Bidding On Government Contracts: Compliance With The DFARS Cyber Rule

Dr. Michael Papay, Vice-President, CISO, Northrop Grumman

Jim Winner, General Counsel, GardaWorld Federal Services

Robert S. Metzger, Shareholder, Rogers Joseph O'Donell PLLC

Jonathan Hard, CEO, H2L Solutions

Rolando R. Sanchez, Owner, R.R. Sanchez PLLC (Moderator)

Phase I - Pre-Solicitation

- **December 2016**
- **Awardee, Inc.** is a technology company with a government services division which creates sophisticated warfighting software tools. The company already has contracts with DOD, both as a prime and as a sub-contractor. The company's new government services director is assessing capabilities for future government contracts and contacts you concerning DFARS 252.204-7012.
  - What assurances do you want to give concerning DFARS compliance?
  - Does the size of the company matter?
  - Is the DFARS the only cybersecurity requirement imposed by the government?
  - Does it matter that it is not yet December 2017?

Phase 2 - Pre-Solicitation

- **January 2017**
- In an effort to prepare for DFARS compliance, **Awardee** decides to conduct a self-assessment of it cybersecurity capabilities and begins to plan for this assessment.
  - How much of the company's leadership/management should be included in this assessment? How should they participate?
  - How should the company focus its self-assessment?
  - Should the capabilities of sub-contractors/vendors be included in this phase? What realistically is happening concerning this sort of information sharing between companies?

Phase 3 - Pre-Solicitation

- **March 2017**
- **Awardee's** self-assessment reveals that it is not in compliance with NIST SP 800-171. It hires **CyberTech, Inc.** to help it achieve full compliance as soon as possible.
  - What are some the considerations for hiring cybersecurity firms? How much reliance should Awardee place on CyberTech?
  - Can **Awardee** avoid NIST SP 800-171's security requirements by using cloud services?
  - Does compliance with NIST (or use of cloud services) equate to DFARS compliance?

Phase 4 - Solicitation

- **January 2018**
- **Awardee** plans to bid on a DOD contract to provide software and related equipment. The software will be export controlled but not classified and some of the equipment will also be export controlled but not classified. **Awardee** will be the prime and plans on using **Sub, Inc.** for some software support. **Sub** informs that it is in compliance with DFARS 252.204-7012 but it is not sure about some of the consultants that it plans to use for the contract. It's also not sure if it will even handle CDI.
  - What are the problems with determining what is CDI? How can a contractor seek definition from the government?
  - How much concern should **Awardee** have if **Sub's** consultants are not compliant with protection safeguards of CDI
  - How much concern should **Sub** have concerning its consultant's possible lack of compliance?
  - How can **Awardee** assure that **Sub** and its consultants are compliant?
  - How should **Awardee** prepare for the DOD's verification of compliance?

Phase 5 - Award

- **May 2018**
- **Awardee** wins the contract.
  - What parting DFARS 252.204-7012 compliance advice would you give Awardee as it begins performance on its new contract?
  - With a new administration taking over in January 2017, what do you expect may change with the DFARS? What do you think should change by way of revisions to the DFARS?