THE COALITION FOR GOVERNMENT PROCUREMENT

1990 M Street, Suite 450
Washington, DC 20036

Phone: 202-331-0975
Fax: 202-822-9788

www.thecgp.org

Re: Federal Acquisition Regulation Interim Rule: Prohibition on a ByteDance Covered Application
FAC 2023-04
FAR Case 2023-010
Docket No. 2023-0010, Sequence No. 1

By this letter, the Coalition for Government Procurement ("the Coalition") conveys the comments of its members on the above referenced Interim Rule instituting a prohibition on a ByteDance Covered Application, which became effective on June 2, 2023. This Interim Rule amends the Federal Acquisition Regulation (FAR) to implement a ban on having or using TikTok or any successor application or service developed or provided by the company that made the application, ByteDance Limited, or an entity owned by ByteDance Limited ("covered application").

By way of background, the Coalition is a non-profit association of firms selling commercial services and products to the Federal Government. The association has over 300 member firms, 25% of which are small businesses. Its members collectively account for a significant percentage of the sales generated through General Services Administration contracts, including the Multiple Award Schedule program. Coalition members also are responsible for many of the commercial item solutions purchased annually by the Federal Government. The Coalition is proud to have collaborated with Government officials for over 40 years in promoting the mutual goal of common-sense acquisition.

The Coalition solicited feedback on the Interim Rule from its members. The submissions received are included in the attached matrix and organized by topic (*see* "Prohibition on a ByteDance Covered Application CGP Comment Matrix" attached below). Generally, member concerns fall under the following:

The breadth of technology addressed by the Interim Rule should be clarified: The Interim Rule prohibits the presence or use of any covered application on any information technology owned or managed by the Government, or on any information technology used or provided by the contractor under a contract, including equipment provided by the contractor's employees, unless an exception is granted in accordance with Office of Management and Budget (OMB) Memorandum M–23–13.[1] Under the rule, a "covered application," is "the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited." "Information technology," defined as set forth in 40 U.S.C. 11101(6), is:

[1] OMB Memorandum M–23–13 lays out limited exceptions that are permitted by the law for law enforcement, national security interests, and security research, but their use should be limited to situations that are critical to the agency mission and where no alternative is available.

> …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;
>
> [It i]ncludes 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
>
> [It d]oes not include any equipment acquired by a Federal contractor incidental to a Federal contract.

Given the inclusion of interconnected systems in the definition of information technology, guidance is needed to identify the bounds on use that is "significant" under a Federal contract or "incidental to a Federal contract." For instance, with messaging or emailing platforms ubiquitous within organizations, it is not clear whether application of the Interim Rule is limited to exchanges associated with the facilitation of work on a contract, or whether it extends to passive receiving (but not sending) contract-related emails or other communications, or to storage applications on a device that could access contract materials. This point represents a matter of significant concern for some members. For a discussion of this concern, please see Comment 16 in the matrix.

The extent to which the government seeks to have contractors address the presence of a covered application should be clarified in the Interim Rule: The prohibition of a covered application applies to "the presence or use of a covered application on information technology, including certain equipment used by Federal contractors." In discussing the rule's expected impact, the Interim Rule states that

> … changes made by this rule do require contractors to leverage existing technology, policies, and procedures already in place and update those to prohibit the presence or use of a covered application or the URLs associated with a covered application on devices used by a contractor under a contract with the Government. 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. Additionally, it is expected that contractors already have policies in place for employees to follow for workplace technology. It is recognized that these policies will need to be updated to include the prohibition on having or using a covered application, and that implementation of the prohibition may also require

> employee communications or training on this new requirement. 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.

Under the Interim Rule, it is not clear to what extent contractors are to address the passive presence of URLs via email, text, or otherwise. Likewise, it is unclear to what extent the government seeks to have contractors control search results where URLs may appear. To the extent that the government seeks to have contractors screen and segregate offending inbound employee correspondence and search results, it should be recognized that contractors may not have technology in place to screen and segregate in this manner, and thus, the requirement to do so likely will increase the cost of implementing the Interim Rule.

The Interim Rule should be clarified to identify the extent to which policy-based and/or technical solutions may allow Federal contractors to use information technology where TikTok is present in a system, but is segregated from those network elements where the Federal work is performed: In the commercial world, many businesses use a combination of technical systems and policies to allow business applications to run securely on personal devices, such as running within a secure container or on separate partitions. It is not clear whether any of these solutions are acceptable under the Interim Rule. Likewise, global enterprises may be networked to firewall operations geographically or by customer, and it is not clear whether those firewalling operations will comply under the Interim Rule.

The Interim Rule should be amended to account for the practical realities faced by some firms: Despite best efforts, some companies technically may not be capable of ensuring full compliance with the prohibition. Given the strong policy interest in sustaining a competitive industrial base, the government should consider identifying circumstances where risk levels permit it to require companies to establish and implement reasonable procedures towards compliance. By way of example, in the Anti-Kickback scenario, FAR 52.203-7 provides an example of what language may be used: "The Contractor shall have in place and follow reasonable procedures designed to prevent and detect possible violations of this clause in its own operations."

The FAR Council's assertion that the rule "is not expected to have a significant economic impact on businesses" may be incorrect: The FAR Council's evaluation of the rule's expected impact and complexity does not fully account for the rule's potential effects. Should the Interim Rule prompt the restriction or elimination of BYOD programs, it could reduce business efficiency and increase the cost of doing business. This cost is not accounted for in the Interim Rule and may represent a significant expense, especially for small and/or disadvantaged businesses.

In addition, because the rule requires contractors to flow down the requirement to subcontractors, even without official supply-chain review requirements, companies will experience analogous costs and challenges if they want to verify their subcontractors' compliance. Some subcontractors, of course, will not be willing or able to comply with the new requirement, leading to further costs for government and industry to find new subcontractors.

Finally, with respect to existing contracts, to the extent that the changes anticipated by the Interim Rule amount to cardinal changes not within the contemplation of the parties at the commencement of an

agreement, there may be need for bilateral contract modifications. The modifications will have cost implications for the programs involved.

The Interim Rule should institute implementation of the rule with a program of education: Understanding the FAR Council's intent and desired scope of the prohibition under the rule may reduce complexity and facilitate compliance. Therefore, it would be helpful for the Interim Rule to require the government to provide contractors with an understanding of its concerns with the application and the company involved, identifying the risks it has identified. This education, including FAQs and a summary of government implementation activities and best practices, would help contractors in their efforts to educate employees and suppliers, raising sensitivity and awareness.

The FAR Council should engage in further discussion with stakeholders in industry and government: Because the rule concerns cybersecurity and national security issues, we understand the decision to issue an Interim Rule and the urgency to establish a final rule. The ambiguities in the Interim Rule, however, create economic and compliance burdens for contractors, as well as administrative burdens for front-line personnel who must understand, discuss, and implement the rule. They also increase the risk that the rule will not be implemented effectively and fail to deliver the full cybersecurity benefits Congress anticipated. Consultation with all stakeholders in government and industry will allow the FAR Council to understand what clarifications are necessary to achieve the policy goals being sought under the rule.

The concerns highlighted herein are addressed more specifically in the attached anonymized member comments. The Coalition hopes you find them useful in your review. In the meantime, please do not hesitate to reach out to me if you would like to discuss our comments further or meet with our members by emailing rwaldron@thecgp.org or calling (202) 315-1051.

On behalf of our members, thank you again for your consideration of these comments.

Sincerely,

Roger Waldron
President

Prohibition on a ByteDance Covered Application CGP Comment Matrix

Number	Part	Topic	Comment
1	4.2201 Definitions	Scope of rule	Scope and Definition of "use of that equipment to a significant extent in the performance of a service or the furnishing of a product." Can the government please define and give an example of "use of equipment to a significant" extent?
2	4.2201 Definitions	Scope of rule	If a corporate wide ban is required, such that our network does not allow access, that may not cover the Guest or Cellular networks. It may not cover individual employees' phones who have the app installed if their access was not through the Corp network. Thus, the question is whether that [the network ban] is enough to comply with the broad rule because this is removed from any information technology essentially in some way involved in performance of the federal contract.
3	4.2201 Definitions	Scope of rule	With respect to the impact to workplace BYOD programs, we add our concerns about the significant financial impact to small businesses if the rule will, in effect, require workplaces to discontinue the BYOD program and issue devices to employees.
4	4.2201 Definitions	Scope of rule	What constitutes the employee engagement in this regard: For example, if we have someone simply entering orders, but they have email on their phone, would they be subject to this? I'm not sure how to clarify the level of "working" on contracts. We have a variety of departments that may "touch" as aspect of contracts such as IT (set up contracts in the system), Order Entry (enter purchase orders), Customer Care (answer questions on shipping, returns, products, etc.), Logistics (coordinating deliveries), etc. We also of course have several sales team members that may be involved in a government project, but that doesn't necessarily mean that confidential or specific information will come across their email as it may be more product based.
5	4.2201 Definitions	Scope of rule	TikTok servers were already blocked by our organization ahead of this rule taking effect. However, this is the first time a contractual requirement has extended coverage to employee-owned personal technology. As such, it was more challenging to manage user perception and change. We thought it best to re-examine our organization's Bring Your Own Device (BYOD) policy as a result of this change.

6	4.2201 Definitions	Scope of rule	Over the last decade, Apple has steadily taken steps to preserve user privacy. These privacy decisions have yielded an operating system privacy architecture that has substantially reduced the visibility, reach, and control of our mobile device management (MDM) software where a personally owned device is concerned. Implementation of this new requirement demonstrated that it is no longer possible for us to detect the presence of covered applications on personally owned Apple devices and have therefore fallen back to Rules of Behavior and other procedural controls.
7	4.2201 Definitions	Secure containers	We have employees that use their personal phones to check email, take calls and attend video conferences. Our technology runs in a secure container designed to keep the company apps and data separate from the apps and data on the phone. Is there any consideration being given to rewording this to allow for a logical separation on the device?
8	4.2201 Definitions	Secure containers	Will the Government give any consideration to technical solutions. Many companies allow personally owned cell phones (bring your own device) to use the company managed applications, which would be used in the support process, in a secured container that separates the employee's personal data from the company's information. This solution is more aligned with employment laws and freedom of choice, which our employees should be entitled to until a decision is made to outlaw TikTok.
9	4.2201 Definitions	Secure containers	A containerized environment is not unreasonable and would meet the requirement to keep TikTok separated. If the Government takes this ban to a certification requirement of policing employee devices this would place an unreasonable financial burden on federal contractors.
10	4.2201 Definitions	Secure containers	Will the government permit the use of Master Data Management (MDM) solutions to secure government data on personal devices used in the performance of government contracts that also access Tiktok?

11	4.2201 Definitions	Secure containers	If a cellphone is logically separated using software (e.g., Intune), will this logical separation suffice to adhere to the TikTok prohibition?
12	4.2201 Definitions	Secure containers	We're very concerned about the scope and what's considered "in performance of a contract." The BYOD piece of this is a huge piece of the puzzle. It's not clear from the write up if we're ok to have Tik Tok on the personal device if it's containerized in such a way that it's unable to touch any of the work-oriented apps/partition of the phone.
13	4.2201 Definitions	Are non-contracting employees exempt even on the same network?	If an employee who does not work on covered government contracts connects to the contractor's wifi on a device that includes TikTok, will that trigger a violation of the rule assuming that other employees who do perform on covered government contracts connect to the same wifi?
14	4.2201 Definitions	What is the technical standard for compliance?	Please provide information on an acceptable standard from a technical perspective to achieving compliance with the rule.
15	4.2201 Definitions	What is the technical standard for compliance?	We request additional information on the technical guidelines to comply with the rule. Specifically, is it sufficient for contractors to block the app via policy on personal devices that are enrolled in inTune? Are there other standards or guidelines that contractors should be aware of that would suffice?
16	52.204-27 (a) & (b)		Guidance is needed to identify the bounds of scope and definition of "used" and "use" under paragraphs (a) and (b) of 52.204-27 (*i.e.*, "or is used by the contractor under a contract with the executive agency that requires the use"; "or on any information technology used or provided by the Contractor under this contract") to clarify what use rises to the level of "significant" to a Federal contract as to warrant the prohibition of TikTok on subject devices, versus what use is only considered "incidental to a Federal contract." See FAR 52.204-27. Does the FAR Council intend "used" to mean: (i) information technology used in performance of the contract, or (ii) a more expansive approach that would include any information technology that is used, whether in performance of the contract or merely to facilitate Federal contract work, would be subject to the prohibition (*e.g.*, a contractor employee's BYOD mobile phone used to respond to an email from U.S. government (USG) contracting officer; a contractor server or internal data management platform used to receive a COTS order from a USG entity; a laptop used for a video teleconference with a USG employee)?

17	52.204–27 (c) Subcontracts.		We work with a network of authorized dealers. Since those dealers work on projects with us (almost as subcontractors) to support government purchasers, would this be expected to flow down to them? Since we don't employ them, how are we expected to enforce and monitor this?
18	IV. Expected Impact of the Rule	Does accessing a Tik Tok URL violate the new rule (is checking the URL equated to checking the app)?	Question/Comment: A device can be void of covered applications and still have the presence of a TikTok associated URL; can the government please clarify if the very presence of a TikTok associated URL is included in this prohibition? If TikTok associated URLs are prohibited, please describe the implications of this rule on BYOD programs and the acceptable protocol contractors should follow to comply.
19	IV. Expected Impact of the Rule	Does accessing a Tik Tok URL violate the new rule (is checking the URL equated to checking the app)?	Does the "use" of TikTok extend to situations where a Federal contractor receives a TikTok via text or other electronic communication. Specifically, if you have a personally owned cellphone that you use to check messages or communicate about the contract and you do not have the TikTok app downloaded, would you be considered non-compliant if a family member or friend texted you a TikTok video? If that sort of scenario would fall within the category of "using" TikTok, it would seem that the ban, as currently structured, would effectively require companies to provide employees that are connected with the contract with work phones to help ensure compliance. Otherwise, you are really at the whims of whoever your employee might communicate with in their personal lives. For companies who currently have bring your own device programs, especially small businesses, transitioning could be pretty costly to implement and maintain.
20	IV. Expected Impact of the Rule		With the increase in remote work, if an individual works remotely while providing services, and if a family member uses TikTok at the same location, will this run afoul of the prohibition?
21	IV. Expected Impact of the Rule		Since there is no timeline on when federal contractors are required to be compliant with the ByteDance Clause, please confirm a federal contractor may continue to contract with the U.S. Government if that federal contractor is diligently and continuously working towards compliance.

22	IV. Expected Impact of the Rule		One thing we would like to see the associations push hard on is the need for education. The Government doesn't do a lot to say why Tik Tok is bad. If the Govt could share an education campaign about the dangers of Tik Tok with industry, that would be helpful to us in educating our employees and suppliers without worrying about crossing lines ourselves. Likewise, if the Government could publish some FAQs or guidance on how they are implementing this internally on government employees' personal phones and/or best practices in implementation, that would also be helpful.
23	IV. Expected Impact of the Rule		We suggest an addition within the rule for a reasonable inquiry / effort clause similar to what is included in FAR 52.204-25 "Reasonable inquiry means 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 that excludes the need to include an internal or third-party audit." Companies can only do so much, block computers on their network from accessing certain websites and block devices from downloading applications. However, they have less control for blocking cell phones from visiting websites when browsing or control over folks' personal devices with regard to BYOD. 2) A reasonable inquiry / effort should be expected but the FAR should not punish companies for actions that are outside of their controls.
24	Supplementary Information		The interim rule states "a personally-owned cell phone that is not used in performance of the contract is not subject to the prohibition" (emphasis added). However, this standard is not included in the new FAR clause (i.e., 52.204-27). Does "in performance of the contract" have any bearing on whether contractor information technology is subject to the prohibition?