FEDERAL DEMONSTRATION PARTNERSHIP
Redefining the Government & University Research Partnership

Contracts and Data Transfer and Use Agreement Updates

FDP Virtual Meeting September 2020

Alexandra Albinak, Johns Hopkins University
Martha Davis, Brandeis University
Melissa Korf, Harvard Medical School

Session Agenda

- Prohibitions on certain telecommunications and video surveillance services or equipment (NDAA Section 889)
- Cybersecurity Maturity Model Certification (CMMC)
- Pending CUI FAR case
- Data Transfer and Use Agreement (DTUA) working group updates
- Overview of new Reciprocal DTUA Template
- Overview of new Collaborative DTUA Sample
- Discussion/next steps

NDAA Section 889

- Section 889 of the National Defense Authorization Act (NDAA) FY19 became effective August 13, 2020.
- The statutory prohibitions of Section 889 are implemented through prohibitions on use of contract funds in Federal Acquisition Regulations (FAR) clauses (52.204-24, 25 and 26) and separately in a prohibition on use of grant funds through the updated Uniform Guidance (UG) (200.216).

FAR 52.204.24, .25 and .26

- 52.204-25(b)(1) Federal Government **may not:**
  - Procure from a contractor equipment, systems or services that uses covered technology as a substantial/essential component.
- 52.204-25(b)(2) Federal Government **may not:**
  - Enter into a contract with a contractor that uses any equipment, systems, or services as a substantial/essential component.
  - ***Regardless of whether such use is in performance of the Federal contract***.

FAR 52.204.24, .25 and .26

- Prior to executing a contract with these FAR clauses, institutions must conduct a “reasonable inquiry” to assure that the university would not violate this prohibition by “using” such telecommunications products or services.
- The FAR requirements are limited to prime contractors and specifically does not apply to subcontractors.
- A certification is being added into SAM.

NDAA Grants Applicability

- Section 200.216 prohibits non-Federal entities **from obligating or expending** loan or grant funds to**:**
  - Procure or obtain,
  - Extend or renew a contract to procure or obtain; or
  - Enter into a contract (or extend or renew a contract) to procure or obtain, equipment, services, or systems that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as a critical technology as part of any system.
- Applies to both domestic and foreign subrecipients.

Uniform Guidance

- Inconsistency in UG language:
  - The UG II.A. states that Federal award recipients are prohibited from using government funds "to enter into contracts (or extend or renew contracts) with entities that **use** covered telecommunications equipment or services."
- COGR letter on 9-24-2020 asked that UG II.A be revised so that the prohibition matches the prohibition as intended by the NDAA.
- WARNING: Institutions are beginning to see the misinterpreted "use" language in grants.

Poll

- Has your institution conducted a “reasonable inquiry” and implemented a plan for compliance with these new FAR clauses?
  - Yes!
  - We are in the process of determining if we use covered technology.
  - We have a plan but have not yet gotten to the implementation phase.
  - We are just beginning our planning.
  - We haven’t received any contracts that include these clauses (thank goodness!) and cannot obtain buy-in to develop a plan until we do.
  - Other

Discussion

- How is your institution working to become compliant with these new requirements?
- Has anyone received a ***grant*** with a prohibition on use of covered technologies?
- How could the FDP be helpful in resolving some of these challenges?

Cybersecurity Maturity Model Certification (CMMC)

- "The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements." (https://www.acq.osd.mil/cmmc/index.html)
- Based on five progressive levels with the expectation that the RFI/RFP will state the required level. Each level consists of more ***practices*** and ***processes*** on top of those in lower levels.

How is this different from CUI?

- CUI:
  - Can be met with a self-assessment.
  - Self-assessment can be performed after award.
- CMMC
  - Certification must be obtained from a third party.
  - Third-party certification must be required prior to award.
  - In addition to assessing the implementation of cybersecurity practices, the CMMC will also assess the institutionalization of cybersecurity processes.

Anticipated Agency Implementation

- Initial implementation is expected only within the DoD.
- Expect to see CMMC requirements added to RFPs beginning in October 2020.
- Eventually, we may see CMMC requirements applying to all DoD funding, including assistance agreements.
- Complete DoD coverage targeted for Fall 2026.

Poll

- Has your institution implemented a plan for compliance with the new CMMC requirements?
  - We don’t receive DoD funding so don’t anticipate needing a plan.
  - We are just beginning to develop a compliance plan.
  - We have developed a plan but are working towards full implementation.
  - Yes, we are ready to go!
  - Other

Discussion

- What challenges has your institution experienced in implementing a plan for compliance with these new requirements?
- How could the FDP be helpful in resolving some of these challenges?
  - Resources/FAQs on how the cost of compliance can be built into the contract budget?
  - Collect data on whether the necessary information is being provided in the RFP and/or how the 5 levels are being applied?
  - Other?

CUI FAR Case

- The new estimated comment period for the CUI FAR case is October 2020 to December 2020.
- FDP does not submit comments, but what are other ways we can collaborate to prepare for the final CUI clause?

Data Transfer and Use Agreement (DTUA) Updates

- Documents recently posted to the website:
  - COVID-19 DTUA Sample
  - Sample DTUA Intake Checklist
  - Reciprocal DTUA Template
  - Collaborative DTUA Sample

New Template and Sample!

Walk through of new Reciprocal DTUA Template and Collaborative DTUA Sample

DTUA – next steps

- Update DTUA FAQs and guidance to reflect information on new Reciprocal DTUA Template and Collaborative DTUA Sample.
- Other suggestions for items to add to the work plan?

Suggestions or willing to volunteer?

Contact Us!

Alexandra Albinak
Johns Hopkins University
amckeow1@jhu.edu

Martha Davis
Brandeis University
mrdavis@brandeis.edu

Melissa Korf
Harvard Medical School
Melissa_Korf@hms.harvard.edu