

UNIVERSITY COMPLIANCE NOTICE

University Compliance Notices provide actionable guidance and general education on University compliance requirements. All employees are responsible for complying with this Notice.

Subject: Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 Prohibition on the purchase or use of Certain Covered Telecommunications or Video Surveillance Equipment, Systems, or Services.

Purpose: This Compliance Notice describes how the University is complying with, and how employees are required to comply with, University policies and federal laws and regulations relating to Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019, Prohibition on Certain Covered Telecommunications or Video Surveillance Equipment, Systems, or Services.

Background: In response to increased U.S. Government security risk, the federal government recently implemented Section 889 of the National Defense Authorization Act for FY 2019, Pub. L. No. 115-232 (NDAA). Section 889 prohibits government contractors, grant recipients, and others from **procuring** or **using** certain telecommunications or video surveillance equipment, systems, or services (“Prohibited Items”).

Additionally, Section 889 prohibits the federal government from entering into, extending, or renewing contracts with any entity that **uses** any Prohibited Items, **regardless** of whether such Prohibited Items are used in performance of work under a federal contract, grant, or cooperation agreement.

The federal government has implemented Section 889 through the Federal Acquisition Regulations (federal contracts)¹ and Uniform Guidance (federal grants and cooperative agreements).²

Definitions: For purposes of this Compliance Notice, the following definitions apply.

“Prohibited Items” are defined as any IT System produced or provided by any of the following entities:³

- Huawei Technologies Company;
- ZTE Corporation;
- Hytera Communications Corporation;
- Hangzhou Hikvision Digital Technology Company;
- Dahua Technology Company;
- Any subsidiary or affiliated of the entities listed above; or
- Any entity owned or controlled by or connected to the government of the People’s Republic of China (PRC)
- Any entity added to this list by the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the FBI

“IT System” is defined as any equipment or device that can store, process, or transmit electronic WSU data that is owned, rented, or leased by WSU, or consumed as a thirty-party service by WSU. This includes, but is not limited to, servers, personal computing devices, applications, printers, networks and networking equipment (virtual, wired, and wireless), supervisory control and data acquisition systems, building control systems, phones and cell phones, tablets, embedded computers, transmission lines, video surveillance equipment, radio equipment, routers, modems, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by WSU.

What this means for WSU: Given its status as a federal contractor and federal grant recipient, WSU and its personnel are now prohibited from procuring and/or using any of the Prohibited Items. This prohibition applies to all campuses and all WSU work and/or activities including but not limited to teaching and research.

¹ FAR 52.204-24; 52.204-25; 52.204-26.

² 2 CFR 200.216

³ Please note: this list is frequently updated and subject to change.

To ensure it is fulfilling its obligations under Section 889, the University has adopted a three-phase compliance plan:

1. Phase 1 – Assessment
 - a. Create a working group comprised of representatives from a cross section of the University
 - b. Conduct a “reasonable inquiry” to determine whether WSU is currently using any Prohibited Items
2. Phase 2 – Prevention/Remediation
 - a. If necessary, terminate, disable, and/or remove from service any Prohibited Items
 - b. If Prohibited Items are not able to be terminated/disabled/removed, request a waiver from the federal government to continue use (even temporarily) of the Prohibited Items
 - c. Develop policies, procedures, and processes to ensure that the University does not begin to use any new and/or additional Prohibited Items (e.g., update P-Card training, implement vendor restrictions to prevent payments to or contracts with covered entities, flow down the Applicable Rules in all agreements (if applicable), etc.).
3. Phase 3 – Oversight/Monitoring
 - a. Monitor federal guidance and/or clarification on Section 889
 - b. Maintain a central repository of vendor certification statements
 - c. Determine means to review P-Card purchases

What should I do right now? To assist WSU with its Section 889 compliance requirements, and to ensure that the University (and its personnel) remain eligible for research contracts and grants from a variety of federal agencies, the University is requiring all faculty, staff, and administrators to be aware of and comply with these restrictions. This means that:

1. Employees are prohibited from purchasing, contracting for, or using Prohibited Items on any of WSU’s campuses and/or for use related to WSU work or activities, including but not limited to teaching and research.
2. Employees must notify InfoSec (askinfosec@wichita.edu) **and** their [Designated Departmental IT](#) contact immediately if any Prohibited Items are located/used in their work areas, laboratories, offices, classrooms, or other University spaces.
3. Employees working on or under a federal contract or grant must immediately notify the Office of Research if they discover any Prohibited Items during the course of federal contract or grant performance (note: this is in addition to notifying InfoSec and their Designated Department IT contact).
4. Employees must work with their Designated Departmental IT contact should they need to purchase **any** telecommunications or video surveillance equipment, systems, or services.
5. All offices that negotiate, review, or manage federal contracts and/or grants must conduct due diligence to ensure that subcontractors, subrecipients, vendors, and other entities are not providing and/or using Prohibited Items.
6. All employees must reach out to the Office of General Counsel immediately if they receive a request to certify to the University’s Section 889 compliance. Employees should **not** contact the external party until further instructed by the Office of General Counsel.
7. All employees must notify the Office of General Counsel immediately if they have made any type of certification and/or representation on behalf of WSU regarding the University’s Section 889 compliance.

Additional Information: For more information, and to see a list of Section 889 FAQs, please visit <http://www.wichita.edu/889faq>

Questions: Should you have questions regarding existing telecommunications or video surveillance equipment, systems, or services, or should you need to purchase new telecommunications or video surveillance equipment, systems, or services, please immediately contact you [Designated Departmental IT](#) contact.