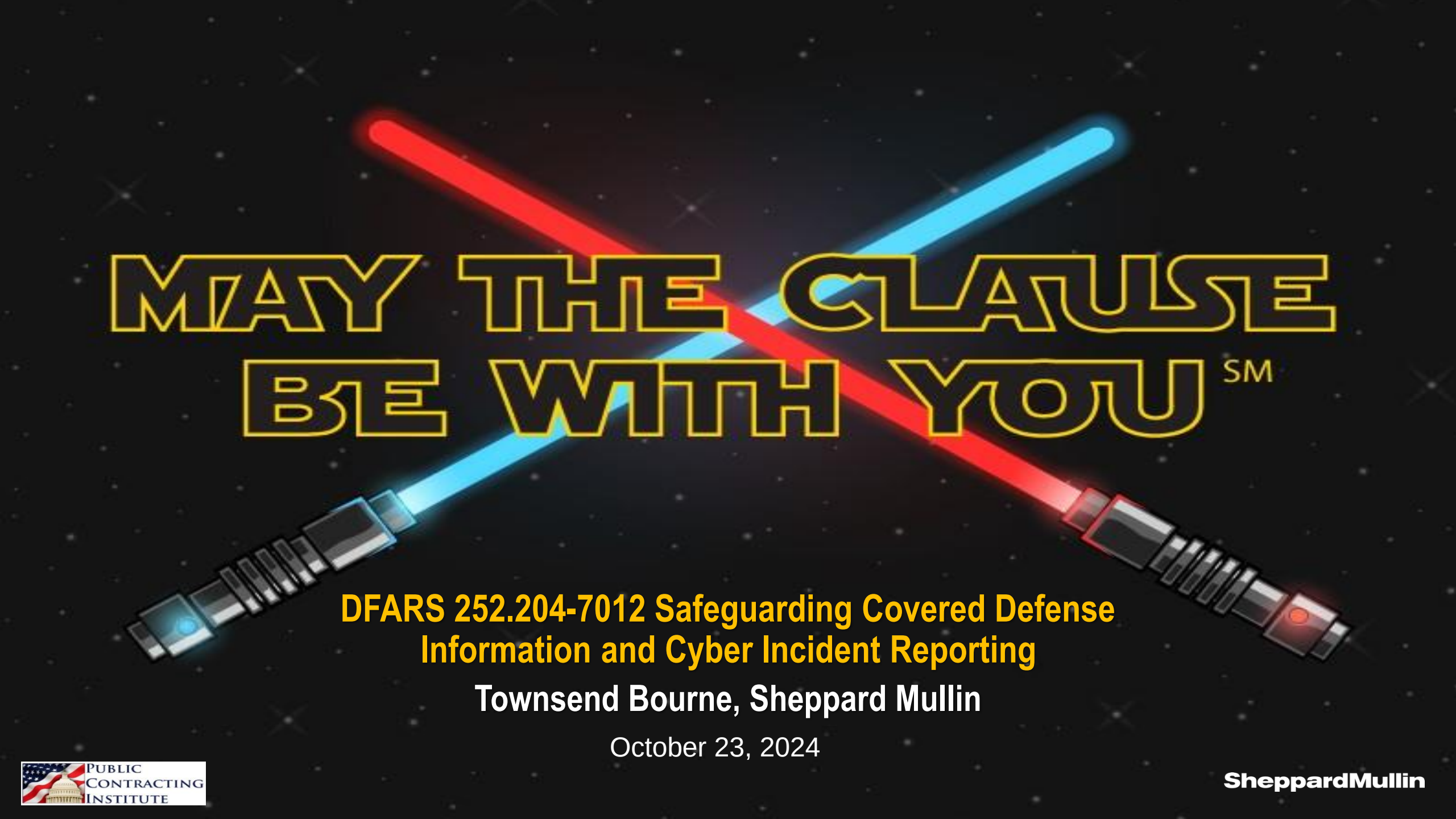


DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

Townsend Bourne, Sheppard Mullin

October 23, 2024

PUBLIC CONTRACTING INSTITUTE

SheppardMullin

Nice To Meet You!

Townsend Bourne

tbourne@sheppardmullin.com

(202) 747-2184

Townsend is a Partner and Aerospace, Defense & Government Services Team leader of Sheppard Mullin in Washington, D.C. Her practice focuses on national security, cybersecurity, and government business issues. She advises clients in a variety of industries, including aerospace and defense, critical infrastructure, IT, emerging technology, commercial products and services, and cloud service providers.

- Cybersecurity (training, policies, regulatory, incident response)
- Government Contracts (policies, investigations, protests, litigation)
- National Security (prohibited sources, supply chain risk, OCONUS work)
- Emerging technology, IT, cloud, AI (security, regulatory, best practices)

Recent Publications

- Countdown to Compliance: DoD Finalizes the CMMC Program Rule, 10.15.2024
- The CMMC Rule To Update the DFARS is Here!, 08.16.2024
- CISA Cyber Incident Reporting for Critical Infrastructure Will Significantly Impact Government Contractors, Suppliers, and Service Providers, 04.08.2024
- Governmental Practice Cybersecurity and Data Protection, 2023 Recap & 2024 Forecast Alert, 02.08.2024
- Unpacking The FAR Council's Cybersecurity Rules Proposal, *Law360*, 10.25.2023
- Bracing For Rising Cyber-Related False Claims Act Scrutiny, *Law360*, 09.18.2023
- ChatUSG: What Government Contractors Need To Know About AI, *BriefingPapers*, 07.2023

DFARS 252.204-7012 – *Safeguarding Covered Defense Information and Cyber Incident Reporting*

- Requires "adequate security" for covered contractor information systems (i.e., systems that process, store, or transmit covered defense information (CDI))
- "Adequate security" (usually) means compliance with NIST SP 800-171
- Incident Reporting: "Rapidly report" (within 72 hours of discovery)
- Cyber incident investigation and preservation requirements
- Flow-down in all subcontracts involving CDI or "operationally critical support"

Part (b) – "*Adequate Security*"

(b) *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections: …

"**Covered contractor information system**" means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

A Slight Detour…

"**Covered defense information**" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

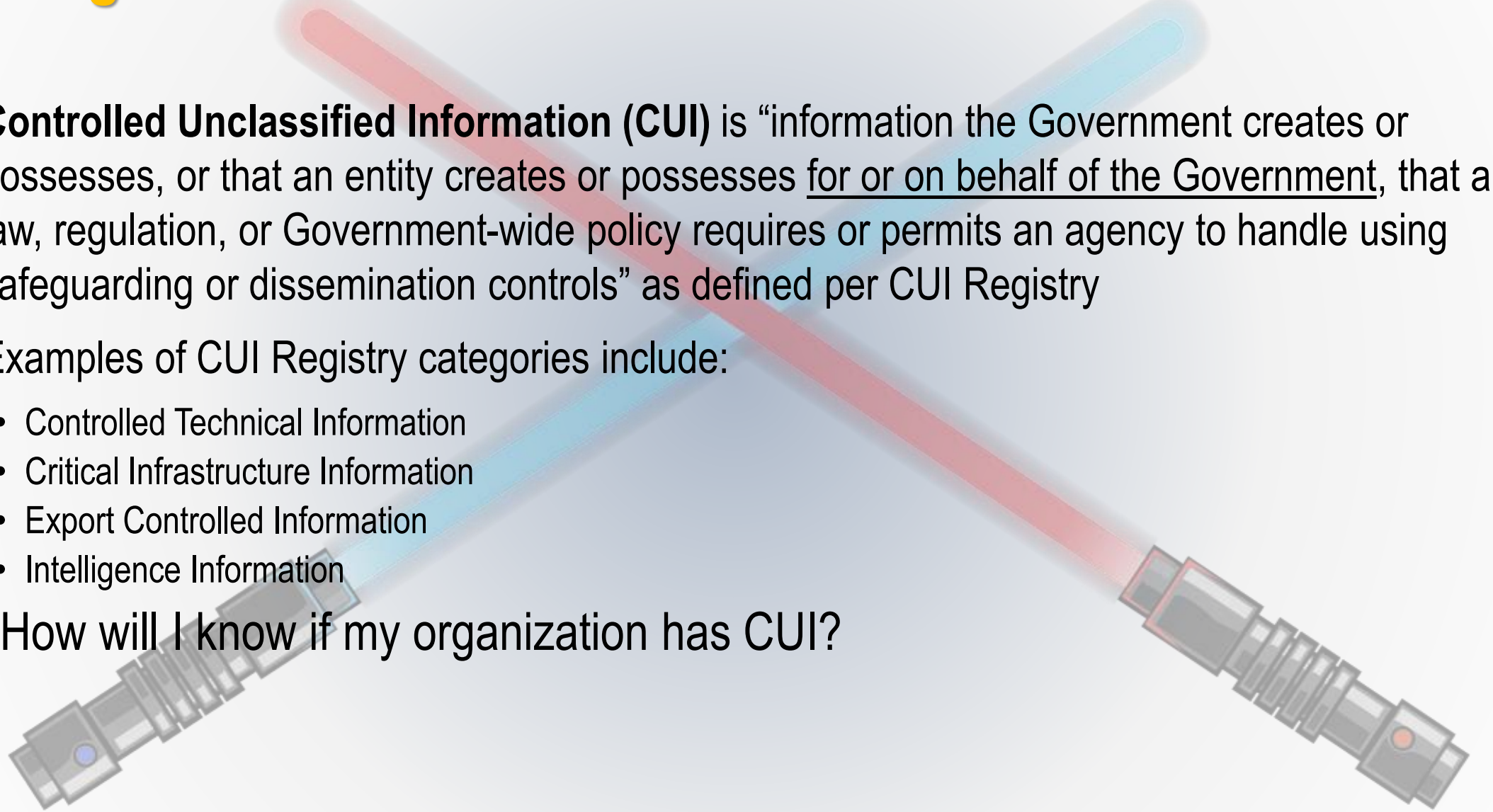
1. Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
2. Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

A Slight Detour…

"**Controlled technical information**" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

A Slight Detour…

- **Controlled Unclassified Information (CUI)** is "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls" as defined per CUI Registry
- Examples of CUI Registry categories include:
  - Controlled Technical Information
  - Critical Infrastructure Information
  - Export Controlled Information
  - Intelligence Information
- *How will I know if my organization has CUI?



Part (b)(1) – "*Adequate Security*"

b. *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

1. For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

i. Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010 , Cloud Computing Services, of this contract.

ii. Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

Part (b)(2)(i) – "*Adequate Security*"

b. *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

2. For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

i. Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at https://csrc.nist.gov/publications/sp800) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

Part (b)(2)(ii) – "*Adequate Security*"

b. (b) *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

2. For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply: …

ii. (A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

B. The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

C. If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.

Part (b)(2)(ii) – "*Adequate Security*"

b. *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

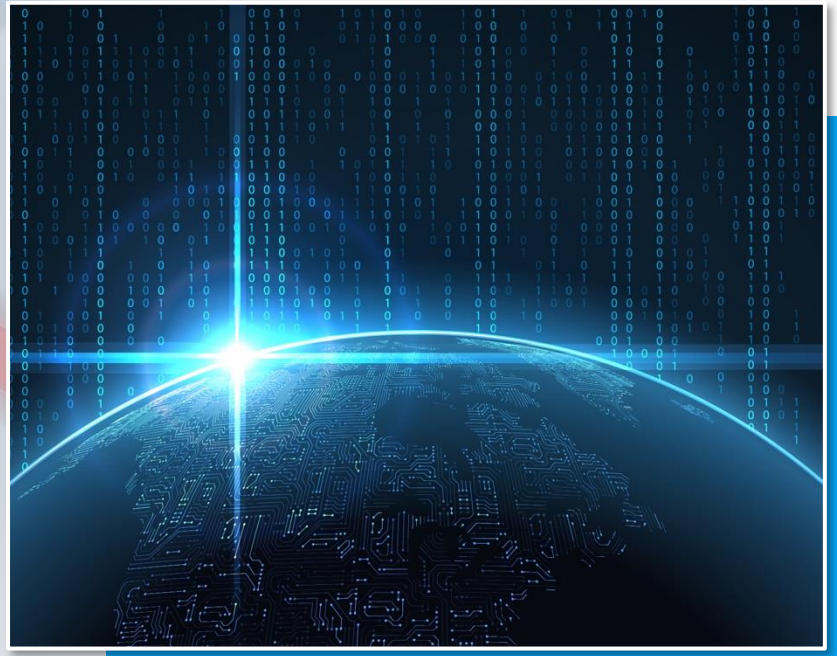
2. For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply: …

ii. (D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/documents-templates/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

Part (b)(3) – "*Adequate Security*"

b. *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

3. Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.



Part (c)(1) – "*Cyber incident reporting requirement*"

c. Cyber incident reporting requirement.

1. When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—

i. Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

Part (c)(1) – "*Cyber incident reporting requirement*"

c. Cyber incident reporting requirement.

1. When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—…

iii. Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.

- "Rapidly report" means within 72 hours of discovery of any cyber incident.

Part (c)(2) – "*Cyber incident reporting requirement*"

c. *Cyber incident reporting requirement*.

2. *Cyber incident report*. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at https://dibnet.dod.mil.

1. Company name
2. Unique Entity Identifier (UEI)
3. Facility CAGE code
4. Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not Applicable)
5. Contract Number (Procurement Instrument Identifier (PIID))
6. Company point of contact information (name, position, telephone, email)
7. U.S. Government Program Manager point of contact (name, position, telephone, email)
8. Contract number(s) or other type of agreement affected or potentially affected
9. Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
10. Contract or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not Applicable)
11. Impact to Covered Defense Information
12. Ability to provide operationally critical support
13. Date incident discovered
14. Location(s) of compromise
15. Incident location CAGE code
16. DoD programs, platforms or systems involved
17. Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
18. Description of technique or method used in cyber incident
19. Incident outcome (successful compromise, failed attempt, unknown)
20. Incident/Compromise narrative (Ex: Chronological explanation of event/incident, threat actor TTPs, indicators of compromise, targeting, mitigation strategies, and any other relevant information to assist in understanding what occurred)
21. Any additional information

Part (c)(3) – "*Cyber incident reporting requirement*"

c. *Cyber incident reporting requirement*.

3. *Medium assurance certificate requirement.* In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.

Part (d) – "*Malicious Software*"

d. *Malicious software.* When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

Part (e) – "*Media preservation and protection*"

e. *Media preservation and protection*. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

Part (f) & (g) – DoD Access and Damage Assessment Activities

(f) *Access to additional information or equipment necessary for forensic analysis.* Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) *Cyber incident damage assessment activities*. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

Part (h) – "DoD safeguarding and use of contractor attributional/proprietary information"

h. *DoD safeguarding and use of contractor attributional/proprietary information.* The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

Part (i) – "Use and release of contractor attributional/proprietary information not created by or for DoD"

i. *Use and release of contractor attributional/proprietary information not created by or for DoD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD—

1. To entities with missions that may be affected by such information;
2. To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;
3. To Government entities that conduct counterintelligence or law enforcement investigations;
4. For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or
5. To a support services contractor ("recipient") that is directly supporting Government activities under a contract that includes the clause at 252.204-7009 , Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

Part (j) – "Use and release of contractor attributional/proprietary information created by or for DoD"

j. *Use and release of contractor attributional/proprietary information created by or for DoD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

Part (k) & (l) – "Other safeguarding or reporting requirements"

k. The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

l. Other safeguarding or reporting requirements. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

Part (m) – "Subcontracts"

m. *Subcontracts*. The Contractor shall—

1. Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial products or commercial services, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and
2. Require subcontractors to—

i. Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

ii. Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

Additional Considerations

- **DFARS 252.204-7019/-7020 – *NIST SP 800-171 DoD Assessment Requirements***
  - Requires NIST SP 800-171 assessment for covered contractor information systems
  - Offeror must have current assessment posted in Supplier Performance Risk System (SPRS) to be considered for award (i.e., within 3 years)
  - Flow-down (-7020) in all subcontracts (except solely COTS) & contractor must ensure subcontractors have completed assessment

- **DoD Cybersecurity Maturity Model Certification (CMMC) Program**
  - DoD program for cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information
  - Goal is to create unified cybersecurity standard and certification program for companies in the defense industrial base to protect sensitive information
    - Federal Contract Information (FCI)
    - Controlled Unclassified Information (CUI)
  - Includes self-attestation, third-party assessment and certification requirements
  - CMMC Title 32 Program Final Rule released this month

Questions?

Sheppard Mullin Resources

Aerospace, Defense & Government Services Team

Governmental Privacy & Cybersecurity

https://www.sheppardmullin.com/tbourne