NDAA Section 889: Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment

Judy Faubert
Associate University Counsel

Brian Collier
Assistant Director of Research Administration, OSR

8th Annual Symposium for Research Administrators

November 10, 2020

UNC SYMPOSIUM for RESEARCH ADMINISTRATORS 2020

Background

U.S. government is taking deliberate steps to address risk to academic freedom and research security presented by foreign state actors

- "According to the National Counterintelligence and Security Center and the 2019 Worldwide Threat Assessment of the Intelligence Community, Chinese intelligence and security services may use Chinese information technology firms and their equipment as routine and systemic espionage platforms" (GSA NDAA Section 889 7.30.2020 presentation)
- "The increasing reliance on foreign-owned or controlled equipment and services, and reliance on those that present national security concerns, creates vulnerabilities in U.S. supply chains" (GSA NDAA Section 889 7.30.2020 presentation)

Government has expressed concern in the areas:

- Theft of intellectual property
- Cyber-security attacks

Risk areas touch various units on campus, including but not limited to:

- IT (both central and unit-based)
- Office of Sponsored Research
- Export Control
- Procurement
- Global

Various UNC working groups tackling the myriad of federal regulatory changes/clarifications in response to inappropriate foreign influence

IT Security Related Regulations

NIST 800-53

- Often applies to federally-funded research projects
- 159 controls for security plus an additional 102 enhancements for security

NIST 800-171

- Often applies to federally-funded research projects
- Focus is on controlled unclassified information (CUI) and covered defense information (CDI)
- 110 controls for security

NIST 800-171B

- Under development; will add additional controls beyond NIST 800-171

Cybersecurity Maturity Model Certification (CMMC)

- Applies to DoD contracts
- Has five certification levels
- Effective November 2020 with phased in approach

Stricter requirements are being included in NC state contracts

Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment

The National Defense Authorization Act (NDAA) FY2019 implements new certification requirements for entities receiving federal funding.

Part A (Contract specific) – requires offeror to represent that it [ ] will, [ ] will not provide ***covered telecommunications equipment or services*** to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation.

- Government cannot obtain prohibited telecom
- Think of this as the "Scope of Work" clause
- Effective August 13, 2019

Part B (Entity-wide) – requires prime federal contractor to certify whether it [ ] does or [ ] does not use ***covered telecommunications equipment or services*** or use any equipment, system, or service that uses ***covered telecommunications equipment or services***

- Contractor cannot use prohibited telecom
- Includes components of equipment
- "Use" is defined as entity-wide; use does not have to be related to federal contract
- Effective August 13, 2020

Implemented through Federal Acquisition Regulations clauses in federal contracts (FAR 52.204-24, -25, -26) and requires annual certification

Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment

Uniform Guidance revisions apply to federal grants

2 CFR 200.216

- Recipients and subrecipients are prohibited from obligating or expending loan or grant funds to:
  (1) Procure or obtain;
  (2) Extend or renew a contract to procure or obtain; or
  (3) 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 critical technology as part of any system.

Federal agency interpretation of Uniform Guidance has varied

- OMB guidance interprets UG term as prohibiting Federal award recipients from using government funds to enter into contracts (or extend or renew contracts) with entities that use covered telecommunications equipment or services.
- OMB interpretation would apply the prohibition even if the contract is not intended to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services.
- OSR is monitoring the situation

Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment

"Covered telecommunications equipment or services" are telecommunications and/or video surveillance equipment or services produced by:

- Huawei Technologies Company;
- ZTE Corporation;
- Hytera Communications Corporation;
- Hangzhou Hikvision Digital Technology Company;
- Dahua Technology Company;
- any subsidiary or affiliate of the entities listed above; or
- any entity you have knowledge of that is owned or controlled by, or otherwise connected to, the government of the People's Republic of China.

Telecommunications is NOT defined in the rule

- UNC current working definition – Electronic transmission of voice, video, data, text, and images between equipment over any distance. There are two important exceptions:
  - *A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or*
  - *Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.*

Scope of "use" currently unclear

- Applies to all University activities performed domestically and internationally
- Does not apply to subcontractors unless they cause UNC to use covered equipment or services

UNC Working Group for NDAA 889 Compliance

A working group, consisting of representatives from multiple central offices, was formed to develop a comprehensive compliance plan to meet these new requirements.

OSR/SPO
Brian Collier
Sherry Whitaker

OUC
Judy Faubert
Sarah Schtakleff

ITS
Mark Johnson
John Mack
Danny Nguyen

Federal Affairs
Kelly Dockham
Roxana Boyd

UNC Global
Andrew Hunt

Procurement Services
Troy Morse
Janet Rupert

Three Part Compliance Plan

Phase 1 (TOP Priority) - Assessment of Current Landscape

- Review to inform how University responds to certification of whether it [ ] does or [ ] does not use *covered telecommunications equipment or services* or use any equipment, system, or service that uses ***covered telecommunications equipment or services***
- *Reasonably Inquiry* standard - **A reasonable inquiry is an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity**. A reasonable inquiry need not include an internal or third-party audit. This inquiry must cover business operations at all levels and across all business lines, because the Section 889 prohibition is not limited to covered telecommunications equipment used in connection with performance of a federal contract.

Phase 2 - Prevention/Remediation

- Develop tools/processes to ensure the University does not begin to use any (new/additional) covered telecommunications equipment or services (i.e., System additions/enhancements, policy changes)
- Develop process to off-line any identified in-scope equipment or services
  - Waiver request until removal complete or if removal not possible

Phase 3 - Oversight/Monitoring

Phase 1: Reasonable Inquiry Steps Taken

Implemented freeze on submission of federal contract proposals and acceptance of new federal contracts and contract amendments with required certifications (effective October 12, 2020)

Queried Connect Carolina for named entities in the definition of Covered telecommunications equipment or services, plus subsidiaries/affiliates (*in progress*)

- Deactivated one identified vendor

Screened the purchase order system to determine if any direct purchases have been made with restricted vendors (*complete*)

Phase 1: Reasonable Inquiry Steps Taken (cont.)

Qualtrics survey to UNC-CH global sites (*in progress*)

- Identified stakeholders through review of UNC/LLC registrations, Ramses project search, working knowledge (9 groups)
- Presentation to University administers and faculty with significant global presence
- Reviewing telecommunications use at UNC global locations; whether use is through agreement of the University or LLC

Soliciting certification statements from telecommunications vendors to UNC-CH (*in progress*)

- Initial outreach to vendors under central ITS management (40 to date)
- Request to unit-based IT personnel for unit telecommunications vendors (25 major units represented between ITS, ITEC and Athletics)
    - Presented to ITEC group and responded to follow-up for questions
- Review of FY20 vendor payments to isolate potential telecommunications providers

Phase 2: Prevention

Communication/Training

- Develop OVCR/OSR communication to research administrators and principal investigators on NDAA 889 requirements
- Develop training materials

Restrict direct procurement from named entities

- Coordinating with Visual Compliance to add covered entities to screening list
- Communicate expected use of Visual Compliance by campus p-card users
- Document current Visual Compliance process for Purchasing
- Require vendor certification in RFP process for telecom commodity vendors

Add Principal Investigator certifications

- NDAA 889 Part A contract specific certification (at time of proposal; confirmed at time of award)
- Uniform Guidance specific certification on limitation on the use of grant funds (at time of award)

Add subcontract and subaward flow-down terms for required flow-down FAR and Uniform Guidance clauses

Phase 2: Remediation

Develop standard process for reporting to sponsor when UNC use of covered equipment or services is identified:

- 1 business day to report
- 10 business days to report mitigation efforts
  - Assess risk level
  - Determine if covered equipment or services can be removed from use without loss of performance
  - If loss of performance expected, develop cost and timeline for replacement
  - If replacement isn't possible, develop plan for minimizing security risks involved with continuing to use the covered equipment or service
  - Request waiver (good only through August 13, 2022)
    - Includes compelling justification for the need for additional time
    - Includes all required details of covered equipment or services
    - Includes a phase-out plan or mitigation plan

Partner with unit-based personnel to obtain required information for disclosure to sponsor

Phase 3: Oversight/Monitoring

- Monitoring federal guidance/clarification on NDAA Section 889
- Annual survey to UNC global sites
- Maintain repository of vendor certification statements and make accessible to campus
- Assess certifications from in-scope vendors
  - Vendors identified during Phase 1 reasonable inquiry; expand as necessary
  - Determine best way to identify/flag new vendors
- Continued use of Visual Compliance for named entities
- Identify campus groups for annual training/reminder (i.e., ITEC, research administrators, unit-based finance)
- Determine means to review p-card purchases

How You Can Help

The heart of the UNC compliance plan will rely on centralized checks and balances. However, you play a vital role in keeping the University compliant.

- Review federal contract funding announcements for any mention of NDAA Section 889 language. Make a note of it in your IPF so that OSR and SPO staff give it careful review
- Review proposed scopes of work that contain deliverables that provide equipment (fabricated or purchased) or services to the government and make sure no covered items are included
- Help educate your campus unit purchasing staff about these requirements and do your best to make sure that no purchases involve covered equipment or services (remember, it can be covered even if it's bought from a third-party vendor). This includes p-card purchases.
- Work with your campus unit IT staff and Central IT staff to help when making purchasing decisions
- Monitor grant expenditures carefully and pre-plan to ensure that no purchases made involve covered equipment or services

Impact to University if out of Compliance

The impacts to UNC if we are out of compliance with these new regulations are serious. They include, but aren't limited to:

- Potential impact to our global operations
- Potential loss of Federal funds, which could impact non-research and research operations
- Potential lawsuit under the False Claims Act

Given what's potentially at stake, it's important that all members of the University help us stay compliant.

CONTACT / RESOURCES

Brian Collier, Assistant Director, Office of Sponsored Research, bcollier@email.unc.edu

Judy Faubert, Associate University Counsel, Office of University Counsel, faubert@email.unc.edu

Questions / Discussion