

**CUSTOMER CONTRACT REQUIREMENTS
HWW Services RMAN/RMON/E-RMAN
CUSTOMER CONTRACT H98230-21-C-0145**

CUSTOMER CONTRACT REQUIREMENTS

The following customer contract requirements apply to this Contract to the extent indicated below. Please note, the requirements below are developed in accordance with Buyer's prime contract and are not modified by Buyer for each individual Seller or statement of work. Seller will remain at all times responsible for providing to any government agency, Buyer, or Buyer's customer, evidence of compliance with the requirements herein or that such requirements are not applicable to the extent satisfactory to the requesting party.

1. FAR Clauses The following contract clauses are incorporated by reference from the Federal Acquisition Regulation and apply to the extent indicated. In all of the following clauses, "Contractor" and "Offeror" mean Seller.

52.203-13 Contractor Code of Business Ethics and Conduct (JUN 2020). This clause applies if this contract exceeds the threshold specified in FAR 3.1004 (a) on the date of contract award and has a performance period of more than 120 days.

52.203-15 Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (JUN 2010). This clause applies if this contract is funded in whole or in part with Recovery Act funds.

52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017).

52.204-13 System for Award Management Maintenance. (OCT 2018).

52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (JUL 2018). In paragraph (c)(1), the term "Government" means "Government or Buyer" and the term "Contracting Officer" means "Buyer." All reporting required by paragraph (c) shall be reported through Buyer. Seller shall report the information in paragraph (c)(2) to Buyer.

52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (AUG 2020). Paragraph (b)(2) is deleted. Paragraph (d)(1) is deleted and replaced with the following: "In the event Seller 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 Seller is notified of such by a subcontractor at any tier or any other source, Seller shall report the information in paragraph (d)(2) of this clause via email to Buyer's Authorized Procurement Representative, with the required information in the body of the email.

52.211-15 Defense Priority and Allocation Requirements (APR 2008). This clause is applicable if a priority rating is noted in this contract.

52.212-4 Contract Terms and Conditions-Commercial Items (OCT 2018). Only paragraph (u) of this clause applies.

52.219-8 Utilization of Small Business Concerns (OCT 2018).

52.222-21 Prohibition of Segregated Facilities (APR 2015).

52.222-26 Equal Opportunity (SEP 2016).

52.222-35 Equal Opportunity for Veterans. (JUN 2020). This clause applies if this contract is valued at or above the threshold specified in FAR 22.1303(a) on the date of subcontract award, unless exempted by rules, regulations or orders of the Secretary of Labor.

52.222-36 Equal Opportunity for Workers with Disabilities (JUN 2020). This clause applies if this contract is in excess of the threshold specified in Federal Acquisition Regulation (FAR) 22.1408(a) on the date of contract award, unless exempted by rules, regulations, or orders of the Secretary.

52.222-37 Employment Reports on Veterans (JUN 2020). This clause applies if this contract is valued at or above the threshold specified in FAR 22.1303(a) on the date of subcontract award, unless exempted by rules, regulations, or orders of the Secretary of Labor.

52.222-40 Notification of Employee Rights Under the National Labor Relations Act. (DEC 2010).

52.222-41 Service Contract Labor Standards (AUG 2018). This clause applies if this contract is subject to the Service Contract Labor Standards statute. Where applicable, Wage Determination(s) shall be attached to the purchase contract at the time of award, or furnished upon request.

52.222-50 Combating Trafficking in Persons (OCT 2020). The term "contractor" shall mean "Seller", except in the paragraph (a) definition of Agent, and except when the term "prime contractor" appears, which shall remain unchanged. The term "Contracting Officer" shall mean "Contracting Officer, Buyer's Authorized Procurement representative" in paragraph (d)(1). Paragraph (d)(2) shall read as follows: "If the allegation may be associated with more than one contract, the Seller shall inform the Buyer's Authorized Procurement Representative for each affected contract." The term "the Government" shall mean "the Government and Buyer" in paragraph (e). The term "termination" shall mean "Cancellation" and "Cancellation for Default", respectively, in paragraph (e)(6). The term "Contracting Officer" shall mean "Contracting Officer and Buyer" in paragraph (f), except in paragraph (f)(2), where it shall mean "Contracting Officer or Buyer". Paragraph (h)(2)(ii) shall read as follows: "To the nature and scope of the activities involved in the performance of a Government subcontract, including the number of non-United States citizens expected to be employed and the risk that the contract or subcontract will involve services or supplies susceptible to trafficking in persons." The term "Contracting Officer" shall mean "Contracting Officer or Buyer" in paragraph (h)(4)(ii). The term "Contracting Officer" shall mean "Buyer" in paragraph (h)(5).

52.222-51 Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (MAY 2014). This clause applies only for exempt services under this Contract. Seller shall provide the certification contained in FAR 52.222-48 Exemption from Application of Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Certification, paragraph (a) to Buyer should Seller intend to rely on 52.222-51.

52.222-53 Exemption From Application Of The Service Contract Labor Standards To Contracts For Certain Services-Requirements (MAY 2014). This clause applies to contracts for exempt services.

52.222-54 Employment Eligibility Verification (OCT 2015). This clause applies to all subcontracts that (1) are for (i) commercial or noncommercial services (except for commercial services that are part of the purchase of a COTS item, or an item that would be a COTS item, but for minor modifications performed by the COTS provider and are normally provided for that COTS item), or (ii) construction; (2) has a value of more than \$3,500; and (3) includes work performed in the United States.

52.222-55 Minimum Wages Under Executive Order 13658 (NOV 2020). This clause applies if this contract is subject to the Service Contract Labor Standards statute or the Wage Rate Requirements (Construction) statute, and is to be performed in whole or in part in the United States. "Contracting Officer" shall mean "Buyer" except for paragraphs (e)(2), (4) and (g). If the Government exercises a withhold identified in the paragraph (g) against Buyer as a result of the Seller's violation of its obligations under this clause, Buyer may impose that withhold against the Seller.

52.222-62 Paid Sick Leave Under Executive Order 13706 (JAN 2017). This clause applies if the Contract is subject to the Service Contract Labor Standards statute or the Wage Rate Requirements (Construction) statute, and are to be performed in whole or in part in the United States.

52.224-3 Privacy Training (JAN 2017). The term "Contracting Officer" shall mean "Contracting Officer or Buyer".

52.224-3 Privacy Training Alternate I (JAN 2017). The term "Contracting Officer" shall mean "Contracting Officer or Buyer".

52.225-13 Restriction on Certain Foreign Purchases (FEB 2021).

52.225-26 Contractors Performing Private Security Functions Outside the United States (OCT 2016). This clause applies if the Contract will be performed outside the United States in areas of (1) combat operations, as designated by the Secretary of Defense; or (2) other significant military operations, upon agreement of the Secretaries of Defense and State that the clause applies in that area. In paragraph (d)(1), Contracting Officer shall mean "Contracting Officer or Buyer" and in paragraph (d) (3), Contracting Officer shall mean Buyer.

52.226-6 Promoting Excess Food Donation to Nonprofit Organizations. (JUN 2020). This clause applies if this contract exceeds the threshold specified in FAR 26.404 on the date of subcontract award and Seller will perform the provision, service, or sale of food in the United States under this contract.

52.227-2 Notice and Assistance Regarding Patent and Copyright Infringement (JUN 2020). This clause applies if the contract is expected to exceed the simplified acquisition threshold, as defined in Federal Acquisition Regulation (FAR) 2.101 on the date of subcontract award. A copy of each notice sent to the Government shall be sent to Buyer.

52.232-40 Providing Accelerated Payments to Small Business Subcontractors. (DEC 2013). This clause applies to contracts with small business concerns. The term "Contractor" retains its original meaning.

52.247-64 Preference for Privately Owned U.S.-Flag Commercial Vessels (FEB 2006). This clause does not apply if this contract is for the acquisition of commercial items unless (i) this contract is a contract or agreement for ocean transportation services; or a construction contract; or (ii) the supplies being transported are (a) items the Seller is reselling or distributing to the Government without adding value (generally, the Seller does not add value to the items when it subcontracts items for f.o.b. destination shipment); or (b) shipped in direct support of U.S. military (1) contingency operations; (2) exercises; or (3) forces deployed in connection with United Nations or North Atlantic Treaty Organization humanitarian or peacekeeping operations.

2. DoD FAR Supplement Clauses DoD Contracts. The following contract clauses are incorporated by reference from the Department of Defense Federal Acquisition Regulation Supplement and apply to the extent indicated. In all of the following clauses, "Contractor" and "Offeror" mean Seller except as otherwise noted.

252.204-7000 Disclosure of Information (OCT 2016). Seller shall submit requests for authorization to release information through Buyer. Seller shall submit written requests to Buyer a minimum of 25 days prior to proposed date of release.

252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information (OCT 2016). This clause applies to contracts for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including contracts for commercial items.

252.225-7012 Preference for Certain Domestic Commodities (DEC 2017).

252.243-7001 Pricing of Contract Modifications (DEC 1991).

3. Prime Contract Special Provisions The following prime contract special provisions apply to this purchase order

H98230-21-C-0145 SPECIAL PROVISIONS .

352,204-9009 ACQUISITION OF INFORMATION SYSTEMS SECURITY (INFOSEC) PRODUCTS, AND THEIR ELECTRONIC COMPONENTS AND PARTS, FROM OUTSIDE THE UNITED STATES (OCT 2011)

(a) Definitions

(1) Component. as used in this provision. means electronic assembly or subassembly incorporated directly into an end product. An electronic assembly is a group of electronic parts, elements, subassemblies, and circuits assembled as a separately removable item of INFOSEC equipment. A subassembly is a major subdivision or an electronic assembly.

(2) Contractor, as used in this provision, means the supplier of the end item and associated support items to the government under the terms of a specific contract.

(3) Information systems security product. as used in this provision, means any item (e.g.. chip, module. assembly, or equipment), technique, or service that performs or relates to information systems security.

(4) Part, as used in this provision, means any single, unassembled element of a major or minor subassembly, accessory, or attachment that is not normally subject to disassembly without the destruction or the impairment of the design use.

(5) Subcontractor, as used in this provision, means a person or business that contracts to provide some service or material necessary for the performance or another's contract.

(6) United States, as used in this provision, means the 50 states and the District of Columbia, Puerto Rico, Guam, American Samoa, the U.S. Virgin Islands, the Northern Mariana Islands, and any other territory or possession over which the United States exercises sovereignty. It is synonymous with "onshore."

(7) Vendor or Supplier, as used in this provision, means a person, company, or agency that sells or supplies materials to a contractor or subcontractor.

(b) An Anonymity Plan is required when INFOSEC products and their electronic components and parts are acquired from sources outside the United States. An Anonymity Plan must be approved before a waiver will be considered for any offshore procurement of INFOSEC products, and their electronic components and parts. At a minimum, the Anonymity Plan should include an outline of offshore procurement procedures that are used for the acquisition of INFOSEC products and their electronic components and parts. Emphasis is placed on establishing offshore procurement procedures ensuring the Seller's subcontractor or vendor of these items remains unaware the Department of Defense/Maryland Procurement Office (MPO) is the recipient of these items.

(c) No Seller subcontracts or purchase orders involving design, manufacture, production, assembly, inspection, or testing outside of the U.S. of INFOSEC product and their electronic components, and parts, for use in INFOSEC systems shall be made under this contract without the prior written approval of the Contracting Officer, requested and provided via the Buyer. Under no circumstances shall any custom integrated circuit, hybrid, multichip module or the documentation associated with these devices or any likeness, thereof, be sent outside the U.S. for additional processing or assembly. In addition, all memory devices, including field programmable gate arrays (FPGAs), with security-related functions shall be programmed onshore.

(d) Requests for permission to deviate from the requirements of paragraph (c).above, are handled on a case-by-case basis through the Buyer. Include in each letter request a strong and compelling reason why the request should be granted in addition to the benefit the Government would gain by granting the request. The Seller shall demonstrate to the Government and Buyer, through submission of an acceptable Communications Security (COMSEC) Anonymity Plan(data Item DI-MGMT-81717C). that procedures are in place to ensure that the offshore vendor/supplier remains unaware of the relationship between the Buyer and the Department of Defense/Maryland Procurement Office (MPO). At a minimum, the following conditions will be imposed if the request is granted:

(1) Purchase orders and drawings provided to a Seller subcontractor or vendor/supplier outside of the United States shall not carry any identification that reveals a contractor relationship with the Department of Defense/MPO. This restriction includes the Buyer's prime contract number with the government and 98230/0NXXXXXX parts identification numbers.

(2) The Seller, when required to mark items with the manufacturer's code 98230 or drawing numbers 0NXXXXXX, shall only mark these items at a facility located within the United States. Marking parts with ON markings and the 98230 code specifies that the parts are for MPO use only. If parts marked with the MPO Identification code (including rejects and parts not usable for MPO programs) are allocated for non-MPO programs or for resale to other customers, then markings associated with the MPO identification code must be removed from the parts before the parts are sent to non-MPO programs or other customers.

(e) The Buyer has the right to an equitable adjustment to the contract price as consideration for granting approval to acquire INFOSEC products, and their electronic components and parts, from sources outside the United States (unless a waiver was granted prior to contract award).

(End of Clause)

352.204-9014 NOTIFICATION OF NON-U.S. CITIZEN PARTICIPATION (OCT 2011)

The Seller shall notify the Buyer thirty (30) calendar days prior to any new Non-U.S. citizen participation on this contract.

The following information should be provided for each individual:

Last Name: _____

First Name: _____

Middle Name: _____

Alias (if any): _____

Place of Birth: _____

Date of Birth: _____

Nationality: _____

Employer Name and Address: _____

Residence including street address: _____

• Other Identifying Information: _____

Scope of *Work* to be performed by non-U.S. citizen participant

NOTICE: This Agency may prohibit non-U.S. citizens from all *or* certain aspects of the work to be performed under any resulting contract.

(End or Clause)

352.204-9015 ABSENT WITHOUT LEAVE (AWOL) REPORTING RESPONSIBILITIES {JUL 2009}

References to Contractor in this article refer to Seller.

(a) The Contractor Special Security Officer (CSSO) shall advise National Security Agency (NSA) cleared contractor personnel or their responsibility to contact their management and the respective site official (that is, the person that is responsible for ensuring that personnel have reported to their work site) should they be forced to take unexpected leave.

(b) If the site official is not a contractor management official, the site official will notify contractor management *or* the CSSO in the event that a contractor employee is Absent Without Leave (AWOL) for more than one hour. The company shall make all reasonable attempts to locate the contractor employee within the second hour of the workday. If after the second hour, the contractor employee has not been located or an explanation received, contractor management shall ensure that the CSSO has been notified. The CSSO shall attempt to locate the contractor employee during the next hour. If the CSSO is unable to locate the contractor employee, the CSSO shall notify the Associate Directorate Security & Counterintelligence (ADS&CI), specifically Industrial Security, 0131, or the Security Operations Command Center (SOCC) at 301-688-6911 after hours.

(c) This shall be a mandatory clause in all contracts and subcontracts at any tier.

(End or Provision)

352.211-9006 NOTICE: ELIMINATION OF USE OF CLASS I OZONE-DEPLETING SUBSTANCES (AUG 1993)

Section 326 of the FY-93 Defense Authorization Act places restrictions on the award and modification or contract is

requiring the use of Class 1-Ozone depleting substances (ODS), Class I ODS are identified in Section 602(a) or the Clean Air Act (42U.S.C. Section 7671(a) and Title 40, Code of Federal Regulations Section 82. Appendix A.

DoD has identified hundreds of military specifications that require Class I ODS. Of these, MPO research indicates that MIL-STD 454, MIL-T-2000, and MIL-T11268 are of particular applicability to some MPO contracts, although others may also apply.

If any of these specifications are included in this acquisition, or if the Seller knows of any other Class I ODS required directly or indirectly at any level or contract performance, the Seller should notify the Buyer immediately. A subsequent assessment will be conducted by the Buyer and/or Government in an attempt to identify economically feasible substitute substances or alternative technology.

(End or Provision)

352,247-9011 SHIPMENT OF UNCLASSIFIED CARGO TO U.S. GOVERNMENT FACILITIES OUTSIDE THE CONTINENTAL UNITED STATES (JUN 2011)

Definitions. As used In this clause:

"Tamper Evident Measures means a device or process that makes unauthorized access to the protected object easily detected.

Shipments of unclassified cargo to any U.S. Government facility outside the continental United States (OCONUS), regardless of whether the shipment originates inside or outside the United States, require the application of tamper evident measures. Tamper evident measures shall be applied to the cargo or conveyance method prior to departure at the point of origin. Acceptable measures shall meet best industry practices and include, at a minimum, inspectable tapes; labels: International Standards Organization (ISO), Publicly Available Standard (PAS) 17712-compliant truck seals, or equivalent; ISO PAS 17712-compliant or equivalent sea container seals; and tamper evident shrink-wrap solutions. The tamper evident measures used

must ensure, to the maximum extent practicable, that the integrity of the cargo remains secure throughout the entire shipping process. Any questions shall be addressed to 443-479•7311.

Information describing the tamper evident measures applied to the cargo shall be documented on the Commercial Bill of Lading or other supporting documentation and accompany the shipment. Documentation or tamper evident measures applied to a shipment shall be sufficient for the end user or responsible receiving party to inspect and authenticate the integrity of the shipment (that is, shipment has not been tampered with while in transit without the need to open or damage the tamper evident measures).

This clause is applicable to all Seller and subcontractors at any tier.

(End or Clause)

352.290-9012 SUPPORT OF ACTIVITIES THAT MAY AFFECT U.S. PERSONS (JAN 2019)

(a) If performance under this contract entails the support of Government activities involving the collection, processing, retention, and/or dissemination of SIGINT information that must be conducted in a manner that protects the privacy rights of U.S. persons. All work and services to be performed hereunder shall be in strict compliance with OIRNSA's SJGINT authorities, NSA/CSS dissemination rules, security directives and procedures, and intelligence oversight policies and directives, including the following:

- (1) Executive Order 12333;
- (2) DoD Manual 5240.01 & DoD 5240.1-R;
- (3) DoD Directive (DoDD) 5148.13;
- (4) NSA/CSS Policy No. 1-23;
- (5) National Security Council Intelligence Directive (NSCID) 6;
- (6) United States Signals Intelligence Directive (USSID) SP0018;
- (7) USSID SP0019;
- (8) NSA/CSS Policy No. 1-46;
- (9) Applicable Foreign Intelligence Surveillance Act procedures; and
- (10) Any other applicable authorities governing activities that may affect U.S. persons

and/or the handling or SIGINT material.

(b) The Seller and its personnel shall thoroughly review the above-referenced materials and abide by them and all NSA oversight and implementing policies, procedures, and legal interpretations thereof. Seller personnel shall also complete and abide by applicable NSA briefings and training, the content and extent of which may vary depending on the specific roles and responsibilities of Seller personnel, the information to which they will require access, and the Government offices that are supported (e.g., training may be more extensive and frequent as the level or exposure to U.S. person information increases). At a minimum, all Seller personnel completing the work describe in (a) above shall complete basic intelligence oversight training.

(c) Periodic review (e.g., annually, semi-annually, etc.) or some or all of the references set forth in section (a), at a frequency and in a manner dictated by the Buyer or sponsoring Government office (i.e., the office or offices that are supported by the Contractor personnel), shall be completed by the Seller personnel.

(d) The use of self-paced resources may be available for some of the briefings, training, and reviews or applicable authorities that are mandated during the contract performance. To ensure that unreasonable amounts of time are not devoted to the completion of such self-paced materials, the following time limit applies to non-firm fixed price contracts (e.g., cost-reimbursement, time and materials, labor hours). Seller personnel are authorized no more than two hours to complete each such briefing, training session, or mandatory review. This limit should afford more than adequate time for thorough review and completion, and the allotment of more than two hours is considered unreasonable. Requests to expend additional time for the completion of a self-paced briefing, training session, or review must be approved in advance by the Government Contracting Officer, as requested through and communicated by the Buyer.

(e) As a precondition to performance under this contract of any of the scope identified in (a) above, each Seller employee will be required to sign an individual statement acknowledging the responsibilities detailed in this clause, including but not limited to the duty to report under DoO 5148.13 any questionable intelligence activity or significant or highly sensitive matter to the NSA Office of General Counsel or NSA Inspector General.

(End of Clause)

352.290-9014 CONTRACTOR USE OF GOVERNMENT INFORMATION SYSTEMS (MAY 2007)

Sellers that require access to NSA/CSS Government Information Systems (GIS) shall comply with the NSA/CSS Policy 6-4, Contractor Use of Government Information Systems. The GIS includes any equipment owned, leased, controlled, or operated on behalf of NSA/CSS through contract as defined within the policy. NSA/CSS Policy 6-4 is applicable to all NSA/CSS Sellers, contractors, subcontractors, and their personnel that use, implement, maintain, or have access to GIS. A copy of NSA/CSS Policy 6-4 can be accessed via the Acquisition Resource Center (ARC) (www.nsaarc.net) by clicking the "Acquisition News" link.

(End of Clause)

352.290-9017 PROTECTION OF UNCLASSIFIED DOD INFORMATION ON NON-DOD SYSTEMS (SEP 2009)

(a) Definitions.

(1) DoD information. Any information that has not been cleared for public release in accordance with DoD Directive 5230.09, "Clearance of DoD information for Public Release," and that is provided by the Department of Defense to a non-DoD entity, or that is collected, developed, received, transmitted, used, or stored by a non-DoD entity in support of an official DoD activity.

(2) Non-DoD entity. Any person who is not a civilian employee or military member of the Department of Defense, or any entity or organization that is not a DoD Component. This includes any non-DoD Federal agency and its personnel, and any contractor, grantee, awardee, partner, or party to any form of legal agreement or understanding with the Department of Defense or another Federal agency.

(3) Non-DoD Information system. Any information system that is not owned, used, or operated by the Department of Defense and that is not used or operated by a contractor or other non-DoD entity on behalf of the Department of Defense.

(b) DOD Information. This clause applies to unclassified DoD Information. Such information may be disseminated by the Seller, Grantee, or Awardee to the extent required to further the contract, grant,

or agreement objectives, provided that the information is disseminated within the scope or assigned duties and with a clear expectation that confidentiality will be preserved. Examples include:

- (1) Non-public Information provided to the Contractor (e.g., with the request for proposal).
- (2) Information developed during the course of the contract, grant, or other legal agreement or understanding (e.g., draft documents, reports, or briefings and deliverables).
- (3) Privileged information contained in transactions (e.g., privileged contract information, program schedules, contract-related event tracking).

(c) Information Safeguards. Seller shall employ the following information safeguards:

- (1) Do not process DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.
- (2) Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.
- (3) Sanitize media (e.g., overwrite) before external release or disposal.
- (4) Encrypt all Information that has been identified as controlled unclassified information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as thumb drives and compact disks, using the best available encryption technology.
- (5) Limit Information transfer to subcontractors or teaming partners with a need to know and a commitment to at least the same level of protection.
- (6) Transmit e-mail, text messages, and similar communications using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS). Encrypt organizational wireless connections and use encrypted wireless connection where available when traveling. If encrypted wireless is not available, encrypt application files (e.g., spreadsheet and word processing files), using at least application-provided password protection level encryption.
- (7) Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.
- (8) Do not post DoD Information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control *may* be provided by the Intranet (vice the Web site itself or the application it hosts).
- (9) Provide protection against computer network intrusions and *data* exfiltration, minimally including the following:
 - i. Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.
 - ii. Monitoring and control of both inbound and outbound network traffic as appropriate (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.
 - iii. Prompt application of security-relevant software patches, service packs, and hot fixes.
- (10) Comply with other current Federal and DoD information protection and reporting requirements for specified categories of Information (e.g., medical, critical program information (CPI), personally identifiable Information, export controlled) as specified in contracts, grants, and other agreements.
- (11) Report loss or unauthorized disclosure of information in accordance with contract or agreement requirements and mechanisms.

(d) Flowdown Requirements. Seller shall flow this clause down to all subcontractors and teaming

partners. (End or Clause)