

University of Rochester Certification of Compliance Form - FAR Clause 52.240-91

Directions: You should read this document in its entirety. When completed, please sign and return this document to your ORPA Research Administrator.

By signing this Certification of Compliance Form (this “Certification”), I hereby certify to the following:

1. I have been provided with a copy of FAR Clause 52.240-91 “Security Prohibitions and Exclusions” (the “FAR Clause”). The FAR Clause is attached to this Certification as Exhibit A.
2. I have reviewed the University’s TikTok and ByteDance Prohibition Guidance (the “Prohibition Guidance”). The Prohibition Guidance is attached as Exhibit B.
3. I have reviewed the FAR Clause and understand that I and all other individuals working on the federal contract for which I am Principal Investigator must comply with its requirements, including those who are added to the contract in the future.
4. I have reviewed the terms of the Prohibition Guidance and understand that I and all other individuals working on the federal contract for which I am Principal Investigator must comply with its requirements, including those who are added to the contract in the future.
5. I have provided copies of the FAR Clause and Prohibition Notice to all individuals working on the federal contract for which I am Principal Investigator, and will provide copies of the FAR Clause and the Prohibition Guidance to individuals added to the contract in the future.
6. I have provided written notification (email acceptable) to all individuals working on the federal contract for which I am Principal Investigator that if they have previously had or used TikTok or any successor application or service developed or provided by ByteDance Limited on any information technology equipment or system used under a University of Rochester (the “University”) federal contract, whether the information technology equipment is issued by the University or is personally owned by them, that they are required to remove such application(s) on or before the date of this Certification. I will provide this same notification to those who are added to the contract in the future.
7. I have provided written notification (email acceptable) to all individuals working on the federal contract for which I am Principal Investigator that they may not have or use TikTok or any successor application or service developed or provided by ByteDance Limited on any information technology equipment or system used under a University federal contract, whether the information technology equipment is issued by the University or is personally owned by them.

Name (Print): _____

Signature: _____

Date: _____

Exhibit A

(see attached)

52.240-91 Security Prohibitions and Exclusions.

As prescribed in 40.205(b), insert the following clause:

SECURITY PROHIBITIONS AND EXCLUSIONS (DEVIATION DATE)

(a) *Definitions.* As used in this clause—

American Security Drone Act-covered foreign entity means an entity included on a list that the Federal Acquisition Security Council (FASC) develops and maintains and publishes in the System for Award Management (SAM) at <https://www.sam.gov> (section 1822 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.).

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered application means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

Covered article, as defined in 41 U.S.C. 4713(k), means:

- (1) Information technology, as defined in 40 U.S.C. 11101, including cloud computing services of all types;
- (2) Telecommunications equipment or telecommunications service, as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);
- (3) The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program (see 32 CFR part 2002); or
- (4) Hardware, systems, devices, software, or services that include embedded or incidental information technology.

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means—

- (1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

- (2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
- (3) Telecommunications or video surveillance services provided by such entities or using such equipment; or
- (4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means—

- (1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;
- (2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled—
 - (i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or
 - (ii) For reasons relating to regional stability or surreptitious listening;
- (3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);
- (4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);
- (5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

FASC-prohibited unmanned aircraft system means an unmanned aircraft system manufactured or assembled by an American Security Drone Act—covered foreign entity.

FASCSA order means any of the following orders issued under the Federal Acquisition Supply Chain Security Act (FASCSA) requiring removing covered articles from executive agency information systems or excluding one or more named sources or named covered articles from executive agency procurement actions, as described in 41 CFR 201-1.303(d) and (e):

(1) The Secretary of Homeland Security may issue FASCSA orders that apply to civilian agencies, to the extent not covered by paragraph (2) or (3) of this definition. This type of FASCSA order may be referred to as a Department of Homeland Security (DHS) FASCSA order.

(2) The Secretary of Defense may issue FASCSA orders that apply to the Department of Defense (DoD) and national security systems other than sensitive compartmented information systems. This type of FASCSA order may be referred to as a DoD FASCSA order.

(3) The Director of National Intelligence (DNI) may issue FASCSA orders that apply to the intelligence community and sensitive compartmented information systems, to the extent not covered by paragraph (2) of this definition. This type of FASCSA order may be referred to as a DNI FASCSA order.

Information technology, as defined in 40 U.S.C. 11101(6)—

(1) Means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—

(i) Of that equipment; or

(ii) Of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(2) Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be

controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but

(3) Does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

Intelligence community, as defined by 50 U.S.C. 3003(4), means the following—

- (1) The Office of the Director of National Intelligence;
- (2) The Central Intelligence Agency;
- (3) The National Security Agency;
- (4) The Defense Intelligence Agency;
- (5) The National Geospatial-Intelligence Agency;
- (6) The National Reconnaissance Office;
- (7) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs;
- (8) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy;
- (9) The Bureau of Intelligence and Research of the Department of State;
- (10) The Office of Intelligence and Analysis of the Department of the Treasury;
- (11) The Office of Intelligence and Analysis of the Department of Homeland Security; or
- (12) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connecting a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Kaspersky Lab-covered article means any hardware, software, or service that—

- (1) Is developed or provided by a Kaspersky Lab-covered entity;
- (2) Includes any hardware, software, or service developed or provided in whole or in part by a Kaspersky Lab-covered entity; or
- (3) Contains components using any hardware or software developed in whole or in part by a Kaspersky Lab-covered entity.

Kaspersky Lab-covered entity means—

- (1) Kaspersky Lab;
- (2) Any successor entity to Kaspersky Lab, including any change in name, e.g., “Kaspersky”;
- (3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
- (4) Any entity of which Kaspersky Lab has a majority ownership.

National security system, as defined in 44 U.S.C. 3552, means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

- (1) The function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or
- (2) Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Sensitive compartmented information means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.

Sensitive compartmented information system means a national security system authorized to process or store sensitive compartmented information.

Source means a non-Federal supplier, or potential supplier, of products or services, at any tier.

Subsidiary means an entity in which more than 50 percent of the entity is owned directly by a parent corporation or through another subsidiary of a parent corporation.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

Unmanned aircraft means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft (49 U.S.C. 44801(11)).

Unmanned aircraft system means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system (49 U.S.C. 44801(12)).

(b) *Prohibitions on providing or using specific products or services in performance of contract.* Unless a waiver or exception applies, the Contractor is prohibited from providing any products or services to the Government or using in the performance of the contract any of the following:

(1) A covered application on any information technology owned or managed by the Government, or on any information technology used or provided by the Contractor under this contract, including equipment provided by the Contractor's employees (section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328));

(2) A Kaspersky Lab-covered article (Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91));

(3) Covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system (paragraphs (a)(1)(A) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232)). This does not prohibit contractors from providing—

(i) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) Prohibition on unmanned aircraft systems manufactured or assembled by American Security Drone Act—covered foreign entities.

(1) Prohibition. The Contractor is prohibited from—

(i) Delivering any FASC-prohibited unmanned aircraft system, which includes unmanned aircraft (i.e., drones) and associated elements (sections 1823 and 1826 of American Security Drone Act of 2023, within the National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, Div. A, Title XVIII, Subtitle B, 41 U.S.C. 3901 note prec.);

(ii) On or after December 22, 2025, operating a FASC-prohibited unmanned aircraft system in the performance of the contract (section 1824 of Pub. L. 118-31); and

(iii) On or after December 22, 2025, using Federal funds to procure or operate a FASC-prohibited unmanned aircraft system (section 1825 of Pub. L. 118-31).

(2) *Procedures.* The Contractor shall search SAM for the FASC-maintained list of American Security Drone Act—covered foreign entities before proposing, or using in performance of the contract, any unmanned aircraft system. Also, the Contractor shall ensure any effort or expenditure associated with a FASC-prohibited unmanned aircraft system is consistent with a corresponding exemption, exception, or waiver determination expressly stated in the contract.

(3) *Exemptions, exceptions, and waivers.* The prohibitions in paragraph (c) of this clause do not apply where the agency has determined an exemption, exception, or waiver applies, and the contract indicates that such a determination has been made. See sections 1823 through 1825 and 1832 of Public Law 118-31 for statutory requirements pertaining to exemptions, exceptions, and waivers.

(d) *Prohibition on using or providing specific products or services or conducting certain transactions regardless of connection to contract.*

(1) *Certain telecommunications and video surveillance equipment, systems, or services.*

(i) Unless an applicable waiver has been issued by the Government, the Contractor cannot use any equipment, systems, or services 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 (paragraph (a)(1)(B) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232)).

(ii) This prohibition applies to using covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. This does not prohibit the contractor from using—

(A) A service that connects to the facilities of a third party, such as backhaul, roaming, or interconnection arrangements; or

(B) Telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(2) Office of Foreign Assets Control Restrictions.

(i) Except as authorized by the Office of Foreign Assets Control (OFAC) in the Department of the Treasury, the Contractor shall not acquire, for use in the performance of this contract, any supplies or services if any proclamation, Executive order, or statute administered by OFAC, or if OFAC's implementing regulations at 31 CFR chapter V, would prohibit such a transaction by a person subject to the jurisdiction of the United States.

(ii) Except as authorized by OFAC, most transactions involving Cuba, Iran, and Sudan are prohibited, as are most imports from Burma or North Korea, into the United States or its outlying areas.

(A) For lists of entities and individuals subject to economic sanctions, see OFAC's List of Specially Designated Nationals and Blocked Persons at <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>.

(B) For more information about these restrictions, as well as updates, see OFAC's regulations at 31 CFR chapter V and at <https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information>.

(C) To conduct electronic screens of potential parties to regulated transactions, see the consolidated screening list at <https://www.trade.gov/consolidated-screening-list>, which consolidates multiple export screening lists of the Departments of Commerce, State, and the Treasury.

(3) *Sudan prohibition.* The Contractor is prohibited from conducting any restricted business operations in Sudan in accordance with Accountability and Divestment Act of 2007 (Pub. L. 110-174).

(4) *Iran prohibitions.*

(i) Unless an exception applies according to paragraph (d)(4)(iii) or the Government grants a waiver, the contractor shall not engage in certain activities or transactions relating to Iran (section 6(b)(1)(A) of Iran Sanctions Act (50 U.S.C. 1701 note)).

(ii) Unless an exception applies according to paragraph (d)(4)(iii) or the Government grants a waiver, contractor shall not export certain sensitive technology to Iran, as determined by the President, and has an active exclusion in SAM (22 U.S.C. 8515).

(iii) The prohibition in paragraphs (d)(4)(i) and (d)(4)(ii) do not apply if the acquisition is subject to trade agreements and the offeror certifies that all the offered products are designated country end products or designated country construction material (see part 25).

(iv) Unless an exception applies or the Government grants a waiver, contractors are prohibited from knowingly engaging in any significant transaction (i.e., over \$15,000) with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked according to the International Emergency Economic Powers Act (section 6(b)(1)(B) of Iran Sanctions Act (50 U.S.C. 1701 note)).

(e) *Governmentwide exclusion and removal orders.*

(1) Unless the Government has issued an applicable waiver, contractors shall not provide or use as part of the performance of the contract any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by an applicable FASCSA order as follows:

(i) For solicitations and contracts awarded by a Department of Defense contracting office, DoD FASCSA orders apply.

(ii) For all other solicitations and contracts, DHS FASCSA orders apply.

(2) The Contractor shall search for the phrase "FASCSA order" in the System for Award Management (SAM) at <https://www.sam.gov> to locate applicable FASCSA orders.

(3) The Government may identify in the solicitation other FASCSA orders that are not in SAM, which are effective and apply to the solicitation and resulting contract.

(4) A FASCSA order issued after the date of solicitation applies to this contract only if added by an amendment to the solicitation or modification to the contract (see FAR 40.204-1(c)).

(f) *Reasonable inquiry.* The contractor shall conduct a reasonable inquiry to determine if there are any prohibited products or services. The inquiry will look at any information in the entity's possession but does not need to include an internal or third-party audit.

(g) *Removal of prohibited products and services.* For Federal Supply Schedules, Governmentwide acquisition contracts, multi-agency contracts or any other procurement instrument intended for use by multiple agencies, upon notification from the Contracting Officer, during the performance of the contract, the Contractor shall promptly make any necessary changes or modifications to remove any product or service produced or provided by a source that this clause prohibits.

(h) *General report.*

(1) If the Contractor identifies or is notified by any source, (including a subcontractor at any tier), that any product or service provided or used (or to be provided or used) during contract performance does not comply with any prohibition in this clause, then the Contractor shall report the following information, or as much information is known, in writing to the contracting office as identified in paragraph (h)(2) within 72 hours:

(i) Contract number and order number, if applicable;

(ii) The specific prohibition the product or service is not complying with;

(iii) A description of the products or services that the Contractor identifies or has reason to suspect is prohibited (include brand; model number, such as the original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

(iv) The entity that produced the product or service (include entity name, unique entity identifier, Contractor and Government Entity (CAGE) code, facilities responsible for design, fabrication, assembly, packaging, and test of the product, and whether the entity was the OEM or a distributor (provide manufacturer codes and distributor codes used for the product));

(v) Description of the functionality of the product or service and how that functionality impacts the risk to the product or service;

(vi) An explanation of any factors relevant to determining if the product or service should be permitted by an applicable exception, exemption, or waiver (if the contractor would like the Government to consider a waiver, and asks for such a waiver);

(vii) Whether alternative products or services are available that would comply with the prohibition;

(viii) If the product or service is related to item maintenance, include the following information on the item being maintained:

(A) Brand;

(B) Model number, OEM number, manufacturer part number, or wholesaler number; and

(C) Item description, as applicable.

(ix) Any readily available information about mitigation actions implemented or recommended.

(2) If a report must be submitted to a contracting office, the Contractor shall submit the report as follows:

(i) If a Department of Defense contracting office, the Contractor shall report to the website at <https://dibnet.dod.mil>.

(ii) For all other contracting offices, the Contractor shall report to the Contracting Officer.

(iii) For indefinite delivery contracts, the Contractor shall report to both the contracting office for the indefinite delivery contract and the contracting office for any affected order.

(3) If the report provided does not contain any of the information required by paragraph (h)(1) of this clause, and the contractor later discovers new information that is required by paragraph (h)(1) of this clause, then the contractor shall submit a subsequent report within 72 hours of discovering the new information.

(4) The contractor shall also report the information in paragraph (h)(1) if the contractor wishes to ask for a waiver of the requirements of a new FASCSA order being applied through modification.

(i) *New FASCSA orders report.*

(1) During contract performance, the Contractor shall review SAM at least once every three months, or as advised by the Contracting Officer, to check for covered articles subject to FASCSA order(s), or for products or services produced by a source subject to FASCSA order(s) not currently identified under paragraph (e) of this clause.

(2) If the Contractor identifies a new FASCSA order(s) that could impact their supply chain, then the Contractor shall conduct a reasonable inquiry to identify whether a covered article or product or service produced or provided by a source subject to the FASCSA order(s) was provided to the Government or used during contract performance. The inquiry will look at any information in the entity's possession but does not need to include an internal or third-party audit.

(3) The Contractor shall submit a report to the contracting office identified in paragraph (h)(2) of this clause if the Contractor identifies, including through any notification by a subcontractor at any tier, that a covered article or product or service produced or provided by a source was provided to the Government or used during contract performance and is subject to a FASCSA order(s). For indefinite delivery contracts, the Contractor shall report to both the contracting office for the indefinite delivery contract and the contracting office for any affected order. The Contractor shall report the following information within 72 hours for each covered article or each product or service produced or provided by a source, where the covered article or source is subject to a FASCSA order:

- (i) Contract number and order number, if applicable;
- (ii) Name of the covered article or source subject to a FASCSA order;
- (iii) The specific FASCSA order the product or service does not comply with;
- (iv) The elements of (h)(1)(iii) through (ix) of this clause.

(j) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (j) but excluding subparagraphs (d)(1) and (i)(1), in all subcontracts and other contractual instruments, including subcontracts for acquiring commercial products or commercial services.

(End of clause)

Alternate I (DATE XXXX). As prescribed in 40.205(b), substitute the following paragraph (e)(1) for paragraph (e)(1) of the basic clause:

(e) Governmentwide exclusion and removal orders.

(1) Contractors are prohibited from providing or using as part of the performance of the contract any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by any applicable FASCSA orders identified by the

checkbox(es) in this paragraph (e)(1). [*Contracting Officer must select either “yes” or “no” for each of the following types of FASCSA orders:*]

Yes ☐ No ☐ DHS FASCSA Order

Yes ☐ No ☐ DoD FASCSA Order

Yes ☐ No ☐ DNI FASCSA Order

Exhibit B

(see attached)

TikTok and ByteDance Prohibition Guidance

Updated August 7, 2026

This guidance is intended to ensure that the University of Rochester community is aware of the restrictions imposed by the Federal Acquisition Regulation (FAR) clause [52.240-91](#) as it relates to the use of TikTok or ByteDance Limited applications. This guidance applies only to requirements under the University's federal contracts, and does not apply to the University's federal grants.

General compliance responsibilities for the University of Rochester community

- Individuals are prohibited from having or using **TikTok** or any successor application or service by **ByteDance Limited** on any information technology equipment or system used under a federal contract that contains FAR clause 52.240-91, whether the information technology equipment is issued by the University or is personally owned.
- Principal investigators who are responsible for federal contracts that contain FAR clause 52.240-91 will be required to sign a certification addressing compliance with the clause.
- Individuals who have the TikTok application on a personally owned device (such as a computer or cell phone), and who use or intend to use such device in the performance of a federal contract that contains FAR clause 52.240-91, must immediately remove the TikTok application.
- Individuals who perform work under a federal contract and who use a mobile device that is fully managed by the University must contact the University IT Helpdesk (univithelp@rochester.edu, (585) 275-2000) or ISD Helpdesk; ISDHelpdesk@URMC.Rochester.edu, (585) 275-3200), who will assist you in removing and blocking covered applications from your mobile device.
- The University must flow down FAR clause 52.240-91 to its subcontractors under an applicable federal contract.
- Contact **Joe Doyle, Research Security Officer** (joe.doyle@rochester.edu) if you have general compliance questions regarding this FAR clause, and **Mark Baker, Information Security Officer – Research & Education** (mbaker30@ur.rochester.edu) if you have IT compliance questions.

Background

The U.S. Government originally issued an interim rule on June 2, 2023, titled Federal Acquisition Regulation: Prohibition on a ByteDance Covered Application” (the Interim Rule). The prohibitions included in the Interim Rule are now included in FAR clause 52.240-91.

A “covered application” under this FAR clause “...means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.”

+++++

Frequently Asked Questions:

1. Does this prohibition apply to employee owned devices that are used in performance of a federal contract?

Yes, the prohibition on covered applications on any information technology used or provided by the University under a contract includes equipment owned by University employees used in the performance of the contract.

2. If I have a personal device that has a covered application on it, may I continue to use it?

A personally owned device (such as a computer or cell phone) that is not used in the performance of the contract is not subject to the prohibition.

3. What should I do if I have a personally owned device with a covered application (such as TikTok) on it, and I use or intend to use such device in connection with a federal contract subject to this prohibition?

You are required to remove the covered application from your personal device if you will use or intend to use the device in connection with performing under a contract. Use of the device for performance under a federal contract includes (i) the direct performance of work required under the contract (such as research activity), or (ii) performing other work in support of the federal contract, such as accessing or sending email, messaging (including on Microsoft Teams, Slack or a similar service), voice calling, or text messaging.

4. How do I remove the TikTok application from my personally owned device?

Instructions on how to remove the TikTok application from devices can be found here: <https://tech.rochester.edu/news-item/tiktok-ban-for-any-federally-impacting-research/>.

5. Does this prohibition also apply to my federal grant(s)?

As stated above, the prohibition does not apply to federal grants at this time.

6. How do I know if my federal award is a contract or grant?

The majority of federal awards to the University are grants (i.e. assistance awards). Federal contracts and subcontracts are considered procurement awards and are governed by fairly onerous requirements and numerous FAR clauses. If you are unsure whether your federal award is a contract or a grant, contact your ORPA Research Administrator.

The University may update this guidance as additional information becomes available.

For additional compliance questions, please contact Joe Doyle and Mark Baker.