assad, Director, Defense Pricing/Defense Procurement and Acquisition Policy (DPAP), published guidance to all DoD contract officers (CO or KO) regarding the implementation of DFARS 252.204-7012 and the other DFARS subparts. There are a number of key takeaways from this memorandum.

1. Purpose of the guidance:

    - *This guidance is provided for DoD acquisition personnel in anticipation of the December 31, 2017, deadline. It outlines, in general, the manner in which contractors are likely to approach implementing NIST SP 800-171; addresses how a contractor may use a system security plan to*

document implementation of the NIST SP 800-171 security requirements; and describes examples of how DoD organizations might choose to leverage the contractor's system security plan, and any associated plans of action, in the contract formation, administration, and source selection processes.

2. Contractors Responsibility:

    - *Ultimately, it is the contractor's responsibility to determine whether it has implemented the NIST SP 800-171 (as well as any other security measures necessary to provide adequate security for covered defense information)*

3. System Security Plan (SSP) & Plan of Actions and Milestones (POA&M):

    - *NIST SP 800-171 was revised (Revision 1) in December 2016 to enable nonfederal organizations to demonstrate implementation or planned implementation of the security requirements with a "system security plan" and associated "plans of action." [Security Requirements 3.12.4 & 3.12.2]*

    - *To document implementation of the NIST SP 800-171 security requirements by the December 31, 2017, implementation deadline, companies should have a system security plan in place, in addition to any associated plans of action to describe how and when any unimplemented security requirements will be met, how any planned mitigations will be implemented, and how and when they will correct deficiencies and reduce or eliminate vulnerabilities in the systems. Organizations can document the system security plan and plans of action as separate or combined documents in any chosen format.*

4. Inclusion in Proposals and Contracts:

    - *In addition, the solicitation may require or allow elements of the system security plan, which demonstrates/documents implementation of NIST SP 800-171, to be included with the contractor's technical proposal, and may subsequently be incorporated (usually by reference) as part of the contract (e.g., via a Section H special contract requirement).*

5. Inclusion as Evaluation Criteria:

    The requiring activity must state in the solicitation whether and how it will consider the contractor's implementation of NIST SP 800-171, as documented in the system security plan or otherwise, as part of the source selection process. Examples of how a requiring activity may utilize the system security plan and associated plans of action include, but are not limited to:

- *Using proposal instructions and corresponding evaluation specifics (detailed in sections L and M of the solicitation as well as the Source Selection Plan) regarding how implementation of NIST SP 800-171 (and other applicable security measures) will be used by DoD to determine whether it is an acceptable or unacceptable risk …*

- *Establishing compliance with DFARS 252.204-7012 as a separate technical evaluation factor and notifying the offeror that its approach to providing adequate security will be evaluated in the source selection process.*

- *Requiring that proposals i) identify any NIST SP 800-171 security requirements not implemented at the time of award and ii) include associated plans of action for implementation. If the implementation date is after the date of award then the contracting officer may choose to incorporate that plan by reference into the contract to ensure the contractor is held accountable to meet the NIST SP 800-171 requirements in accordance with its own plans. Identifying in the solicitation that all security requirements in NIST SP 800-171 must be implemented at the time of award.*

So, the situation appears to be that the deadline has NOT changed, but rather the DoD is willing to work with contractors via their SSP and POA&M. They will expect a well-reasoned and documented SSP and POA&M at the time of procurement after the end of this year (2017). This is consistent with the DFARS 204.73 /239.76 and the prescribed clauses 252.204-7012 /-7008 /-7009 all of which carry the deadline of December 31, 2017. It is also consistent with very unofficial rumors that DoD will be willing to work with the SSP/POA&M in 2018 but will expect full compliance by 2019.

In this author's opinion, an opinion shared by the DIB ISAC (Defense Industrial Base Information Sharing and Analysis Center), the most important part of the guidance provided to COs is the requiring activity or procurement office to consider the contractor's (bidder's) implementation of NIST 800-171 as part of the source selection process. They can establish acceptable levels of risk as a screening factor, identify the compliance of NIST 800-171 as a separate technical evaluation factor, and can include portions of the SSP/POA&M as part of any resulting contract. Cybersecurity is now a part of the fabric of competitive procurements within DoD. This is major. This is genius if used. There is no stronger motivator than competition and all its force will be unleashed on cyber compliance. Compliance today is a competitive advantage. Period. [Drop the mic.]

The SSP generally consists of 4 or5 major parts depending on the inclusion of the POA&M. These are:

1. The System Description and Definition (description, scope, system diagram(s), inventory, etc.)
2. The Governance (organization, authorizations, specific responsibilities and accountability)
3. Risk Assessment and Categorization (understanding of environment, threats, and risks.)
4. System assessment of compliance with the 110 requirements of NIST (SP) 800-171.
5. The POA&M be provided separately or be integrated with the assessment and remediation plan.

All Imprimis classes and webinars on the topic of compliance identify that the milestone of completing the assessment of compliance with NIST (SP) 800-171 (and preferably with a vulnerability scan) and identifying the remediation activities as a very critical milestone. The criticality of these milestones cannot be emphasized enough! It is at this point that the management and leadership of the organization can identify both their compliance status and the remaining requirements, and then develop an implementation plan that fits their organization, their capability and available resources. Our suite of tools and services have been developed to support management's reaching this milestone as rapidly as possible with a solid technical grasp on their specific situation. Now, with the September guidance provided by DPAP, this critical milestone has become even more important.

Performing a compliance assessment and formulating the remediation tasks should be about a two-day process for most organizations – a little more if bigger and slightly less if smaller. At this point some significant decisions need to be made regarding the compliance effort. These mostly deal with the approach or the "how" to achieve compliance. What are the policies of the organization? Are they complete? How will scanning be done? How will constant monitoring be done? How will multi-factor authentication be addressed?

Once these questions are answered, a budget and schedule of these tasks can be laid out and the SSP and POA&M can be completed.

On a final note, the contractor needs to be cautious with the use of the SSP / POA&M, particularly with the signing of the Certifications & Representations included in the proposal. The existence of a POA&M is a dispositive statement that the contractor is NOT in full compliance with NIST (SP) 800-171. So, take caution not to sign any certification or representation document that would state that you are in full compliance. Rather, refer to your SSP and incorporate all or part of the SSP / POA&M as part of your proposal and potentially the resulting contract. The September guidance is fully supportive of this approach. And above all, talk with the Contracting Officer to make sure you are responding to the requirements that they are specifying for the procurement.

The September Guidance Memorandum and the June Briefing to Industry are available at www.imprimis-inc.com, and the short video describing the process of achieving and sustaining compliance can be found at www.i2compliancetools.com. Call (719) 785-0320 for information.

ABOUT IMPRIMIS: Imprimis, Inc., or i2, is a technical professional services firm specializing in cybersecurity risk management and compliance, cybersecurity technology, advanced training, and space technology. Imprimis maintains a suite of cybersecurity compliance tools that empower management of organizations to effectively assess risk and their state of compliance, develop remediation approaches and System Security Plans (SSP) including a Plan of Action and Milestones (POA&M).