520.743.7554
info@computerdimensions.net
www.computerdimensions.net

DOD Will Start Requiring Contractors To Meet Cybersecurity Standards In 2020

The Department of Defense (DOD) will roll out its Cybersecurity Maturity Model Certification (CMMC) in January 2020 so that it can ensure contractors on government projects have the necessary cybersecurity practices in place to protect the controlled unclassified information (CUI) to which they are privy. The type of information the DOD is trying to protect includes data pertaining to critical infrastructure, nuclear, proprietary business information, procurement and acquisition.

All DOD contractors must be certified through the third-party provider of their choice at the contractor's expense. Certification levels range from basic to advanced, and in June 2020 contractors will start seeing references to CMMC requirements in Requests for Proposals. Some higher-level assessments may be performed by the DOD, the Defense Contract Management Agency or the Defense Counterintelligence and Security Agency.

The loss of CUI, the DOD said, poses risks to the United States' economic security and national security, so the department is trying to better secure this information. The Executive Office of the President's Council of Economic Advisers estimated in 2016 that malicious cyber activity cost the nation's economy between $57 billion and $109 billion. The DOD released the latest draft version of the CMMC for public review earlier this month. In that document, the DOD delves deeper into the levels of certification.

Level 1 - the contractor demonstrates basic cyber hygiene as defined by Federal Acquisition Regulation
Level 2 - the contractor demonstrates intermediate cyber hygiene and has established standard operating procedures, policies and plans for all its practices.
Level 3 - the contractor demonstrates good cyber hygiene and effective NIST SP 800-171 Rev 1 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations) security requirements and reviews its activities for adherence to policies and procedures.
Level 4 - the contractor demonstrates a substantial and proactive cybersecurity program, reviews activities for effectiveness and informs management of any issues.
Level 5 - the contractor demonstrates a proven ability to optimize capabilities in an effort to repel advanced persistent threats, standardizes its activities across all applicable business units and shares identified improvements. Additionally, areas that contractors will be required to address in the certification process are:

- Access control policies
- Identification and authentication procedures
- Media protection strategies
- Protecting physical access
- System and communication protection
- System and informational integrity

As construction industry contractors continue to take bigger steps toward technology adoption, cyberattacks are not the only issue that should concern them. A rise in the popularity of wearables — heart rate monitors, location trackers, fall and fatigue detectors — and detect falls, and hard hat inserts that check for fatigue — has also raised questions about data collection and privacy. The Safety Equipment Association has started preliminary discussion around a standard that would protect worker privacy when it comes to wearables, but that process could take years. In the meantime, contractors should start thinking about the potential for abuse and misuse. Any company that adopts these tools must consider all of the value-adds and the potential risks before implementing these new technologies.