SENTAR

DFARS 252.204-7012

DFARS, SMEAFARS and NIST, OH MY!

J. Chandler Hall
Cybersecurity Evangelist

Chandler.Hall@Sentar.com

Related Terminology

- DFARS CDI – Covered Defense Information
- FARS CUI – Controlled Unclassified Information (coming late this year)
- NIST SP 800-171 (CUI)
- Other:
  - UCTI – Unclassified Controlled Technical Information
  - NIST SP 800-53
- Assessment is NOT an Audit

What's this all about?

- Obligation:
  - Contractors will now need to meet minimum cyber security requirements for non-classified information that may not have been previously controlled
- The DFARS 252.240-7012 requirement is expected to be in **ALL** DoD solicitations and contracts going forward.

Overview of the Requirement

- Requires DoD Contractors and Subcontractors:
  - Safeguard Covered Defense Information
  - Also called Unclassified Controlled Technical Information (UCTI), or Controlled Unclassified Information (CUI)
  - MARKED OR UNMARKED
  - Report cyber security incidents within 72 hours
- Some Primes are requiring Subs to provide their Gap Analysis; not a requirement of DFARS

DFARS CDI Requirement Specifics

- DoD Prime- and Sub-Contractors must be compliant by end of 2017
  - Must have completed a Gap Analysis within 30 days of new contract award; “flow down” requirements vary
  - Must have a documented POA&M (Plan of Action & Milestones); this plan should show how Gaps will be removed/solved by end of 2017
  - Must provide commitment & documentation to DoD; also to your prime

CDI/CUI/UCTI Exposure

- On laptop, on phone; email within in-house server, in Dropbox, iCloud, Skydrive…SNAPCHAT?
- Bring Your On Device (BYOD) creates exposure
  - Clarification of CDI Contract specification is requested in email; email is on phone; they print the data or their phone is backed-up on home computer or iCloud…
- Examples: Contracts, Cost Data, Technical reports & orders; Research & Engineering data; Computer s/w & source; Engineering drawings; Specifications; Data sets; and Studies or Analyses
- There is a CUI Registry online

What are Your Options?

- Hire an Assessor
- Use your own IT & Security experts
  - Consider hiring a consultant to conduct a Pre-Assessment or Train-the-Assessor session
  - Purchase Tools (Policy Templates, CyberProtex; Imprimus, CSET (this is free); etc)
  - Spreadsheet and labor hours
  - Strongly recommend hiring a “check the work” consultant if DIY
- Isolate CUI or walk-away from the business

Costs?

- The cost of the assessment (averages)
  - Minimal-medium complexity: $15K - $50K
  - Medium-large complexity: $20K - $250K+
- The cost of COMPLIANCE could be higher
- The cost of NOT complying could mean loss of all DoD revenue; Sanctions, Stop Work Orders
  - We think stop work orders are a likely penalty
  - Competitively, you may not win bids against others in 2017 that are DFARS compliant

Do's

- Do review your contract for the clause
- Do your assessment
- Do follow through with your POA&M
- Do create your Incident Reporting Account
- Do flow-down the requirement to your subs
- Do consider hiring experts for the Assessment
- Do consider air gapping/isolating that work, if appropriate, to reduce impact of compliance

Don’ts

- Don’t ignore the requirement
  - EVERY client we have assessed confirmed they had CDI and must implement the controls
  - Even if all of your personnel are onsite using Government Systems
- Don’t wait long: earlier = less pain
- Don’t turn in a “No Gaps” assessment – you will certainly be questioned and may be audited
- Don’t miss your POA&M dates

Questions?

Chandler Hall
256.653.3233
Chandler.Hall@Sentar.com