EDUCAUSE

August 1, 2023

Janet Fry
Deputy Director
Office of Government-wide
Acquisition Policy
General Services Administration
1800 F Street NW
Washington, DC 20405

RE: Comments in response to FAC 2023–04, FAR Case 2023–010, submitted electronically at https://www.regulations.gov/commenton/FAR-2023-0010-0001

Dear Deputy Director Fry:

On behalf of EDUCAUSE, I would like to thank you for the opportunity to provide input from the higher education cybersecurity community on Federal Acquisition Regulation (FAR) Case 2023-010, which discusses the interim rule establishing FAR 52.204–27, Prohibition on a ByteDance Covered Application. As the association for advancing higher education through information technology (IT), EDUCAUSE represents over 2,100 colleges, universities, and related organizations. Higher education IT leaders and professionals at all levels of the institution work together through EDUCAUSE to develop and strengthen the role of technology in helping higher education institutions to achieve their missions.

EDUCAUSE member representatives will be tasked with fulfilling the requirements of FAR 52.204-72 at institutions of higher education where the clause is applicable. Higher education institutions must maintain unique technology environments that span academic and administrative functions, including the research activities to which FAR requirements often apply. Colleges and universities take the compliance obligations arising from FAR clauses such as 52.204-72 very seriously and strive to meet them while continuing to facilitate teaching and learning, service, and other core higher education activities. The EDUCAUSE community thus has great interest in seeing the clause clarified and, in some areas, revised in ways that will allow affected colleges and universities to comply effectively. EDUCAUSE makes the following requests and recommendations with this essential balance in mind.

Definition of "Covered Application"

The interim rule defines "covered application" as "the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity

4845 Pearl East Circle, Suite 118, PMB 43761, Boulder, CO 80301-6112
Main 303-449-4430 / **Fax** 303-440-0461

owned by ByteDance Limited."[1] As currently written, the interim rule does not provide further scope around what may constitute a "successor application or service." As one member institution explained to its researchers,[2] the ByteDance portfolio contains at least eleven (11) different applications whose identifiers, network addresses and other actionable attributes may change over time. EDUCAUSE asks that the final rule state explicitly whether the scope of "successor application or service" is specifically limited to TikTok and any of its future iterations or alternatives, or whether the term should be understood as encompassing all ByteDance applications or services, both current and future.

Expected Impact of the Rule

The Federal Register notice discussing the anticipated impact of the rule asserts the following: "The changes made in this rule are less complex than other prohibitions that have been incorporated into the FAR, such as the prohibition on contracting for certain telecommunications and video surveillance services or equipment, which requires reviewing a contractor's supply chain to uncover any prohibited equipment or services."[3] However, EDUCAUSE members believe that a thorough "on the ground" evaluation of the actual effects of the rule's provisions will be necessary in order for the regulated community and relevant federal agencies to effectively understand the complexities of complying with the rule. Therefore, the final rule should be clearer about what it intends covered entities to bar and how the federal government will provide the information at the rule's implementation, and consistently over time, that covered entities will need to ensure compliance. Such information would include, for example, key identifiers that would enable the accurate development and dissemination of compliance guidance to institutional stakeholders via institutional policy as well as the accurate application of technical measures when specifically warranted. With this in mind, the final rule should also much more clearly allow for the use of policy-based compliance measures as compared to technology-based measures, which is consistent with federal compliance requirements in other relevant contexts.

Following from the previous point, EDUCAUSE would call attention to this sentence regarding the rule's anticipated regulatory impact: "It is expected that contractors already have technology in place to block access to unwanted or nefarious websites, prevent the download of prohibited applications (apps) to devices, and remove a downloaded app."[4] This statement does not necessarily reflect the complexity of research university network and device support operations. In addition, as noted above, federal regulations have explicitly allowed for the use

[1] Department of Defense, General Services Administration, and National Aeronautics and Space Administration, "48 CFR Chapter 1 [Docket No. FAR–2023–0051, Sequence No. 3], Federal Acquisition Regulation; Federal Acquisition Circular 2023–04; Introduction," *Federal Register*, Vol. 88, No. 106, June 2, 2023, p. 36433.
[2] "ByteDance/TikTok Memorandum: Implementation of FAR 52.204-27," Office of Research and Creative Achievement and Department of Information Technology, University of Maryland, Baltimore County, June 16, 2023.
[3] Department of Defense, et al, "48 CFR Chapter 1 [Docket No. FAR–2023–0051, Sequence No. 3] …," *Federal Register*, Vol. 88, No. 106, June 2, 2023, p. 36432.
[4] Ibid.

of policy-based controls to fulfill compliance obligations stemming from similar regulations, but this statement implies that affected organizations *must* deploy technology-based controls in order to comply with the rule's provisions. If that is the intent behind the rule, then it should be clearly stated in the text, rather than being left to implication. The effects of such a mandate on the complexities that the rule raises for compliance by covered entities, as well as the information and resources that federal agencies will need to provide to enable accurate compliance, will also have to be assessed in much greater detail. EDUCAUSE members firmly believe, however, that the statement should be omitted as compliance can be effectively achieved without the mandated use of technology-based controls. The final rule should include text that makes clear that affected entities have discretion in determining how best to meet their compliance obligations while satisfying other business objectives.

Finally, the regulatory impact section includes the following statement: "It will be particularly important for contractors to clearly explain to their employees when a covered application is prohibited on a personal device used in performance of a Federal contract."[5] EDUCAUSE finds that the rule's definition of "information technology," which excludes "equipment acquired by a Federal contractor *incidental* [emphasis added] to a Federal contract,"[6] combined with a lack of a definition of "performance" as used in the statement, makes providing employees with such an explanation especially difficult. Our members are concerned that faculty, staff, and students working on a covered project will be confused about whether they can read an email or have a phone call in which information related to the project is discussed on a personal device that has a prohibited application installed on it, given that the scope of what constitutes "performance of a Federal contract" in this context is unclear and use of the device in question might be considered "incidental." Prohibiting the use of personal devices for quick tasks that don't entail substantive project information will undermine researchers, staff, and students in their efforts to conduct covered projects efficiently and effectively, leading to longer project timelines and higher costs. With this in mind, EDUCAUSE requests that the final rule provide a practical description of what constitutes "incidental" equipment in this context, and that this description encourage efficient performance without creating undue risk. For example, rather than attempting to regulate personal devices, a focus on implementing effective access control should be sufficient to address the underlying concern. The final rule should also define the "performance" threshold that would trigger an actual prohibition on the use of a device with a covered application installed on it.

Definition of "Information Technology"

The definition of "information technology" and the scope of the technology environment it may cover leads to particularly thorny questions in the higher education context given the reference to "any equipment or interconnected system or subsystem…, used in the automatic… management, movement, control, …, switching, interchange, transmission, or reception of data

[5] Ibid.

[6] Ibid, pp. 36433 and 36434.

or information…."[7] As previously noted, the IT infrastructure of a college or university supports multiple purposes beyond covered research; this is especially the case for institutions with residential campuses. Would the "information technology" covered by the rule include an institution's general purpose network, such that TikTok data traffic must be barred from the college or university network entirely because the same underlying infrastructure is used to switch, interchange, transmit, and receive data, email, or other information related to covered projects? Higher education institutions simply could not afford to segregate their networks and cannot differentiate between encrypted data streams as such a determination would imply, nor would it be reasonably necessary to do so to address the compliance interests that the rule is intended to serve. EDUCAUSE asks that the rule be revised to explicitly exclude general purpose network infrastructure from its scope.

The issue of what constitutes "incidental" equipment arises again when considering the institution's general IT environment. Would a computer acquired for general productivity purposes (e.g., payroll services, standard administrative tasks) or instructional needs come into scope if it is subsequently used in relation to a covered project awarded at a later time? The final rule must provide much clearer, more specific guidance on what aspects of an institution's IT environment are excluded from its scope, who makes that determination, and how. General purpose devices and network infrastructure could be construed as "incidental" in a higher education setting. As a result, the exceedingly broad definition of "information technology" in the rule makes it difficult to understand where the line between covered and excluded technology should be drawn, as well as the extent to which the covered entity has the discretion to draw it.

Exception for "Security Research Activities" in OMB Memorandum M-23-13

The notice and rule text contain numerous references to Office of Management and Budget (OMB) Memorandum M-23-13, "'No TikTok on Government Devices' Implementation Guidance." EDUCAUSE members believe that the final rule will need to "fill in the gaps" in terms of how the "Security Research Activities" exception in M-23-13[8] may be applied in this context. To avoid confusion, the final rule should explicitly specify the scope of the research activities that may be excluded from the ban, and thus make clear whether such activities pertain to security research on TikTok specifically or to security research in general.

Conclusion

Again, higher education institutions and the federally funded research that they conduct present unique challenges for interpreting and complying with the rule as presented in its interim form. EDUCAUSE hopes that its comments provide useful indicators of where modest clarifications or revisions in the final rule may substantially mitigate those challenges. If our

[7] Ibid.

[8] Shalanda D. Young, "'No TikTok on Government Devices' Implementation Guidance," Memorandum M-23-13, Office of Management and Budget, Executive Office of the President, February 27, 2023, p. 4.

members can assist further in resolving the issues discussed above, please contact me at your earliest convenience. EDUCAUSE would be happy to work with you and/or other federal agency representatives to facilitate such efforts.

Please also note that EDUCAUSE enjoys the support of COGR (cogr.edu) in submitting these comments and would be happy to have COGR members and staff participate with us in discussion sessions on this topic. COGR is an association of over 200 public and private U.S. research universities and affiliated academic medical centers and research institutes. It focuses on the impact of federal regulations, policies, and practices on the performance of research conducted at COGR member institutions, and it advocates for sound, efficient, and effective regulation that safeguards research and minimizes administrative and cost burdens. EDUCAUSE and COGR have previously held joint discussions with federal government representatives on issues of shared interest and found that having the research and cybersecurity perspectives reflected in the same discussion can be highly productive.

Sincerely,

Jarret S. Cummings
Senior Advisor, Policy and
Government Relations
EDUCAUSE

cc: Krystal Toups, Director, Contracts & Grants Administration, COGR