AMS/FAST CHANGE REQUEST (CR) COVERSHEET

Change Request Number: 23-98

Date Received: May 25, 2023

Title: Information and Communication Technology & No Tik Tok on Government Devices

---

Initiator Name: Dan DeNicuolo

Initiator Organization Name / Routing Code: Procurement Policy Branch, AAP-110

Initiator Phone: 856-889-6383

ASAG Member Name*:* Monica Rheinhardt

ASAG Member Phone*:* 202-267-1441

Policy and Guidance: (Please check only one box)

- ☐ Policy
- ☒ Guidance
- ☐ Procurement Samples
- ☐ Procurement Templates
- ☐ Procurement Forms
- ☐ Procurement Checklists
- ☐ Procurement Tools and Resources
- ☐ Real Property Templates and Samples
- ☐ Procurement Clauses
- ☐ Real Property Clauses
- ☐ Other Tools and Resources

Summary of Change:
This change continues an ongoing effort to consolidate all AMS procurement matters related to Information and Communication Technology (ICT) into Section T3.8.9. Existing AMS Guidance applicable to ICT is transferred to T3.8.9 and updated to implement the updated policy at AMS Policy 4.9. Also included in this change is the implementation of the No TikTok on Government Devices Act of the Consolidated Appropriations Act, 2023.

ICT-related topics transferred from existing Guidance sections and added to T3.8.9 as individual Subsections are as follows:
- Internet Protocol Version 6
- Positioning, Navigation and Timing Services
- Commercial Software Licensing Agreements
- Cloud Computing Services
- Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Section 889 of NDAA 2019)
- Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities

The following Subsection implements to AMS Guidance a new prohibition on Bytedance covered applications:
- Prohibition on Using Bytedance Covered Applications Including TikTok

Reason for Change:
Consolidation of ICT matters to a single AMS Guidance Section is purposed with improving FAA ICT acquisition effectiveness and security. Additionally FAA is implementing the No TikTok on Government Devices Act into AMS for national security purposes.

Development, Review, and Concurrence: AAP-110

Target Audience: FAA Acquisition Workforce

Briefing Planned: Yes.

ASAG Responsibilities: Review and comment. Present to the ASAG on June 20, 2023.

Section / Text Location:
AMS Procurement Policy & Guidance - Procurement Guidance Section T3.8.9

The redline version must be a comparison with the current published FAST version.

(•) I confirm I used the latest published version to create this change / redline

or

( ) This is new content

Links: https://fast.faa.gov/docs/procurementGuidance/guidanceT3.8.9.pdf

Attachments: Redline and final documents.

Other Files: N/A.

Redline(s): See below.

Section Revised: T3.8.9 – Information and Communication Technology

Procurement Guidance - (~~4/2023~~7/2023)

T3.8.9 Information and Communication Technology Added 4/2023

A Acquisition of Information and Communication Technology Added 4/2023

1 Section 508 of the Rehabilitation Act ~~Added 4/2023~~Revised 7/2023

~~a.~~ *Applicability*.

a. ~~(1) Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended in 1998,~~This subsection applies to all SIRs ~~and~~, contracts ~~for~~, orders and purchase card transactions which include the acquisition of Information and Communication Technology (ICT) made on or after June 21, 2001 with the exception of those procurements listed in ~~(d) *Exceptions*, below. In accordance with Section 508, ICT products and services must meet the applicable Access Board ICT Accessibility Standards and Section 508 requirements. Any ICT procured prior to June 21, 2001 is not required to be retrofitted. When procuring ICT, the procurement team must ensure:~~ paragraph c. *General*, subparagraph (3) *Exceptions*, below.

~~(i) applicable Section 508 technical standards are identified;~~

~~(ii) solicitations include references to the identified standards;~~

~~(iii) market research is performed to include consideration of Section 508 compliance;~~

~~(iv) selection of the product or service that meets business requirements and best meets Section 508 requirements is selected; the product or service that meets business requirements and Section 508 requirements is selected; and~~

~~(v) documentation is retained to demonstrate compliance with Section 508 requirements.~~

~~(1) (2) *Legacy ICT*. Any component or portion of existing ICT procured, maintained or used prior to January 18, 2018 is not required to comply with the most current ICT standards if it—~~

~~(A)(i) Complies with an earlier standard issued pursuant to section 508, which is set forth in Appendix D to 36 CFR 1194.1; and~~

~~(A)(ii) Has not been fundamentally altered (*i.e.*, changed in a manner that affects interoperability, the user interface, or access to information or data) after January 18, 2018.~~

~~(3) *Alterations of Legacy ICT*. When altering a component or portion of existing ICT, after January 18, 2018, the component or portion must be modified to conform to the most current ICT accessibility standards in 36 CFR 1194.1~~

b. ~~b.~~ *Definitions*. As used in this subsection—

(1) ~~(1)~~ "Alternate ~~Means~~means of ~~Access~~access" means different methods of providing information, including product documentation, to people with disabilities when meeting the Access Board standards would impose an undue burden or fundamental alteration in the ICT. The term may include, but is not limited to, voice, fax, relay service, TTY, internet posting, captioning, text-to-speech synthesis, and audio description.

(2) ~~(2)~~ "Commercial ~~Non~~non-availability" means an instance where FAA is unable to find a commercial item that meets applicable information and communication accessible standards or when an item cannot be furnished to satisfy FAA's requirements.

(3) ~~(3)~~ "Content" means electronic information and data, as well as the encoding that defines its structure, presentation, and interactions.

(4) ~~(4)~~ "Disability" means a physical or mental impairment that substantially limits one or more major life activities.

(5) ~~(5)~~ "Information and Communication Technology (ICT)" means information technology, as defined by The Access Board, at 36 CFR 1194.4, and any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion or duplication of data or information. ICT includes, but is not limited to: software applications and operating systems, telecommunications products, information kiosks and transaction machines, Web sites (Internet, Intranet and Extranet), video and multimedia products, desktop and portable computers, office equipment such as copiers and fax machines, and documents posted online (e.g., Word, PDF). For the purposes of this definition, equipment is used by the FAA if:

(A) ~~(i)~~ It is used directly by FAA; or

(B) ~~(ii)~~ It is used by a contractor under a contract with FAA that—

~~(a)~~i. Requires use of such equipment; or

ii. ~~(b)~~ Requires use, to a significant extent, of such equipment in performance of a service of furnishing of a product.

(6) ~~(6)~~ "Fundamental ~~Alteration~~alteration" means incorporating accessibility features into a product that alters the product in such a way as to reduce substantially the functionality of the product, to render some features inoperable, to impede substantially or deter use of the product by individuals without the specific disability the feature is designed to address, or to alter substantially and materially the shape, size or weight of the product.

(7) ~~(7)~~ "National ~~Security Systems~~security system" means any telecommunications or

information system operated by the United States Government, the functions, operation, or use of which involves intelligence activities; cryptologic activities related to national security; the command and control of military forces; equipment that is an integral part of weapon or weapons system or before is critical to the direct fulfillment of military or intelligence missions. This does not include a system that is to be used for routine administrative and business applications, such as payroll, finance, logistics, and personnel management applications.

(8) ~~(8)~~ "Incidental ~~Contract~~contract" means a contract of a contractor that acquires products that are neither used nor accessed by Federal employees or members of the public (contracted employees in their professional capacity are not considered members of the public).

(9) ~~(9)~~ "Undue ~~Burden~~burden" means significant difficulty or expense when considering all agency resources available to the program or component for which the product is being developed, procured, maintained, or used.

(10) ~~(10)~~ "Web Content Accessibility Guidelines (WCAG)" are the guidelines published by the Web Accessibility Initiative of the World Wide Web Consortium which explain how web content can be made to be more accessible to people with disabilities.

c. ~~c.~~ *General*.

(1) *Incorporation of FAA Order*. Federal agencies are required to ensure ~~information and communication technology (~~ICT~~)~~ that is procured, developed, maintained, or used meets the requirements of Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) (referred to in this subsection by its shorthand "Section 508"). FAA's enterprise-wide adherence to these requirements is established by FAA Order 1370.~~120A, Section 508 Accessibility~~120B, FAA Information Security and Privacy: Policy. In accordance with FAA Order 1370.~~120A~~120B, this ~~AMS Guidance~~ subsection ~~implements~~incorporates into AMS Section ~~508~~508's and the Architectural and Transportation Barriers Compliance Board's (U.S. Access Board) ICT accessibility standards at 36 CFR 1194.1 to ensure that ICT procured by the FAA provides employees and members of the public with disabilities access to and use of ICT that is comparable to that of individuals without disabilities.

(2) *Legacy ICT*. Any component or portion of existing ICT procured, maintained or used prior to January 18, 2018 is not required to comply with the most current ICT standards if it—

(A) Complies with an earlier standard issued pursuant to section 508, which is set forth in Appendix D to 36 CFR 1194.1; and

(B) Has not been fundamentally altered (*i.e.*, changed in a manner that affects interoperability, the user interface, or access to information or data) after January 18, 2018.

(C) *Alterations of Legacy ICT.* When altering a component or portion of existing ICT, after January 18, 2018, the component or portion must be modified to conform to the most current ICT accessibility standards in 36 CFR 1194.1 ~~d.~~.

(3) *Exceptions*.

(A) ~~(1)~~ Section 508 requirements do not apply to the following procurements—

i. ~~(i)~~ ICT operated by FAA as part of a national security system;

ii. ~~(ii)~~ ICT acquired by a contractor incidental to a contract; or

iii. ~~(iii)~~ ICT which is located in spaces frequented only by service personnel for maintenance, repair or monitoring of equipment~~;~~.

(B) ~~(2)~~ *Documentation*. If the requiring service organization determines that an exception applies, it must document the exception and ensure such documentation is maintained in the contract file.

(4) ~~e.~~ *Waivers*.

(A) ~~(i)~~ A waiver to Section 508 requirements may be appropriate and sought under the following circumstances—

i. ~~(a)~~ *Undue Burden.* Complying with ICT would impose an undue burden to FAA. If such a waiver is authorized, the applicable procurement need only to conform with Section 508 requirements to the extent they will not create an undue burden. (*Note: An exception from the WCAG is considered an exception for undue burden.*)

ii. ~~(b)~~ *Fundamental Alteration*. Complying with ICT would result in a fundamental alteration in the nature of the ICT. If such a waiver is authorized, procurements need only to conform with Section 508 requirements to the extent they will not create a fundamental alteration.

iii. ~~(c)~~ *Commercial Non-availability*. ICT products and or services are not commercially available, or such an item cannot be furnished to satisfy the requirement. In such instances FAA must procure such products or services in the commercial marketplace that best meet the ICT accessibility standards consistent with the agency's needs.

(B) ~~(ii)~~ *Alternate Means of Access*. When a waiver is granted under this subsection, FAA

must provide individuals with disabilities access to and use of information and data by an alternative means.

(C) ~~(iii)~~ *Authorization and Documentation of Waivers*.

i. ~~(a)~~ *Authorization Process.* Waivers to Section 508 requirements made under this subsection require review from multiple parties and authorization from the DOT Secretary or their designee. If a service organization determines that a waiver is appropriate and should be sought, the ~~serice~~service organization must consult AIT's Policy and Administrative Branch (ASP-110) for guidance on the appropriate action to be taken.

ii. ~~(b)~~ *Documentation*. A determination of (~~a~~)(A)i~~)~~. *Undue Burden* or (~~a~~)(A)ii~~)~~. *Fundamental Alteration* must, respectively, address the extent compliance with applicable ICT standards would constitute a significant hardship on the agency or how compliance would result in a fundamental alteration of the ICT. A determination of (~~a~~)(A)iii~~)~~. *Commercial Non-availability* must include ~~(1)~~ :

(a) A description of the market research performed; ~~(2)~~

(b) A listing of the requirements that cannot be met; and ~~(3)~~

(c) The rationale for determining that the ICT to be procured best meets the ICT accessibility standards in 36 CFR 1194.1, consistent with the agency's needs.

(5) ~~f.~~ *Roles and Responsibilities*. Requiring Officials, Contracting Officers~~,~~ (COs), Contracting Officer's Representatives (CORs) and Purchase Cardholders are responsible for ensuring accessibility requirements are addressed in all applicable procurements. To carry out their specific responsibilities, outlined below, the "~~Accessibility Requirements Tool~~Accessibility Requirements Tool," provided by GSA, must be used. The Accessibility Requirements Tool is a step-by-step guide that helps identify relevant Section 508 accessibility requirements and incorporate them into procurement and SIR documentation, as well as in-house IT development.

(A) ~~(1)~~ *Requiring ~~Officials~~.* ~~Requiring officials~~*Service Organization*. When procuring ICT, the procurement team must ~~identify and incorporate relevant~~ensure:

i. Applicable Section 508 ~~accessibility~~technical standards are identified;

ii. Solicitations include references to the identified standards;

iii. Market research is performed to include consideration of Section 508 compliance;

iv. Selection of the product or service that meets business requirements ~~in their procurements. These~~and best meets Section 508 requirements is selected; and ~~or determinations that an exception applies must be documented in the contract file.~~

v. ~~(2)~~ Documentation is retained to demonstrate compliance with Section 508 requirements.

(B) *Contracting Officers ~~(CO)~~.* COs must review all SOWs and purchase requests to ensure requiring officials have included necessary Section 508 documentation within the requirements documentation. COs must ensure this documentation ~~as well as a Section 508 Checklist~~ is incorporated into the contract file~~. The Section 508 Checklist can be found in Procurement Checklists~~.

(C) ~~(3)~~ *Contracting Officer's Representatives ~~(COR)~~.* CORs must ensure any ICT deliverables meet the Section 508 requirements as outlined in procurement documents by validating vendor claims prior to acceptance of deliverables~~;~~.

(D) ~~(4)~~ *Purchase Cardholders*. When procuring ICT by purchase card, the purchase cardholder must verify any ICT products and services meet Section 508 requirements prior to purchase, as appropriate.

2 Internet Protocol Version 6 Added 7/2023

a. *Applicability.* This subsection applies to all SIRs, contracts and orders for Information and Communication Technology (ICT) assets, software and network services.

b. *General.*

(1) Internet Protocol Version 6 (IPv6) requirements must be included in all SIRs, contracts, and orders for ICT assets, software and network services. When acquiring ICT assets, software and network services, the requirements documents must include reference to the appropriate technical capabilities as defined in USGv6 Profile (Special Publication (NIST SP) - 500-267Br1) or, if applicable, the most recent superseding publication. Corresponding declarations of conformance are defined in the USGv6 Test Program Guide (Special Publication (NIST SP) - 500-281Ar1) or, if applicable, the most recent superseding publication. The applicability of IPv6 to agency networks, infrastructure, and applications specific to individual acquisitions will be in accordance with the FAA's Enterprise Architecture and Office of Management and Budget Memorandum M-21-07 "Completing the Transition to Internet Protocol Version 6 (IPv6)."

(2) *Roles and Responsibilities*. When acquiring ICT assets, software and network services, the requiring service organization must contact the Office of Information and Technology (AIT) to determine IPv6 applicability. For AIT points of contact and other additional information, see FAA's Internet Protocol Version 6 (IPv6) website (*FAA only*).

3 Positioning, Navigation and Timing Services Added 7/2023

a. *Applicability*. This subsection applies to all SIRs, contracts and orders for products, systems, and services that integrate or utilize Time and Frequency (T&F) systems or services.

b. *Definitions*. As used in this subsection— "Positioning, Navigation and Timing (PNT) Services" means any system, network, or capability that provides a reference to calculate or augment the calculation of longitude, latitude, altitude, or transmission of time or frequency data, or any combination thereof.

c. *General*.

(1) FAA Order 1770.68 (or the latest version), Selection and Use of Time and Frequency Sources for all Systems, Services, and Applications Supporting NAS Operations, establishes the policy by which FAA T&F sources will be selected, modified, upgraded, implemented, and used by systems, services, and applications supporting National Airspace System (NAS). All applicable acquisitions for such products, systems or services must be made in accordance with the FAA Order.

(2) *Roles and Responsibilities*. The Office of Primary Responsibility (OPR) for PNT requirements is the NAS Enterprise Analysis Branch (ANG-B21). Requiring service organizations must contact ANG-B21 to determine PNT applicability to any SIR, contract, or order.

B Acquisition of Commercial Software ~~Added 4/2023~~Revised 7/2023

1 Commercial Software Licensing Agreements Added 7/2023

a. *Applicability*. This subsection applies to all SIRs, contracts, orders, and purchase card transactions which include the acquisition of commercial software.

b. *Definition*. As used in this subsection— "Commercial Software Licensing Agreement" means contractual terms and conditions for the use of a software by a licensee. (The word "agreement" within this term is used to align with the commonplace phrase of "licensing agreement." It should be understood within this subsection to mean a "contract.")

c. *General*.

(1) Often embedded in commercial software licensing agreements are terms and conditions that could create unexpected liabilities for the FAA. Such potential liabilities must be addressed prior to procurement.

(2) *Roles and Responsibilities*.

(A) *Contracting Officers.* Prior to entering into a commercial software licensing agreement, COs must:

i. Complete and include in the contract file the "Checklist for Review of Commercial Software Licenses/Contracts" checklist located in Procurement Checklists;

ii. Consult with the Office of the Chief Counsel (AGC) to ensure that agreement terms and conditions minimize FAA's liability, and strike a balance between the FAA's requirements needs and the contractor's proprietary interest;

iii. Review clauses with relevance to the acquisition of commercial software to determine if they should be inserted in applicable SIRs and contracts. These clauses are:

(a) 3.5-13 "Rights in Data – General;"

(b) 3.5-14 Representation of Limited Rights Data and Restricted Computer Software

(c) 3.5-15 "Additional Data Requirements"

(d) 3.5-16 "Rights in Data – Special Works;"

(e) 3.5-17 "Rights in Data – Existing Works;"

(f) 3.5-18 "Commercial Computer Software License."

(B) *Purchase Cardholders.* Prior to entering into a commercial software licensing agreement, Purchase Cardholders must consult with the Office of the Chief Counsel (AGC) to ensure that agreement terms and conditions minimize FAA's liability, and strike a balance between the FAA's requirements needs and the contractor's proprietary interest.

2 Cloud Computing Services **Added 7/2023**

a. *Applicability*. This subsection is applicable to all SIRs, contracts, orders and purchase card transactions when using cloud computing to provide ICT services in the performance of a contract or order.

b. *Definitions*. As used in this subsection—

(1) "Software as a service (SaaS)" means a software licensing and delivery model in which the software is based on a subscription and is centrally hosted.

(2) "Cloud computing" means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

c. *General*.

(1) FAA requires that contracts for cloud computing services including SaaS:

(A) Adhere to Federal Risk and Authorization Management Program (FedRAMP) compliance requirements.

(B) Select a FedRAMP-certified Cloud Service Provider (CSP).

(C) Be granted Authority to Operate (as defined in FedRAMP website at https//www.fedramp.gov) from the designated FAA Authorizing Official (AO).

(D) CSPs granted an Authority to Operate by other agencies or that are in the process of acquiring FedRAMP certification may be selected, but systems being hosted or SaaS licenses being purchased must not be placed into production at the FAA without a signed Authority to Operate from the designated FAA AO.

(2) In addition to the use of a FedRAMP-certified CSP and the FedRAMP baseline controls, all FAA cloud-hosted systems must implement additional FAA security controls as defined on the FedRAMP website, applicable FAA Policy, and the DOT Departmental Cybersecurity Compendium to operate securely based on the current DOT and FAA policy.

(3) A CSP must maintain their FedRAMP certification throughout the contract and adhere to continuous FAA monitoring that ensures the security posture of the CSP throughout the lifecycle of the service agreement. The security posture of the CSP is the implementation of

security controls to protect the information contained on and the infrastructure of CSP systems that must be maintained throughout the life of the contract.

(4) The CSP must continue to maintain the security posture of additional FAA security controls upon which the FAA ATO is based. A Third Party Assessment Organization (3PAO) must perform a security assessment on the CSP at least annually. The CSP must inform the FAA if there is a security breach or outage, with the protocol for notifying the FAA as well as the United States Computer Readiness Support Team (US-CERT) of such a breach or outage set by each individual contract.

(5) *Roles and Responsibilities*. COs and requiring service organizations must ensure the following is considered when acquiring cloud computing services:

(A) All FAA contracts using cloud technology including SaaS must be documented in the systems security assessment and maintained in FAA FISMA system inventory and follow the Office of Management and Budget (OMB) reporting requirements.

(B) All FAA contracts using cloud technology must be coordinated from initial procurement planning with the FAA Office of Cloud Services (AIF-001).

C Prohibitions on Covered Information and Communication Technology ~~Added 4/2023~~Revised 7/2023

1 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment Added 7/2023

a. *Applicability*. The prohibitions described in this subsection apply to all SIRs, contracts, orders and purchase card transactions.

b. *Definitions*. As used in this subsection—

(1) "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).

(2) "Covered foreign country" means The People's Republic of China.

(3) "Covered telecommunications equipment or services" means–

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

(B) 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);

(C) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(D) 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.

(4) "Critical technology" means–

(A) 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;

(B) 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;

(C) 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);

(D) 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);

(E) 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

(F) Emerging and foundational technologies controlled pursuant to section 1758 of the

Export Control Reform Act of 2018 (50 U.S.C. 4817).

(5) "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., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

(6) "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.

(7) "Roaming" means cellular communications services (e.g., voice, video, data) received from a visited network when traveling outside the geographical coverage area of a home network.

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

c. *General*.

(1) *Prohibitions*. This subsection implements paragraph (a)(1)(A) and paragraph (a)(1)(B) of section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115-232). Per these paragraphs of section 889:

(A) On or after August 13, 2019, agencies are prohibited from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service 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, unless an exception at subparagraph (2) *Exceptions* of this subsection applies or the covered telecommunications equipment or services are covered by a waiver described in subparagraph (5) *Waivers*.

(B) On or after August 13, 2020 agencies are prohibited from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service 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, unless an exception below at subparagraph (2) *Exceptions* applies or the covered telecommunication equipment or services are covered by a waiver described below at subparagraph (5) *Waivers*. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(2) *Exceptions*. This subsection does not prohibit agencies from procuring or contractors from providing:

(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, redirect user data traffic, or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(3) *Roles and Responsibilities*. Unless an exception described in subparagraph (2) *Exceptions* above applies or the covered telecommunications or video surveillance services or equipment is covered by a waiver as described in subparagraph (5) *Waivers*, COs and purchase cardholders will not:

(A) Procure or obtain, or extend or renew a contract (e.g., exercise an option) to procure or obtain, any equipment, system, or service 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; or

(B) Enter into a contract, or extend or renew a contract, with an entity that uses any equipment, system, or services as a substantial or essential component of any system, or as critical technology as part of any system.

(4) *Procedures for Offeror/Vendor Representations and Reports*.

(A) *Offeror/Vendor Representations*.

(i) If an offeror selects "does not" in response to paragraphs (c)(1) and/or (c)(2) of provision 3.8.9-3 "Covered Telecommunications or Services – Representation", the CO may rely on the representation unless the CO has reason to question the representation. If the CO has reason to question the representation, the CO will follow agency procedures.

(ii) If the offeror selects "does" in response to paragraph (c)(1) of provision 3.8.9-3, the offeror must complete the representation at paragraph (d)(1) of provision 3.8.9-1 "Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment". If an offeror selects "does" in response to paragraph (d)(2) of provision 3.8.9-3, the offeror must complete the representation at paragraph (d)(2) of provision 3.8.9-1.

(iii) If an offeror provides an affirmative response to the representations or discloses

information in accordance with paragraphs (d) and (e) of the provision at 3.8.9-1 , the CO or purchase cardholder must not make an award to the offeror unless the requiring activity provides a written determination that the covered telecommunications equipment or services included in their offer, in accordance with paragraph (e) of the provision, are not being used as a substantial or essential component of any system, or as critical technology as part of any system. If the requiring activity is unable to provide a written determination as described above and no other offerors provide a negative representation, then no award will be made unless a waiver is granted.

(iv) If the apparently successful offeror provides a negative response to the representation in (d) of provision 3.8.9-1, the CO/purchase cardholder may rely on the representation, unless the CO/purchase cardholder has an independent reason to question the representation. If the CO/purchase cardholder has an independent reason to question a negative representation of the otherwise successful offeror, the CO/purchase cardholder must consult with the requiring activity and legal counsel on how to proceed to ensure that the procurement would not violate the statutory prohibition.

(B) If a contractor provides a report pursuant to paragraph (d) of the clause 3.8.9-2 "Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment", the CO/purchase cardholder will consult with the requiring activity and legal counsel on how to proceed using existing contractual remedies.

(5) *Waivers*.

(A) The head of an agency may, on a one-time basis, waive a prohibition described in this subsection for FY 2019 with respect to a Government entity (e.g., requirements office, contracting office) that requests such a waiver.

(i) The waiver may be provided, for a period not to extend beyond August 13, 2021 for the prohibition at paragraph b (1) or beyond August 13, 2022 for the prohibition at paragraph b (2), if the Government entity seeking the waiver submits to the head of the executive agency–

(a) A compelling justification for the additional time to implement the requirements under this subsection, as determined by the head of the executive agency; and

(b) A full and complete description of the presences of covered telecommunications or video surveillance equipment or services in the relevant supply chain and a phase-out plan to eliminate such covered

telecommunications or video surveillance equipment or services from the relevant systems.

(ii) Before head of the agency can grant a waiver to a prohibition described by this subsection, the agency must–

(a) Have designated a senior agency official for supply chain risk management, responsible for ensuring the agency effectively carries out the supply chain risk management functions and responsibilities described in law, regulation, and policy;

(b) Establish participation in an information-sharing environment when and as required by the Federal Acquisition Security Council (FASC) to facilitate interagency sharing of relevant acquisition supply chain risk information;

(c) Notify and consult with the Office of the Director of National Intelligence (ODNI) on the waiver request using ODNI guidance, briefings, best practices, or direct inquiry, as appropriate; and

(d) Notify the ODNI and the FASC 15 days prior to granting the waiver that it intends to grant the waiver.

(B) *Waivers for Emergency Acquisitions*.

i. In the case of an emergency, including a declaration of major disaster, in which prior notice and consultation with the ODNI and prior notice to the FASC is impracticable and would severely jeopardize performance of mission-critical functions, the head of an agency may grant a waiver without meeting the notice and consultation requirements under of T3.8.9C.1.c(5)(A)ii., components (c) and (d) above to enable effective mission critical functions or emergency response and recovery.

ii. In the case of a waiver granted in response to an emergency, the head of an granting the waiver must–

(a) Make a determination that the notice and consultation requirements are impracticable due to an emergency; and

(b) Within 30 days of award, notify the ODNI and FASC of the waiver issued under emergency conditions in addition to the waiver notice to Congress per the requirements below in item (C) *Waiver Notice*.

(C) *Waiver Notice*.

i. For waivers to the prohibition at item (A)of paragraph c. *General*, subparagraph (1) *Prohibitions* (T3.8.9C.1.c(1)(A)), the head of the executive agency will, not later than 30 days after approval–

(a) Submit in accordance with agency procedures to the appropriate congressional committees the full and complete laydown of the presences of covered telecommunications or video surveillance equipment or services in the relevant supply chain; and

(b) The phase-out plan to eliminate such covered telecommunications or video surveillance equipment or services from the relevant systems.

ii. For waivers to the prohibition at item (B) of paragraph c. *General*, subparagraph (1) *Prohibitions* (T3.8.9C.1.c.(1)(B)), the head of the executive agency will, not later than 30 days after approval submit in accordance with agency procedures to the appropriate congressional committee:

(a) An attestation by the agency that granting of the waiver would not, to the agency's knowledge having conducted the necessary due diligence as directed by statute and regulation, present a material increase in risk to U.S. national security;

(b) The full and complete laydown of the presence of covered telecommunications or video surveillance equipment or services in the relevant supply chain, to include a description of each category of covered technology equipment or services discovered after reasonable inquiry, as well as each category of equipment, system, or service used by the entity in which covered technology is found, and after conducting a reasonable inquiry; and

(c) The phase-out plan to eliminate such covered telecommunications or video surveillance equipment or services from relevant systems.

(D) *Director of National Intelligence*. The Director of National Intelligence may provide a waiver if the Director determines the waiver is in the national security interests of the United States.

2 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities **Added 7/2023**

a. *Applicability*. The prohibitions described in this subsection apply to all SIRs, contracts, orders and purchase card transactions.

b. *Definitions*. As used in this subsection—

(1) "Covered article" means any hardware, software, or service that–

(A) Is developed or provided by a covered entity;

(B) Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or

(C) Contains components using any hardware or software developed in whole or in part by a covered entity.

(2) "Covered entity" means–

(A) Kaspersky Lab;

(B) Any successor entity to Kaspersky Lab;

(C) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(D) Any entity of which Kaspersky Lab has a majority ownership.

c. *General*.

(1) *Prohibition*. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Federal government use of any covered article as defined in this subsection. Contractors are prohibited from—

(A) Providing any covered article that the Government will use; and

(B) Using any covered article in the development of data or deliverables first produced in the performance of the contract.

(2) *Contract Clause and Notification*.

(A) *Clause*. The CO must insert the clause AMS 3.8.9-4 "Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other

Covered Entities," in all SIRs and contracts. For existing contracts, please refer to the clause prescription.

(B) *Notification*. When a contractor provides notification pursuant to clause 3.8.9-4, the following offices must be notified as soon as possible by the CO or the COR with the information provided by the contractor:

(i) The Chief Information Officer (CIO) (AIT-001);

(ii) The Director, Information Security & Privacy Service (AIS-001); and

(iii) The Enterprise Software Board (ESB) (ASP-200).

3 Prohibition on Using Bytedance Covered Applications Including TikTok **Added 7/2023**

a. *Applicability*. The prohibition described in this subsection applies to all SIRs, contracts, orders purchase card transactions effective respective as of the dates specified in paragraph c. *General*, subparagraph (3) *Roles and Responsibilities*, below.

b. *Definitions*. As used in this subsection—

(1) "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.

(2) "Information technology," as defined by 40 U.S.C. 611101(6)—

(A) 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;

(B) 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

(C) Does not include any equipment acquired by a Federal Contractor incidental to a Federal contract.

c. *General*.

(1) *Prohibition*.

(A) Section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328), the No TikTok on Government Devices Act, and its implementing guidance provided by Office of Management and Budget Memorandum M-23-13, dated February 27, 2023, "No TikTok on Government Devices" Implementation Guidance, collectively prohibit the presence or use of a covered application on information technology, including certain equipment used by Federal contractors.

(B) This prohibition applies to the presence or use of a covered application on any information technology owned or managed by the FAA, or on any information technology used or provided by the contractor under a contract, including equipment provided by the contractor's employees, unless a waiver is granted in accordance with this AMS subsection.

(2) *Waivers*. As limited by items (A) *Waiver Categories* and (B) *Waiver Terms*, when use of a covered application is deemed critical to the FAA mission and alternative approaches are not viable, the FAA Acquisition Executive (FAE) may grant a waiver to the requirements of this Guidance subsection.

(A) *Waiver Categories*. Blanket waivers applying to an entire agency are not permitted. FAA must only grant a waiver exclusive to specific FAA programs or operational actions covered by the following waiver categories:

i. *National Security Interests and Activities*. A waiver may be granted when it is determined that use of a covered application has a clear nexus with national security interests or activities.

ii. *Law Enforcement Activities*. A waiver may be granted for activities such as those that are performed by or in coordination with an agency that is part of the Federal law enforcement community, in response to a law enforcement emergency, or in the course of investigating potential violations of Federal statutes or regulations.

iii. *Security Research Activities*. A waiver may be granted for activities such as those that may include investigations to limit harm to individual, public, private, or national physical or digital infrastructure through the identification of vulnerabilities, security weaknesses, or actionable threats, as well as agency investigation into suspected malign foreign influence.

(B) *Waiver Terms*. Waivers may last up to one year, after which the FAE must reevaluate the waiver for renewal or termination.

(C) *Documentation*. Waivers must be documented in the contract file. This documentation must include, at a minimum, the following information:

i. Date of approval;

ii. Applicable waiver category (as outlined in this subsection);

iii. Description of the circumstances under which the waiver applies;

iv. Period of the waiver; and

v. Risk mitigation actions that will be taken to prevent access by a covered application to sensitive data.

(3) *Roles and Responsibilities*. Unless a waiver has been granted in accordance with this subsection, COs must insert AMS clause 3.8.9-5 "Prohibition on Using ByteDance Covered Applications Including TikTok," as follows—

(A) *New SIRs and resulting contracts*. All SIRs published and resulting contracts awarded after June 8, 2023 must include this clause.

(B) *Existing SIRs*. Existing SIRs published prior to June 8, 2023 for which an award to a resulting contract has not been issued, must be amended to include this clause by July 3, 2023.

(C) *Existing indefinite delivery contracts*. Existing indefinite delivery contracts must be modified to include this clause by July 3, 2023 to apply to future orders.

(D) *Exercising of options or modifying of an existing contract or task or delivery order*. If exercising an option or modifying an existing contract or task or delivery order to extend the period of performance, this clause must be included. When exercising an option, COs should consider modifying the existing contract to add the clause in a sufficient amount of time before exercising the option so as to provide contractors with an adequate amount of time to adjust and comply as needed.

~~B~~D Clauses ~~Added 4/2023~~Revised 7/2023

view contract clauses

~~C~~E Procurement Forms ~~Added 4/2023~~Revised 7/2023

Document Name

~~D~~F Procurement Samples ~~Added 4/2023~~Revised 7/2023

Document Name

~~E~~G Procurement Templates ~~Added 4/2023~~Revised 7/2023

Document Name

~~F~~H Procurement Tools and Resources ~~Added 4/2023~~Revised 7/2023

Document Name
Accessibility Requirements Tool

~~G~~I Procurement Checklists ~~Added 4/2023~~Revised 7/2023

Document Name
Checklist for Review of Commercial Software Licenses/Contracts