New Cybersecurity Compliance Guidelines for all Defense Contractors and what to do about them

By Jeremy Rasmussen, CISSP, CEH, PMP
Cybersecurity Director, Abacode

March 24, 2017

Summary

New guidance[1] in the Defense Federal Acquisition Regulation Supplement (DFARS) requires all companies doing business with the US Department of Defense (DoD) – including both prime contractors and subcontractors – to safeguard sensitive defense-related data and report cybersecurity incidents. To do this, companies must show compliance with the US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. Abacode provides a specialized compliance assessment package that performs a gap analysis of a company's security posture in accordance with NIST SP 800-171 and helps prioritize remediation efforts.

This is required **right now for all defense contractors!** Non-compliant companies will not be able to bid on any new work with the DoD until they become compliant. All 10,000+ DoD contractors (including small businesses) must be compliant by Dec. 31, 2017.

Background

Controlled Unclassified Information (CUI) is any defense-related data that includes all unclassified data not for public release, such as:

- Export Controlled information
- Privacy Information
- Protected Health Information
- For Official Use Only (FOUO)

The Defense Security Service (DSS) manages handling of classified data at contractor sites in accordance with the National Industrial Security Program Operating Manual (NISPOM). However, up till now, there has been little guidance on contractor handling of CUI.

The DFARS is required for all contractors doing business with DoD. They must follow it in the procurement process for goods and services. A recent change in Section 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting – pertains to cybersecurity controls of CUI. DFARS 252.204-7012 states that for any I.T. services **not** operated on behalf of the government, DoD contractors must:

- Implement all security requirements in **NIST SP 800-171**.
- Notify DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or

[1] The "Final Rule" was promulgated on August 26, 2015 initially; however, some of the key provisions were updated on December 30, 2015. See the Federal Register, Vol. 80, No. 250 here: https://www.gpo.gov/fdsys/pkg/FR-2015-12-30/pdf/2015-32869.pdf.

- Have a Plan of Actions and Milestones (POA&M) for correcting any deficiencies

Abacode's Approach

Our Abacode cybersecurity engineering team contacted authors of NIST SP 800-171, including Patrick Viscuso and Mark Riddle of the **Information Security Oversight Office (ISOO)** in the **National Archives and Records Administration (NARA)**, which has the role of defining policy for the confidentiality of CUI in contractor owned information systems – to seek further clarification on compliance.

We learned that the NARA is doing the following for deployment of the new guidelines:

- Added standard language to all new defense acquisition contracts to require **self-asserted compliance** (as of August, 2016).
- Plans to add same language and requirements for **all** federal acquisition contracts (by end of 2017).
- Plans to add an adjunct to General Services Administration (GSA) System for Award Management (SAM) contractor portal to allow for upload of self-assertion compliance reports (by 2018).
- Plans to add federal audit teams that will come out and audit contractors on a limited basis (by 2020).

We also requested specific guidance on how companies to need to show compliance against the NIST SP 800-171 standard. NARA stated that they intentionally left this somewhat vague to allow some flexibility in the self-reporting process. However, they concurred that Abacode's compliance assessment approach was a "best practice." The justification for our approach and high-level description of our methodology is as follows:

- NIST SP 800-171 is derived from the security controls in NIST SP 800-53 Risk Management Framework (RMF).
- The corresponding validation procedures for RMF are published in the RMF Knowledge Service https://rmfks.osd.mil).
- Compliance for each security control in NIST SP 800-171 generally means implementing security settings in accordance with the Defense Information Systems Agency (DISA) published **Security Technical Implementation Guides (STIGs)** and Security Requirements Guides (SRGs).
- Therefore, Abacode's assessment approach incorporates verifying that all I.T. system components are configured in accordance with the STIGs and SRGs.

Impactful Controls – Start Planning Now!

There are some potentially impactful controls in NIST SP 800-171 for which defense contractors should be cognizant and begin planning for implementation. These include the following:

- **Multi-Factor Authentication** for both local and remote access.
    - Reference OMB memo M-14-04 and Homeland Security Presidential Directive-12
    - This is a critical White House initiative, especially for organizations handling Personally Identifiable Information (PII) — due to the number of breaches of this type of data over the past few years.

Abacode can assist in providing solutions that implement multi-factor authentication for enterprise login, email, and other services.

- **Continuous Monitoring** – there are 15 separate requirements in NIST SP 800-171 that address this, including:
    - Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
    - Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
    - Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.
    - Identify, report, and correct information and information system flaws in a timely manner.

Abacode provides the **Cyber Lorica™** Network Intrusion Detection System (IDS) / Security Information and Event Management (SIEM) and outsourced 24/7 Security Operation Center (SOC) monitoring for security-relevant events. Without this, an organization is "flying blind", and all incident response tends to be very reactionary with a wide margin for error (e.g., attackers having opportunity to cover their tracks).

Other Provisions

Besides compliance with NIST SP 800-171, DFARS 252.204-7012 states also requires that when defense contractors discover a cyber incident that affects CUI, they must:

1. Conduct a review and forensic investigation
2. Report cyber incidents via report form at http://dibnet.dod.mil

Note: This requires a DoD-approved medium assurance certificate, available from: http://iase.disa.mil/pki/eca/Pages/index.aspx

The regulation further stipulates:

1. Any **malicious software** found in connection with the incident must be submitted securely to the DoD in accordance with contractual guidelines.
2. Contractors must **preserve and protect media** of all known affected information systems and **all relevant monitoring/packet capture data** for at least 90 days from the

submission of the cyber incident report to allow DoD to request the media or decline interest
3. Upon DoD request, contractors must **allow access** to additional information or equipment necessary for forensic analysis.
4. Upon DoD request, contractors must provide all **damage assessment** information gathered.

Besides providing continuous monitoring, Abacode's Cyber Lorica™ solution helps create a state of forensic readiness by pulling all log and event data into one aggregation center. This allows for proper incident response in compliance with these guidelines as follows:

1. Maximizing an environment's ability to collect credible digital evidence; and
2. Minimizing the cost of forensics during an incident response.

Conclusion

This is a great opportunity for defense contractors to get out ahead of the curve by being proactive, completing their NIST 800-171 gap assessment and Plan of Actions and Milestones (POA&M), and then leading the charge for any subcontractor partners. Please call Abacode today at (813) 321-4949 or email insight@abacode.com to schedule your compliance assessment today!