FLOWDOWN CLAUSES FOR PURCHASE ORDERS ISSUED IN SUPPORT OF CONTRACT NO. 70RTAC21D00000001

1. INCORPORATION BY REFERENCE. These Flowdown Clauses for Purchase Orders Issued in Support of Contract No. 70RTAC21D00000001 ("Flowdown Clauses") are incorporated in their entirety into any Purchase Order issued under the Reseller Agreement in support of Contract No. 70RTAC21D00000001. In the event of a conflict between these Flowdown Clauses and the Agreement, these Flowdown Clauses shall prevail.

2. RATED ORDER. If this is a "rated order" certified for national defense use, Company shall follow all the requirements of the Defense Priorities and Allocation System Regulations (15 C.F.R. § 700).

3. CERTIFICATIONS. By accepting or performing this Purchase Order, Company certifies that:

a. Neither Company nor any of its Principals are presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency. "Principal" means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (*e.g.*, general manager; plant manager; head of a division or business segment; and similar positions).

b. If Company is registered in the System for Award Management ("SAM"), by accepting a Purchase Order, Company certifies that its representations and certifications in SAM (or any other successor system) are current, accurate and complete as of the date of Company's offer for a given Purchase Order, including, but not limited to, Company's representations and certifications regarding Company's size or socioeconomic status. Company's representations and certifications in SAM, if any, are incorporated herein by reference.

c. To the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, or an employee of a Member of Congress on its behalf in connection with the awarding of this Purchase Order. If any registrants under the Lobbying Disclosure Act of 1995 have made a lobbying contact on behalf of Company with respect to this Purchase Order, Company shall complete and submit, with its offer, OMB Standard Form LLL, Disclosure of Lobbying Activities, to provide the name of the registrants. Company need not report regularly employed officers or employees of Company to whom payments of reasonable compensation were made. Submission of this certification and disclosure is a prerequisite for making or entering into this Purchase Order imposed by 31 U.S.C. 1352. Any person who makes an expenditure prohibited under this provision or who fails to file or amend the disclosure required to be filed or amended by this provision, shall be subject to a civil penalty of not less than $10,000, and not more than $100,000, for each such failure. As used in this Certification, "Lobbying contact" has the meaning provided at 2 U.S.C. 1602(8) and the

remaining terms are defined in FAR clause 52.203-12, "Limitation on Payments to Influence Certain Federal Transactions."

d. Unless Company sells only COTS items (as defined in Paragraph 8 below) to Reseller, Company shall implement the security requirements required by DFARS clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting."

e. Company will not provide "covered telecommunications equipment or services," as defined in FAR 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, to Reseller in the performance of this or any Purchase Order.

f. Unless Company sells only COTS items (as defined in Paragraph 8 below) to Reseller, Company certifies that it has, within the within the last 3 years, conducted a Basic Assessment as described in DFARS 252.204-7020(d)(1) and submitted the summary level scores of such assessments for all contractor information systems covered by Defense Federal Acquisition Regulation System (DFARS) clause 252.204-7020 to the Government for posting to the Company Performance Risk System, and that Company fully complies with the requirements of DFARS 252.204-7020.

4. CERTIFICATES OF CONFORMANCE.

a. Company shall include with each shipment of Equipment a Certificate of Conformance as follows:

> I certify that on [*insert date*], the [*insert Company's name*] furnished the Equipment called for by Purchase Order No. [*insert Purchase Order number*] via [*insert Carrier*] on [*identify the bill of lading or shipping document*] in accordance with all applicable requirements. I further certify that the Equipment is of the quality specified and conform in all respects with the contract requirements, including specifications, preservation, packaging, packing, marking requirements, and physical item identification (part number), and are in the quantity shown on this or on the attached acceptance document. I further certify that, except as stated below, the Equipment has been mined, produced, or manufactured in the United States or substantially transformed in the United States into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was transformed.
>
> Date of Execution: _____
>
> Signature: _____
>
> Title: _____

The following Equipment supplied under this Purchase Order have not been mined, produced, or manufactured in the United States or substantially transformed in the United States:

Item Number or Identifier:_____

Country of manufacture or substantial transformation: _____

Reseller will not accept shipments of Equipment that do not contain a properly executed Certificate of Conformance as required in this Paragraph 4.

5. EQUAL EMPLOYMENT OPPORTUNITY. Reseller and Company shall abide by the requirements of 41 CFR §§ 60-300.5(a) and 60-741.5(a) and 29 CFR Part 471, Appendix A to Subpart A. These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities. Moreover, these regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard protected veteran status or disability. Company shall include this Paragraph 5 in each lower-tier subcontract it issues.

6. COMPTROLLER GENERAL EXAMINATION OF RECORD. The Comptroller General of the United States, an appropriate Inspector General appointed under section 3 or 8G of the Inspector General Act of 1978 (5 U.S.C. App.), or an authorized representative of either of the foregoing officials shall have access to and right to examine any of Company's or any subcontractors' records that pertain to, and involve transactions relating to, this Purchase Order. Company shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this Purchase Order or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this Purchase Order. If this Purchase Order is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals or to litigation or the settlement of claims arising under or relating to this Purchase Order shall be made available until such appeals, litigation, or claims are finally resolved. As used in this Paragraph 6, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require Company to create or maintain any record that Company does not maintain in the ordinary course of business or pursuant to a provision of law.

7. DISPUTES.

a. If Reseller elects to prosecute any dispute involving this Purchase Order under the disputes procedure applicable to the U.S. Government prime contract or higher-tier subcontract, Company shall cooperate fully with Reseller in prosecuting the dispute. Company shall be bound by the final outcome of the disputes procedure if Reseller has afforded Company an opportunity to participate in Reseller's prosecution of the dispute.

b. Pending the final resolution of any dispute arising out of or relating to this Purchase Order, Company shall proceed diligently with performance of this Purchase Order, including the delivery of goods and performance of services, in accordance with Reseller's direction.

8. FAR/HSAR CLAUSES.

The following clauses set forth in the Federal Acquisition Regulation ("FAR" available at https://www.acquisition.gov/browse/index/far) and the Homeland Security Acquisition Regulation ("HSAR" available at https://www.acquisition.gov/hsar) are incorporated herein by reference with the same force and effect as if they were given in full text. For purposes of the Purchase Order, the following clauses shall operate, impose the obligations and responsibilities of the parties, and be interpreted as if: "Contract" means Purchase Order; "Contracting Officer" means an authorized representative of Reseller; "Contractor" means Company; "Government" means Reseller, and "Subcontractor" means Company's lower-tier subcontractors and suppliers. References to the "Disputes clause" shall mean Paragraph 7 of these Flowdown Clauses.

Commercially available off-the-shelf" or "COTS" means any item of supply that is (a) a Commercial Product (as defined in FAR 2.101); (b) sold in substantial quantities in the commercial marketplace; and (c) offered to the Government under this Purchase Order, without modification, in the same form in which it is sold in the commercial marketplace.

For clauses marked with an asterisk (*) references to the "Government" shall remain the U.S. Government.

Reseller may modify this list of clauses to add any clauses that are reflected in an applicable prime contract or higher-tier subcontract or in subsequent modifications to an applicable prime contract or higher-tier subcontract. Accordingly, Company agrees that upon the request of Reseller, Company will negotiate in good faith with Reseller relative to modifications to this Purchase Order to incorporate additional provisions herein or to change provisions hereof, as Reseller may reasonably deem necessary in order to comply with the provisions of an applicable prime contract or higher-tier subcontract, or with the provisions of modifications to an applicable prime contract or higher-tier subcontract.

Company shall include these clauses in each lower-tier subcontract it issues, as applicable.

FAR Clause	**Title**	**Date**	**Limitations on Applicability (if blank, the clause applies to all Purchase Orders)**
52.202-1	Definitions	JUN 2020	
52.203-6	Restrictions on Subcontractor Sales to the Government, Alt. I (OCT 1995)	JUN 2020	Applies if the Purchase Order value exceeds $250,000
52.203-12	Limitation on Payments to Influence Certain Federal	JUN 2020	Applies if the Purchase Order value exceeds $150,000

	Transactions		
52.203-13	Contractor Code of Business Ethics and Conduct	JUN 2020	Applies if the Purchase Order value exceeds $6 Million and has a period of performance of more than 120 days. All disclosures of violations of the civil False Claims Act or of Federal criminal law shall be directed to the agency Office of the Inspector General, with a copy to the Contracting Officer
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights	JUN 2020	Applies if the Purchase Order value exceeds $250,000
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements	JAN 2017	
52.204-2	Security Requirements	AUG 1996	Applies if the Purchase Order requires access to classified information
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011	Applies if Company's employees are required to have routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	JUN 2020	Company is only required to provide Reseller with the information required for Reseller to comply with its obligations under the clause; Company is not required to issue reports on its first-tier subcontractors; the information provided by Company will be made publicly available
52.204-15	Service Contract Reporting Requirements for Indefinite-Delivery Contracts	OCT 2016	For Purchase Orders for the performance of services, Company shall provide Reseller with the information Reseller needs to comply with this clause
52.204-19	Incorporation by	DEC 2014	Applies if Company is registered in

	Reference of Representations and Certifications		the System for Award Management
52.204-23	Prohibition on Contracting for Hardware, Software, Services Developed or Provided by Kaspersky Lab and other Covered Entities	JUL 2018	
52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment	AUG 2020	
52.209-6	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment	JUN 2020	Applies to Purchase Orders that exceed $35,000, unless the Purchase Order is for COTS items
52.211-15	Defense Priority and Allocation Requirements	APR 2008	Applies to rated Purchase Orders
52.212-4	Contract Terms and Conditions—Commercial Products and Commercial Services	NOV 2023	Only Paragraphs (f), (h), (k), (l), (m), (o), (q), (r) and (u) apply to Purchase Orders; Alt I applies to time-and-materials and labor-hour Purchase Orders
52.219-8	Utilization of Small Business Concerns	FEB 2024	Applies if the Purchase Order offers further subcontracting opportunities
52.219-28	Post-Award Small Business Program Representation	FEB 2024	
52.222-3	Convict Labor	JUN 2003	
52.222-19	Child Labor – Cooperation with Authorities and Remedies	JAN 2020	
52.222-35	Equal Opportunity for Veterans	JUN 2020	Applies if the Purchase Order has a value of $150,000 or more
52.222-36	Equal Opportunity for Workers with Disabilities	JUN 2020	Applies if the Purchase Order has a value exceeding $15,000
52.222-37	Employment Reports on Veterans	JUN 2020	Applies if the Purchase Order has a value of $150,000 or more

52.222-40	Notification of Employee Rights Under the National Labor Relations Act	DEC 2010	Applies if the Purchase Order has a value exceeding $10,000 and will be performed wholly or partially in the United States
52.222-50	Combating Trafficking in Persons	OCT 2020	Paragraph (h) only applies if any portion of the Purchase Order is for supplies, other than COTS items, acquired outside the United States or services to be performed outside the United States that has an estimated value exceeding $550,000. If paragraph (h) applies to the Purchase Order, Company shall submit to Reseller the certification required by this clause prior to award of the Purchase Order and annually thereafter
52.222-54	Employment Eligibility Verification	OCT 2015	Applies if: (i) the Purchase Order is for services (except Commercial Services (as defined in FAR 2.101) that are part of the purchase of COTS items, or items that would be COTS items, but for minor modifications, performed by COTS providers, normally provided for the COTS item) or construction; (ii) the Purchase Order value exceeds $3,500; and (iii) the Purchase Order includes work performed in the United States
52.223-15	Energy Efficiency in Energy-Consuming Products	MAY 2020	
52.223-18	Encouraging Contractor Policies to Ban Text Messaging while Driving	JUN 2020	
52.225-13	Restrictions on Certain Foreign Purchases	FEB 2021	
52.227-14	Rights in Data - General	MAY 2014	
52.233-3	Protest After Award	AUG 1996	In paragraph (b)(2), the term “30 days” is changed to “15 days”
52.237-3	Continuity of Services	JAN 1991	
52.239-1	Privacy or Security Safeguards	AUG 1996	Applies to Purchase Orders for information technology which require security of information

			technology, and/or are for the design, development, or operation of a system of records using commercial information technology services or support services
52.242-3	Penalties for Unallowable Costs	MAY 2014	Applies to cost-reimbursement Purchase Orders
52.245-1*	Government Property	JAN 2017	
52.245-9	Use and Charges	APR 2012	Applies if FAR 52.245-1 applies to the Purchase Order
52.246-25	Limitation of Liability - Services	FEB 1997	
52.247-64	Preference for Privately Owned U.S.-Flag Commercial Vessels	NOV 2021	Not applicable to Purchase Orders for commercial products or commercial services unless an exception in paragraph (e)(4) of the clause applies
52.251-1	Government Supply Sources	APR 2012	

HSAR Clause	Title	Date	Applicability
3052.203-70	Instructions for Contractor Disclosure of Violations	SEP 2012	
3052.205-70	Advertisements, Publicizing Awards, and Release – Alt I	SEP 2012	
3052.222-70	Strikes or Picketing Affecting Timely Completion of the Contract Work	DEC 2003	
3052.222-71	Strikes or Picketing Affecting Access to a DHS Facility	DEC 2003	
3052.228-70	Insurance	DEC 2003	Applies if the Purchase Order requires work on a Government installation

CLAUSES IN FULL TEXT

Qualified Contractor Personnel

The Contractor shall be responsible for employing technically qualified personnel to perform the

work specified in the Purchase Order. The Contractor shall maintain the personnel, organization, and administrative control necessary to ensure that the work delivered meets the government's specifications and requirements. Each Contractor employee must possess knowledge and experience directly related to work he/she is required to perform under this Purchase Order.

The Government reserves the right, during the life of this Purchase Order, to request work histories on any contractor employee for the purposes of verifying compliance with the above requirements; additionally, the Government reserves the right to review and approve resumes of contractor personnel proposed to be assigned to any Component order. In addition, the contractor shall have the demonstrated ability to reach out to a wide variety of subject matter experts in relevant fields, retain their services, and productively engage them in support of government requirements.

Identification of Contractor Personnel

The Contractor shall ensure that its employees identify themselves as employees of their respective company while working on DHS contracts. For example, contractor personnel shall introduce themselves in person and in voice-mail, and sign attendance logs as employees of their respective companies, and not as DHS employees. The contractor shall ensure that their personnel use the following format signature on all official e-mails generated by DHS computers:

Name
Position or Professional Title
Company Name
Supporting the Component / Component Office of DHS
Phone
Fax
Other contact information as desired

Security Requirements

All contractor personnel under this Purchase Order shall be required to complete DHS Entry on Duty (EOD) and will not be permitted access to DHS facilities, systems and information until EOD status is approved.

The procedures outlined below will be used by the DHS Office of the Chief Security Officer (OCSO), Personnel Security Division (PSD) to process background investigations, EOD determinations, and Fitness determinations, as required, in a timely and efficient manner.

Contractor employees (to include applicants, temporary, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position-sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS OCSO/PSD. Prospective contractor employees shall submit the below completed forms to the DHS

OCSO/PSD. The Standard Form (SF) 85-P must be completed electronically through the Office of Personnel Management's e-QIP SYSTEM. The SF-85P signature pages and other completed forms must be given to the OSCO/PSD no less than thirty (30) calendar days before the start date of the contract or thirty (30) calendar days prior to the requested entry on duty date, for all contractor employees whether a replacement, addition, subcontractor employee, or vendor:

a. Standard Form (SF) 85-P, "Questionnaire for Public Trust Positions"
    i. SF-85P Certification
    ii. SF-85P Authorization for Release of Information
b. FD Form 258, "Fingerprint Card" (2 copies)
c. DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
d. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

Only complete packages will be accepted by the DHS OCSO/PSD. Specific instructions on submission of packages will be provided upon award of the contract.

The DHS OCSO/PSD may, as it deems appropriate, authorize and grant a favorable EOD decision based on preliminary checks. A favorable EOD decision allows a contractor employee to commence work temporarily prior to the completion of the full background investigation. The granting of a favorable EOD decision shall not be considered as assurance that a favorable Fitness determination will follow. In addition, a favorable EOD or Fitness determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the contract. No employee of the contractor shall be allowed unescorted access to a Government facility without a favorable EOD or Fitness determination by the DHS OCSO/PSD.

Limited access to Government buildings is allowable without an EOD decision if the contractor is escorted by a Government employee and the purpose of the visit is to attend a limited number of required briefings or nonrecurring meetings in order to facilitate the transition of a contract. The intent of this statement is to allow a minimum amount of meeting/transition attendances to prepare for the new contract.

The DHS OCSO/PSD shall be notified of all terminations/resignations within five (5) calendar days of occurrence. The contractor shall return to the COR all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to whom it was issued and the last known location and disposition of the pass or card.

When sensitive Government information is processed on Department telecommunications and automated information systems, the contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have a favorable EOD or Fitness determination by the DHS OCSO/PSD, to access this information. Contractors who fail to comply with Department security policy are subject to having their access to Department IT

systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

Requests for Exception to U.S. Citizenship Requirement

Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. citizens. Under normal circumstances, only U.S. citizens are allowed access to DHS systems and networks; but there is a need at times to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to citizenship requirements are treated differently from security policy waivers. Exceptions to the U.S. citizenship requirement should be requested by completing a Foreign National Visitor Access Request, DHS Form 11052-1, which is available online or through the DHS Office of the Chief Security Officer (OCSO). Components who have access may file their request via the Foreign National Vetting Management System (FNVMS), a part of the DHS OCSO Integrated Security Management System's (ISMS).

For further information regarding the citizenship exception process, contact the DHS OCSO
This Policy Directive and the DHS 4300A Sensitive Systems Handbook apply to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS information unless an approved waiver has been granted. This includes prototypes, telecommunications systems, and all systems in all phases of the Systems Engineering Life Cycle (SELC).

Failure to follow these instructions may delay the completion of background investigations, EOD and Fitness determinations. Note that any delays in this process, which are not caused by the Government, do not relieve a contractor from performing under the terms of the contract.
Your POC at the Security Office is: DHS OCSO/PSD Security Customer Service Center
Telephone: (202) 447-5010
E-mailbox: officeofsecurity@dhs.gov.

Disclosure of Information

1. Contractor is reminded that information incorporated into the Purchase Order may be subject to disclosure under the Freedom of Information Act (FOIA). See paragraph (e) of FAR 52.212-1, Instructions to Offerors – Commercial Items, for guidance on marking data submitted as part of a quotation for the IDIQ contract or for an order.

2. Any information made available to Contractor by the Government or Reseller must be used only for the purpose of carrying out the provisions of this Purchase Order and all subsequent orders and must not be divulged or made known in any manner to any person except as may be necessary in the performance of the order.

3. In performance of this Purchase Order, Contractor assumes responsibility for protection of the confidentiality of Government records and must ensure that all work performed by its

subcontractors shall be under the supervision of Contractor or Contractor's responsible employees.

4. Each officer or employee of Contractor or any of its subcontractors to whom any Government record may be made available or disclosed must be notified in writing by Contractor that information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein.

52.204-23 PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED E NTITIES (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://dibne t.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.

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

(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;

(i) 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-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;

(2) 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);

(3) 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);

(4) 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

(5) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (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)(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 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)(1)(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 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.

(e) 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)

52.222-19 Child Labor—Cooperation with Authorities and Remedies. (DEVIATION 20-07)

(a) Applicability. This clause does not apply to the extent that the Contractor is supplying end products mined, produced, or manufactured in—

(1) Israel, and the anticipated value of the acquisition is $50,000 or more;

(2) Mexico, and the anticipated value of the acquisition is $83,099 or more; or

(3) Armenia, Aruba, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, Ireland, Italy, Japan, Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Singapore, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Taiwan, Ukraine, or the United Kingdom and the anticipated value of the acquisition is $182,000 or more.

(b) Cooperation with Authorities. To enforce the laws prohibiting the manufacture or importation of products mined, produced, or manufactured by forced or indentured child labor, authorized officials may need to conduct investigations to determine whether forced or indentured child labor was used to mine, produce, or manufacture any product furnished under this contract. If the solicitation includes the provision 52.222-18, Certification Regarding Knowledge of Child Labor for Listed End Products, or the equivalent at 52.212-3(i), the Contractor agrees to cooperate fully with authorized officials of the contracting agency, the Department of the Treasury, or the Department of Justice by providing reasonable access to records, documents, persons, or premises upon reasonable request by the authorized officials.

(c) Violations. The Government may impose remedies set forth in paragraph (d) for the following violations:

(1) The Contractor has submitted a false certification regarding knowledge of the use of forced or indentured child labor for listed end products.

(2) The Contractor has failed to cooperate, if required, in accordance with paragraph (b) of this clause, with an investigation of the use of forced or indentured child labor by an Inspector General, Attorney General, or the Secretary of the Treasury.

(3) The Contractor uses forced or indentured child labor in its mining, production, or manufacturing processes.

(4) The Contractor has furnished under the contract end products or components that have been mined, produced, or manufactured wholly or in part by forced or indentured child

labor. (The Government will not pursue remedies at paragraph (d)(2) or paragraph (d)(3) of this clause unless sufficient evidence indicates that the Contractor knew of the violation.)

(d) Remedies.

(1) The Contracting Officer may terminate the contract.

(2) The suspending official may suspend the Contractor in accordance with procedures in FAR Subpart 9.4.

(3) The debarring official may debar the Contractor for a period not to exceed 3 years in accordance with the procedures in FAR Subpart 9.4.

(End of clause)

52.232-40 Providing Accelerated Payments to Small Business Subcontractors (DEC 2013) (DEVIATION APR 2020)

(a)

(1) In accordance with 31 U.S.C. 3903 and 10 U.S.C. 2307, upon receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract in accordance with the accelerated payment date established, to the maximum extent practicable and prior to when such payment is otherwise required under the applicable contract or subcontract, with a goal of 15 days after receipt of a proper invoice and all other required documentation from the small business subcontractor if a specific payment date is not established by contract.

(2)The Contractor agrees to make such payments to its small business subcontractors without any further consideration from or fees charged to the subcontractor.

(b)The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

(c)Include the substance of this clause, including this paragraph ©, in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial items.

(End of clause)

HSAR 3052.204-71 Contractor Employee Access (SEP 2012)

(a) Sensitive Information, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of clause)

Alternate I
(SEP 2012)
When the contract will require Contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the IDIQ, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and

(2) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

3052.209-73 Limitation of future contracting (JUN 2006)

(a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of the contractor is invited to FAR Subpart 9.5--Organizational Conflicts of Interest.

(b) The nature of this conflict is [Applicable at the task order level, as appropriate].

(c) The restrictions upon future contracting are as follows:

(1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing DHS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract). DHS shall not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.

(2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

The Contracting Officer's determination described above will be made at the task order level.

HSAR 3052.215-70 Key Personnel or Facilities (DEC 2003)

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

Any Key Personnel will be identified in the Purchase Order.

HSAR 3052.225-70 Requirement for Use of Certain Domestic Commodities (AUG 2009)

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

(1) Commercial," as applied to an item described in subsection (b) of this clause, means an item of supply, whether an end product or Component, that meets the definition of "commercial item" set forth in (FAR) 48 CFR 2.101.

(2) Component" means any item supplied to the Government as part of an end product or of another Component.

(3) End product" means supplies delivered under a line item of this contract.

(4) Non-commercial," as applied to an item described in subsections (b) or (c) of this clause, means an item of supply, whether an end product or Component, that does not meet the definition of “commercial item” set forth in (FAR) 48 CFR 2.101.

(5) Qualifying country" means a country with a memorandum of understanding or international agreement with the United States under which DHS procurement is covered.

(6) United States" includes the possessions of the United States.

(b) The Contractor shall deliver under this contract only such of the following commercial or noncommercial items, either as end products or Components, that have been grown, reprocessed, reused, or produced in the United States:

(1) Clothing and the materials and Components thereof, other than sensors, electronics, or other items added to, and not normally associated with, clothing and the materials and Components thereof; or

(2) Tents, tarpaulins, covers, textile belts, bags, protective equipment (such as body armor), sleep systems, load carrying equipment (such as field packs), textile marine equipment, parachutes or bandages.

(c) The Contractor shall deliver under this contract only such of the following non-commercial items, either as end products or Components, that have been grown, reprocessed, reused, or produced in the United States:

(1) Cotton and other natural fiber products.

(2) Woven silk or woven silk blends.

(3) Spun silk yarn for cartridge cloth.

(4) Synthetic fabric or coated synthetic fabric (including all textile fibers and yarns that are for use in such fabrics).

(5) Canvas products.

(6) Wool (whether in the form of fiber or yarn or contained in fabrics, materials, or manufactured articles).

(7) Any item of individual equipment manufactured from or containing any of the fibers, yarns, fabrics, or materials listed in this paragraph (c).

(d) This clause does not apply--

(1) To items listed in (FAR) 48 CFR 25.104, or other items for which the Government has determined that a satisfactory quality and sufficient quantity cannot be acquired as and when needed at United States market prices;

(2) To incidental amounts of cotton, other natural fibers, or wool incorporated in an end product, for which the estimated value of the cotton, other natural fibers, or wool is not more than 10 percent of the total price of the end product; or

(3) To items that are eligible products per (FAR) 48 CFR Subpart 25.4.

(End of clause)

25.0 DHS Special Clause Class Deviation 15-01

25.1 INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Security Training Requirements.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually, and the COR will provide notification when a review is required.

(c) Privacy Training Requirements. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take

Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)

25.2 SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Definitions. As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under

criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation

(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) Authorities. The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) Handling of Sensitive Information. Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook provide the policies and procedures on security for Information Technology (IT) resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program

establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute DHS Form 11000¬6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) Authority to Operate. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.
(1) Complete the Security Authorization process. The SA process shall proceed according to the DHS Sensitive Systems Policy Directive 4300A (Version 11.0, April 30, 2014), or any successor publication, DHS 4300A Sensitive Systems Handbook (Version 9.1, July 24, 2012), or any successor publication, and the Security Authorization Process Guide including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90-day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) Security Review. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and

confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) Continuous Monitoring. All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with FIPS 140-2 Security Requirements for Cryptographic Modules and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) Revocation of ATO. In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) Federal Reporting Requirements. Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) Sensitive Information Incident Reporting Requirements.

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with 4300A Sensitive Systems Handbook Incident Response and Reporting requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use FIPS 140-2 Security Requirements for Cryptographic Modules compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same

email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in 4300A Sensitive Systems Handbook Incident Response and Reporting, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);

(ii) Contract numbers affected unless all contracts by the company are affected;

(iii) Facility CAGE code if the location of the event is different than the prime contractor location;

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);

(v) Contracting Officer POC (address, telephone, email);

(vi) Contract clearance level;

(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;

(viii) Government programs, platforms or systems involved;

(ix) Location(s) of incident;

(x) Date and time the incident was discovered;

(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;

(xii) Description of the Government PII and/or SPII contained within the system;

(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and

(xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,

(ii) Investigations,

(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) Additional PII and/or SPII Notification Requirements.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) Credit Monitoring Requirements. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or
(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and

(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;

(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;

(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;

(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) Certification of Sanitization of Government and Government-Activity-Related Files and Information. As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in NIST Special Publication 800-88 Guidelines for Media Sanitization.

(End of clause)