THE UNIVERSITY OF ARIZONA

Compliance Notice: This notice describes how to comply with federal laws and regulations regarding the Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment (Refence: The National Defense Authorization Act (NDAA) FY 2019, Section 889).

Date: April 1, 2021

Overview of NDAA FY2019, Section 889

Effective on August 13, 2020, the NDAA FY 2019, Section 889, prohibits federal agencies from entering, extending, or renewing contracts or awarding grants to universities that provide or use certain telecommunications and surveillance equipment or services which are owned, connected, or controlled by the People's Republic of China (PRC). To comply with Section 889, the University may not provide the government **or** use any equipment, system, or service that uses telecommunications or surveillance equipment or services as a "substantial or essential component of any system" or as "critical technology as part of any system" from the following companies/entities:

- Huawei Technologies Company
- Hangzhou Hikvision Technology Company
- Hytera Communications Corporation
- ZTE Corporation
- Dahua Technology Company
- Any subsidiary or affiliate of these **companies/entities**[1]

Actions

In order to comply with Section 889 and ensure the University remains eligible for research contracts and grants from a variety of federal agencies, University personnel will do the following:

1.	Not purchase or contract for equipment or services from any of the listed companies for use on UArizona's campus or research, work, or other activities (includes P-Card purchases).
2.	Not use any telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, from the listed companies.
3.	Notify department leadership immediately if any equipment or services provided by these companies is located/used in their work areas, labs, offices, classrooms, or other University spaces. Report prohibited equipment to their leadership and to export@arizona.edu.
4.	If faculty, researchers, or staff discover prohibited equipment/services during the course of federal contract or grant performance, they must also notify Sponsored Projects & Contracting Services (SPCS) and Department leadership, immediately.
5.	Department leadership will immediately remove/dispose of the following equipment from the listed companies: network servers, network switches, routers, hotspots, surveillance cameras and similar equipment or services as well as equipment or services that store substantial amounts of data.
6.	Conduct due diligence to ensure subcontractors, subrecipients, vendors, and other entities are not providing prohibited equipment/services.
7.	Not accept gifts or transfer equipment to the University without reviewing the acquisition source.

[1] All restricted companies are maintained in the Visual Compliance Restricted Party Screening Tool and on the Export Control website.

Section 889 is implemented in FAR 52.204-24 and 52.204-25

FAR 52.204-24 (**Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment):** This requires federal contractors to submit a representation with their proposal identifying any covered telecommunications equipment or services that will be provided under the contract. If a contractor provides covered telecommunications equipment or services, the contractor must identify the equipment or services and describe the proposed use under the contract. The federal agency will then determine if the equipment or service is substantial or essential. In rare instances, if the hardware is essential, the government may receive a limited one-time waiver.

FAR 52.204-25 (**Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment):** This disallows the federal government from contracting with entities that **use** "covered telecommunications equipment or services" as a substantial or essential component of any system or "covered telecommunications equipment or services" as "critical technology" as part of any system.

Frequently Asked Questions:

- **My department/office/lab is not funded by a federal contract or grant; can we use prohibited equipment/services?** No, the law does not include an exception. Your department/office/lab can**not** continue to use prohibited equipment/services.

- **What is the definition of prohibited equipment/services?** Telecommunications or surveillance equipment or services from the companies listed above or their subsidiaries, which are a substantial or essential component or as critical technology as part of any system.

- **My department identified prohibited equipment that we need replaced; how do we get a replacement?** If equipment must be replaced, work with department leadership to replace required items. ***The department cannot charge a sponsored project twice for the same item.*** If required items cannot be funded by the department, consult with RII for funding options.

- **I have a personal cell phone or laptop from one of the companies listed; can I use it?** Yes, the law does not preclude using a personal device for personal use.

- **What if I do University work on my personal device?** It is a best practice not to use any devices from listed companies for any University work, including research.

- **What should I do if I am unsure if I have a prohibited device?** Contact your department leadership and **export@arizona.edu**.

- **Where can I get more information about these restrictions?** Full text of the statute and the notice of the regulation provide more details.

Direct Questions to:

- **Department specific actions and disposal questions:** department leadership.
- **Contract and grant questions:** SPCS at contracting@arizona.edu.
- **General compliance questions:** Export Control at export@arizona.edu.

Reference: Federal government flyer on Section 889 for additional guidance.