U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

MEMORANDUM FOR: Heads of the Contracting Activities

PAUL R COURTNEY Digitally signed by PAUL R COURTNEY Date: 2024.07.22 15:04:42 -04'00'

FROM: Paul Courtney
Chief Procurement Officer

SUBJECT: Federal Acquisition Regulation Class Deviation (Number 20 - 05), Revision 3, 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities, and 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

Purpose: This FAR Class Deviation 20-05, Revision 3 supersedes Revision 1 and 2 to the class deviation. This revision is necessary to update the clause at FAR 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities to change the terms "covered article" and "covered entity" to "Kaspersky Lab covered article" and "Kaspersky Lab covered entity". This change was made to avoid confusion with the definition of a covered article excluded or removed in the Federal Acquisition Supply Chain Security Act (FASCSA) final rule. In addition to the name changes, paragraph (c)(2)(i) of FAR 52.204-23 is updated to change the reporting time frame for the initial report from 1 business day to 3 business days to align paragraph (c)(4) of FAR 52.204-30, Federal Acquisition Supply Chain Security Act Orders-Prohibition, which was added to the FAR in December 2023. Additionally, this revision consolidates Attachments 1 from Revisions 1 and 2. Please note that deviated clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment remains unchanged.

Effective Date: Immediately.

Background: FAR Class Deviation 20-05, Revision 1, issued on August 6, 2020, inadvertently omitted the words "and excluding paragraph (b)(2)" from paragraph (e) of the clause at 52.204-25. Therefore, where the FAR Class Deviation 20-05, Revision 1 clause was included in a contract, the Department will not enforce the contractual requirement that contractors include paragraph (b)(2) in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items. However, FAR Class Deviation 20-05, Revision 2, issued December 10, 2020, added the omitted words "and excluding paragraph (b)(2) to paragraph (e) of 52.204-25 to make this correction and revised paragraph (d) of the clause to require the contractor to report the incident concurrently to the contracting officer, COR and the Network Operations Security Center (NOSC).

This was added to ensure timely reporting to the NOSC, to enable the Department to quickly assess and mitigate the security incident.

FAR 4.2002 prohibits Government use on or after October 1, 2018, of any hardware, software, or services developed or provided, in whole or in part, by Kaspersky Lab covered entities. It also prohibits contractors from providing any Kaspersky Lab covered article that the Government will use on or after October 1, 2018 and (b) using any Kaspersky Lab covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract. FAR Subpart 4.21 addresses supply chain risks associate with certain telecommunications and video surveillance equipment and services from China (i.e., Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, and their subsidiaries and affiliates). In accordance with FAR 4.2102, agencies are prohibited from procuring or entering into a contract with an entity that uses certain covered telecommunications equipment or services, or extending or renewing such a contract.

Requirement: DHS contracting officers shall include the deviated clause at 52.204-23 in all solicitations and contracts that are issued and awarded on or after the issuance date of this class deviation. Accordingly, applicable solicitations issued on or after the issuance date of this class deviation shall be amended to include the modified clause. Additionally, applicable contracts awarded on or after the issuance date of this class deviation shall be modified to include the revised clause. Please note that the deviated clause at 52.204-25 is still applicable and remains unchanged.

Applicability: This class deviation is applicable to all solicitations and contracts.

Expiration Date: This class deviation will remain in effect until it is incorporated into the Homeland Security Acquisition Regulation or is otherwise rescinded.

Additional Information: Component Acquisition Policy Chiefs should coordinate with the appropriate Component Contract Writing Systems (CWS) personnel to use the modified clause at 52.204-23 in Attachment 1.

Attachments: Attachment 1: 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (DEVIATION 20-025) (JUN 2024) and 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (DEVIATION 20-05) (DEC 2020).

Questions or comments about this class deviation may be directed to Camara Francis at 301-356-1181 or Camara.Francis@hq.dhs.gov.

52.204-23 PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB COVERED ENTITIES

(DEVIATION 20-05) (JUL 2024)

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

(b) *Prohibition*. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any Kaspersky Lab covered article. The Contractor is prohibited from—

(1) Providing any Kaspersky Lab covered article that the Government will use on or after October 1, 2018; and
(2) Using any Kaspersky Lab covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

(c) *Reporting requirement.*

(1) In the event the Contractor identifies covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report, in writing, via email, to the Contracting Officer, Contracting Officer's Representative, and the Enterprise Security Operations Center (SOC) at NDAA_Incidents@hq.dhs.gov, with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Enterprise SOC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (c)(1) of this clause:

(i) Within 3 business days from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or

wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a Kaspersky Lab covered article, any reasons that led to the use or submission of the Kaspersky Lab covered article, and any additional efforts that will be incorporated to prevent future use or submission of Kaspersky Lab covered articles.

(d) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.

(End of clause)

52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (DEVIATION 20-05) (DEC 2020)

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

"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 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-

(l) 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 of2018 (50 U.S.C. 4817).

"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.

"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.

"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.

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

(b) *Prohibition.*

(1) Section 889(a)(l)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, 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. The Contractor is prohibited from providing to the Government 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 paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(l)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, 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 at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. 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.

(c) *Exceptions.* This clause does not prohibit contractors from providing-

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

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

(d) *Reporting requirement.*

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause in writing via email to the Contracting Officer, Contracting Officer's Representative, and the Network Operations Security Center (NOSC) at NDAA_Incidents@hq.dhs.gov, with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the NOSC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.clod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(l) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)