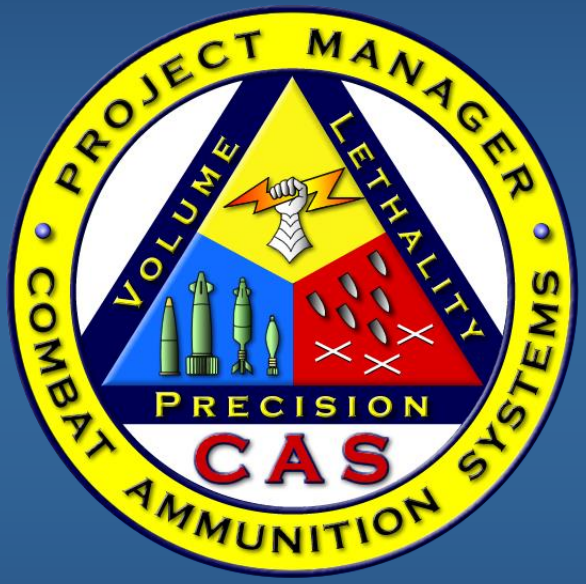
Cyber Security Update



September 2016

Raymond Colón
Conventional Ammunition Division
973-724-7617

"The Final Rule"

- In May 2016, DoD, GSA, and NASA issued a Final Rule to add a new subpart and contract clause 52.204-21 to the FAR "for the basic safeguarding of contractor information systems that process, store, or transmit Federal contract information."
  - ✓ See 81 Fed. Reg. 30439
- The focus of the Final Rule was changed from safeguarding of "specific government information" to safeguarding of "contractor systems"
- The Final Rule establishes a closer linkage with NIST SP 880-171 guidelines, which are appropriate to the level of technology, and are updated as technology evolves
  - ✓ Contractors that are in compliance with DFARS 252.204-7012 will be in compliance with this new FAR rule
- Contracting Officers are required to include FAR 52.204-21 in "solicitations and contracts when the contractor or a subcontractor at any tier *may have* Federal contract information residing in or transiting through its information systems"

Basic safeguards must be applied

Fifteen "basic" security controls for contractor information systems

- The above rule imposes fifteen "basic" security controls for contractor information systems upon which "Federal contract information" transits or resides

  (i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

  (ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

  (iii) Verify and control/limit connections to and use of external information systems.

  (iv) Control information posted or processed on publicly accessible information systems.

  (v) Identify information system users, processes acting on behalf of users, or devices.

  (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

  (vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

  (viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

  (ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

  (x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

  (xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

  (xii) Identify, report, and correct information and information system flaws in a timely manner.

  (xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

  (xiv) Update malicious code protection mechanisms when new releases are available.

  (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

- This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.
- Compliance deadline has been extended to December 2017