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

Homeland Security

April 10, 2020

MEMORANDUM FOR: Heads of the Contracting Activities

FROM: Soraya Correa
Chief Procurement Officer

SORAYA CORREA
Digitally signed by SORAYA CORREA
Date: 2020.04.11 14:02:28 -04'00'

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

Purpose: This class deviation is issued in accordance with Federal Acquisition Regulation (FAR) 1.404 to (1) advise contracting activities that the Department has revised the reporting requirements in FAR clauses 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities, and 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, to require contractors to submit reports required by subparagraphs (c) and (d)(1) of the clauses to the contracting officer, contracting officer's representative (COR), and the Enterprise Security Operations Center (SOC) and (2) require contracting activities to include the modified clauses in all solicitations and contracts, as required in FAR 4.2004 and 4.2105.

Effective Date: Immediately.

Background: FAR Subparts 4.20 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and 4.21 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment address supply chain risks associated with products and services provided by Kaspersky Lab and certain telecommunications and video surveillance equipment and services from China (e.g., Huawei Technologies Company or ZTE Corporation). 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 and other covered entities. It also prohibits contractors from providing any covered article that the Government will use on or after October 1, 2018 and (b) using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract. Similarly, in accordance with FAR 4.2102, agencies are prohibited from procuring, or extending or renewing a contract to procure, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system.

FAR clauses 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities, and 52.204-25,

Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment require contractors to submit a report to the contracting officer in the event the contractor identifies covered equipment or services being used during contract performance, including by any subcontractor(s) at any tier or by any other source used by the contractor in performance of the contract. The FAR directs contracting officers to follow agency procedures when a report is received. The Department has determined that reports under both clauses are considered a security incident and should be treated as such. Consistent with DHS policy, i.e., 4300A Sensitive Systems Handbook, incidents are required to be reported to the Enterprise SOC. This FAR Class Deviation requires the contractor to report the incident concurrently to the contracting officer, COR and the Enterprise SOC. This approach ensures timely reporting to the SOC and better enables the Department to quickly assess and mitigate the security incident. The SOC will review the information provided by the contractor, coordinate this review with other stakeholders as needed, and then provide the results of this review to the contracting officer and COR for resolution.

Requirement: DHS contracting officers shall insert modified clauses 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities and 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (see Attachment 1) 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 clauses. Additionally, applicable contracts awarded on or after the issuance date of this class deviation shall be modified to include the revised clauses.

Applicability: This class deviation is applicable to all solicitations and contracts, as defined in FAR 2.101 and consistent with FAR 4.2004 and 4.2105(b), awarded on or after the issuance date of this class deviation.

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: In order to provide access to clauses 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (DEVIATION 2020-05) and 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (DEVIATION 20-05) in Component Contract Writing Systems (CWS), Component Acquisition Policy Chiefs should coordinate with the appropriate Component CWS personnel to determine if the addition of the clause to their CWS is possible.

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 20-05) and 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (DEVIATION 20-05)

Questions or comments about this class deviation may be directed to Ann Shujath at (202) 447-0230 or Ann.Shujath@hq.dhs.gov; and to Joanne Battaglia at (202) 447-5020 or Joanne.Battaglia@hq.dhs.gov.

Class Deviation from the Federal Acquisition Regulation (FAR) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities and 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

Findings

The Department of Homeland Security (DHS), in accordance with FAR 4.2003 and 4.2103, has determined that the reports required by subparagraphs (c) and (d)(1) of FAR clauses 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities and 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, are security incidents and must comply with Departmental incident reporting requirements. Departmental policies and procedures for security incidents are defined in 4300A Sensitive Systems Handbook. Consistent with the requirements of 4300A, DHS has determined that the reports under both clauses must be submitted to the contracting officer, contracting officer's representative (COR), and the Enterprise Security Operations Center (SOC). Such notification ensures timely reporting to the appropriate organizations within the Department and better enables DHS to quickly assess and mitigate the impacts associated with the security incident.

Determination

In accordance with FAR 1.404, I hereby issue a class deviation to 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities and 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. This deviation implements the requirement that contractors submit the reports required by subparagraphs (c) and (d)(1) of the clauses to the contracting officer, COR and Enterprise SOC. This deviation requires contracting officers to insert modified clauses 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities and 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (see Attachment 1) in all applicable solicitations and contracts meeting the requirements of FAR 4.2004 and 4.2105(b).

As required by FAR 1.404, the Office of the Chief Procurement Officer has consulted with the Chairperson of the Civilian Agency Acquisition Council regarding this class deviation.

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

SORAYA CORREA Digitally signed by SORAYA CORREA
Date: 2020.04.11 14:04:40 -04'00'

Soraya Correa
Chief Procurement Officer
Department of Homeland Security

Date

52.204-23 PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (DEVIATION 20-05)

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

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

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

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

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

"Covered entity" means–

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab;

(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 covered article. The Contractor is prohibited from—

(1) Providing any covered article that the Government will use on or after October 1, 2018; and

(2) Using any 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 1 business day 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 covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.

(c) *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)

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

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

"Covered telecommunications equipment or services" means–

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

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

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

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

"Critical technology" means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);
(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

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

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

(b) *Prohibition.* Section 889(a)(1)(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 Federal Acquisition Regulation 4.2104.

(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 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 (d)(1) 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.

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

(End of clause)