CYBERSECURITY

DATE
April 6, 2017

SPEAKERS
Ms. Vicki Michetti (pictured above)
Director, Defense Industrial Base (DIB) Cyber Security (CIB CS) Program, DoD CIO

Ms. Mary Thomas
Program Analyst, DPAP

BACKGROUND
The Department of Defense (DoD) Office of Small Business Programs (OSBP) in partnership with the Small Business Administration sponsored Small Business Training Week (SBTW17) at the Sheraton Atlanta in Atlanta, Georgia. Answers to questions submitted through the OSBP SBTW mobile app are included below.

QUESTIONS AND ANSWERS
Many primes do not know the suppliers in their supply chain below the next tier. How does a prime manage the cybersecurity of its supply chain if it does not know the suppliers?
DFARS Clause 252.204-7012 flows down to subcontractors when performance will involve operationally critical support or covered defense information. The contractor will determine if the information required for subcontractor performance retains its identity as covered defense information or if the effort will involve operationally critical support, thus requiring flowdown of the clause. Once the clause is flowed down to a subcontractor, the subcontractor must in turn determine if the information required for its subcontractors' performance retains its identity as covered defense information or if the effort will involve operationally critical support, thus requiring flowdown of the clause. Flowdown is to be enforced by the prime contractor to its subcontractor(s), by subcontractor(s) to any subtier subcontractor(s) and so on down the supply chain.

TWEETS

Check out videos from #SBTW17 at http://tiny.cc/kny0ry.

Check out the presentations from #SBTW17 at https://go.usa.gov/x5GJG.

Has DCMA been trained on how to provide oversight for this new requirement?
DCMA's surveillance of cybersecurity contract requirements is consistent with the self-assessment model on which the clauses are based. Essentially, at the time of award, the contractor self-attests to be compliant with DFARS Clause 252.204-7012.

DCMA will verify that the contractor has a system security plan and associated plans of action as appropriate. DCMA will not assess the system security plan against the NIST 800-171 standards.

The cybersecurity requirements identified in the clause are part of existing DCMA software surveillance activities.

Additional actions DCMA will take in regards to cyber-security are:

1. If a potential cyber-security issue is detected, DCMA will notify the contractor, DoD program office and the DoD CIO.

2. During the normal Contract Receipt and Review process, DCMA will verify that applicable cybersecurity clauses are in the contract.

3. Through Oct 2017 verify that the contractor submitted notification within 30 days of award to the DoD CIO a list of the security requirements that the contractor is not yet implementing.

4. Verify that the contractor possesses the necessary DoD-approved medium assurance certificate required to report cyber incidents.

5. As required, facilitate the entry of government external assessment team into applicable contractor facilities via coordination with cognizant government and contractor stakeholders.

Training and guidance for these minimal tasks are being incorporated into DCMA training, manuals, tools, templates and reports. DCMA personnel are engaging with contractors to implement these actions as part of normal software surveillance activities. DCMA is not performing technical assessment of the cyber-security standards, i.e. NIST 800-171.

Do you require contractors who have a Facility Clearance to adhere to the same rules of information protection as if on a government facility for information-protection purposes?
DFARS Clause 252.204-7012 requires a contractor or subcontractor to safeguard covered defense information that is resident on or transiting through a contractor's internal unclassified information system or network.

The requirements for protection of an unclassified system are not in any way associated with the requirements for a facility clearance. A facility clearance (FCL) is an administrative determination that, from a national security standpoint, a facility is eligible for access to classified information at the same or lower classification category as the clearance being granted. The FCL may be granted at the Confidential, Secret or Top Secret level.

LEARN MORE

We are the Department of Defense (DoD) Office of Small Business Programs (OSBP). We maximize opportunities for small businesses to contribute to national security by providing combat power for our troops and economic power for our nation.