

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT

32a. QUANTITY IN COLUMN 21 HAS BEEN

RECEIVED INSPECTED ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE
--	-----------	---

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE
	32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT <input type="checkbox"/> COMPLETE <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL	37. CHECK NUMBER
--	--------------------	---------------------------------	--	------------------

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY
------------------------	------------------------	-------------

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT	42a. RECEIVED BY (<i>Print</i>)	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT (<i>Location</i>)
		42c. DATE REC'D (<i>YY/MM/DD</i>)

Table of Contents

<u>Section</u>	<u>Description</u>	<u>Page Number</u>
1	Solicitation/Contract Form.....	1
2	Commodity or Services Schedule.....	4
3	Contract Clauses.....	7
	2852.223-70 Unsafe Conditions Due to the Presence of Hazardous Material (June 1996).....	7
	DJAR-PGD-02-02A Non-U.S. Citizens Prohibited from Access to DOJ Information Technology (IT) Systems.....	8
	52.24-403-70 Notice of Contractor Personnel Security Requirements (OCT 2005).....	8
	52.218-000 CONTINUING CONTRACT PERFORMANCE DURING A PANDEMIC INFLUENZA OR OTHER NATIONAL EMERGENCY (May 2008).....	9
	52.21-603-70 Contracting Officer's Representative (COR) (June 2012).....	10
	52.27-103-72 DOJ CONTRACTOR RESIDENCY REQUIREMENT BUREAU OF PRISONS (JUNE 2004).....	10
	DJAR-PGD-15-03 Security of Department Information and Systems.....	10
	52.204-18 Commercial and Government Entity Code Maintenance (Aug 2020).....	15
	52.203-13 Contractor Code of Business Ethics and Conduct (Jun 2020).....	16
	52.213-4 Terms and Conditions-Simplified Acquisitions (Other Than Commercial Items) (Aug 2020).....	18
	52.247-21 Contractor Liability for Personal Injury and/or Property Damage (Apr 1984).....	22
4	List of Attachments.....	23

Section 2 - Commodity or Services Schedule

Contract Guarantee:

Minimum Guaranteed Quantity	Minimum Guaranteed Amount	Maximum Guaranteed Quantity	Maximum Guaranteed Amount
	\$0.00		\$0.00

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	MAX. QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	Tuition FCI Dublin Base Year (12 Months to be Determined by Next College Enrollment date) Modification to Incorporate Dates will need to be done. Firm Fixed Price PSC: U005 Base Period	20	EA	Previous: \$0.0000 Change: \$1,012.0000 Current: \$1,012.0000	Previous: \$0.00 Change: \$20,240.00 Current: \$20,240.00
0002	Books and Supplies FCI Dublin Base Year (12 Months to be Determined by Next College Enrollment date) Firm Fixed Price PSC: 7610 Base Period	20	EA	Previous: \$0.0000 Change: \$660.0000 Current: \$660.0000	Previous: \$0.00 Change: \$13,200.00 Current: \$13,200.00
0003	Other Fees FCI Dublin Base Year (12 Months to be Determined by Next College Enrollment date) Firm Fixed Price PSC: U005 Base Period	0	EA	Previous: \$0.0000 Change: \$0.0000 Current: \$0.0000	Previous: \$0.00 Change: \$0.00 Current: \$0.00

ITEM NO.	SUPPLIES/SERVICES	MAX. QUANTITY	UNIT	UNIT PRICE	AMOUNT
0004	Tuition FCI Dublin Option One Firm Fixed Price PSC: U005 Unexercised Option	20	EA	Previous: \$0.0000 Change: \$1,150.0000 Current: \$1,150.0000	Previous: \$0.00 Change: \$23,000.00 Current: \$23,000.00
0005	Books and Supplies FCI Dublin Option One Firm Fixed Price PSC: 7610 Unexercised Option	20		Previous: \$0.0000 Change: \$670.0000 Current: \$670.0000	Previous: \$0.00 Change: \$13,400.00 Current: \$13,400.00
0006	Other Fees FCI Dublin Option One Firm Fixed Price PSC: U005 Unexercised Option	0	EA	Previous: \$0.0000 Change: \$0.0000 Current: \$0.0000	Previous: \$0.00 Change: \$0.00 Current: \$0.00
0007	Tuition FCI Dublin Option Two Firm Fixed Price PSC: U005 Unexercised Option	20	EA	Previous: \$0.0000 Change: \$920.0000 Current: \$920.0000	Previous: \$0.00 Change: \$18,400.00 Current: \$18,400.00

ITEM NO.	SUPPLIES/SERVICES	MAX. QUANTITY	UNIT	UNIT PRICE	AMOUNT
0008	Books and Supplies FCI Dublin Option Two Firm Fixed Price PSC: 7610 Unexercised Option	20		Previous: \$0.0000 Change: \$679.0000 Current: \$679.0000	Previous: \$0.00 Change: \$13,580.00 Current: \$13,580.00
0009	Other Fees FCI Dublin Option Two Firm Fixed Price PSC: U005 Unexercised Option	0	EA	Previous: \$0.0000 Change: \$0.0000 Current: \$0.0000	Previous: \$0.00 Change: \$0.00 Current: \$0.00
Base Total:					\$33,440.00
Exercised Options Total:					\$0.00
Unexercised Options Total:					\$68,380.00
Base and Options Total:					\$101,820.00

FUNDING DETAILS:

ITEM NO.	FUNDING LINE	OBLIGATED AMOUNT	ACCOUNTING CODES
N/A	1	\$101,820.00	SA-2020-02-FP090022XF-95F-2523-2020
		TOTAL: \$101,820.00	

Notice to Contractor: All contractors must wear a protective vest while at the institution. This will issued to the contractor upon entry. Contractors are not considered employees and must provide identification upon entry of any government facility under this award. Cell phones are never authorized in institutions. Contractors must pass a background investigation before entry of the institution. A badge must be worn at all times by the contractor. Contractors may not respond to any body alarms, mock drills or play any part of Bureau emergency drills. Please ensure your contractor understands that during an emergency, they must ask a point BOP employee to get escorted out of the facility. It is required that they are escorted out for accountability. Although the contractor is performing duties at the institution, they may not wear any Bureau logos or participate in any government functions. Contractor must also abide by standard government policy. Professional Attire is Required. More direction will be issued at the local level. The CEO has the authority to deny entry to the contract employee if any discipline matters arise until contracting is able to address with the authorized party of this award.

Section 3 - Contract Clauses

Clauses By Reference

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)		
This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): www.acquisition.gov		
Clause	Title	Fill-ins (if applicable)
52.249-1	Termination for Convenience of the Government (Fixed-Price) (Short Form) (Apr 1984)	
52.249-8	Default (Fixed-Price Supply and Service) (Apr 1984)	
52.203-7	Anti-Kickback Procedures (Jun 2020)	
52.225-13	Restrictions on Certain Foreign Purchases (June 2008)	
52.232-39	Unenforceability of Unauthorized Obligations (Jun 2013)	
52.233-1	Disputes (May 2014)	
52.233-1 Alt I	Disputes (May 2014) - Alternate I (Dec 1991)	
52.233-4	Applicable Law for Breach of Contract Claim (Oct 2004)	
52.244-6	Subcontracts for Commercial Items (Aug 2020)	

Clauses By Full Text

2852.223-70 Unsafe Conditions Due to the Presence of Hazardous Material (June 1996)

- (a) "Unsafe condition" as used in this clause means the actual or potential exposure of contractor or Government employees to a hazardous material as defined in Federal Standard No. 313, and any revisions thereto during the term of this contract, or any other material or working condition designated by the Contracting Officer's Technical Representative (COTR) as potentially hazardous and requiring safety controls.
- (b) The Occupational Safety and Health Administration (OSHA) is responsible for issuing and administering regulations that require contractors to apprise its employees of all hazards to which they may be exposed in the course of their employment; proper conditions and precautions for safe use and exposure; and related symptoms and emergency treatment in the event of exposure.
- (c) Prior to commencement of work, contractors are required to inspect for and report to the contracting officer or designee the presence of, or suspected presence of, any unsafe condition including asbestos or other hazardous materials or working conditions in areas in which they will be working.
- (d) If during the performance of the work under this contract, the contractor or any of its employees, or subcontractor employees, discovers the existence of an unsafe condition, the contractor shall immediately notify the contracting officer, or designee, (with written notice provided not later than three (3) working days thereafter) of the existence of an unsafe condition. Such notice shall include the contractor's recommendations for the protection and the safety of Government, contractor and subcontractor personnel and property that may be exposed to the unsafe condition.

(e) When the Government receives notice of an unsafe condition from the contractor, the parties will agree on a course of action to mitigate the effects of that condition and, if necessary, the contract will be amended. Failure to agree on a course of action will constitute a dispute under the Disputes clause of this contract.

(f) Nothing contained in this clause shall relieve the contractor or subcontractors from complying with applicable Federal, State, and local laws, codes, ordinances and regulations (including the obtaining of licenses and permits) in connection with hazardous material including but not limited to the use, disturbance, or disposal of such material.

(End of Clause)

DJAR-PGD-02-02A Non-U.S. Citizens Prohibited from Access to DOJ Information Technology (IT) Systems

The Department of Justice does not permit the use of Non-U.S. citizens in the performance of this contract or commitment for any position that involves access to or development of any DOJ IT system. By signing the contract or commitment document, the contractor agrees to this restriction. [In those instances where other non-IT requirements contained in the contract or commitment can be met by using Non-U.S. citizens, those requirements shall be clearly described.].

(End of Clause)

52.24-403-70 Notice of Contractor Personnel Security Requirements (OCT 2005)

Compliance with Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201) ¹ entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," Phase I.

1. Long-Term Contractor Personnel:

In order to be compliant with HSPD-12/PIV I, the following investigative requirements must be met for each new long-term ² contractor employee whose background investigation (BI) process begins on or after October 27, 2005:

- a. Contractor Personnel must present two forms of identification in original form prior to badge issuance (acceptable documents are listed in Form I-9, OMB No. 1615-0047, "Employment Eligibility Verification," and at least one document must be a valid State or Federal government-issued picture ID);
- b. Contractor Personnel must appear in person at least once before a DOJ official who is responsible for checking the identification documents. This identity proofing must be completed sometime during the clearance process but prior to badge issuance and must be documented by the DOJ official;
- c. Contractor Personnel must undergo a BI commensurate with the designated risk level associated with the duties of each position. Outlined below are the minimum BI requirements for each risk level:

- * High Risk - Background Investigation (5 year scope)
- * Moderate Risk - Limited Background Investigation (LBI) or Minimum Background Investigation (MBI)
- * Low Risk - National Agency Check with Inquiries (NACI) investigation

d. The pre-appointment BI waiver requirements for all position sensitivity levels are a:

- 1) Favorable review of the security questionnaire form;
- 2) Favorable fingerprint results;
- 3) Favorable credit report, if required;³
- 4) Waiver request memorandum, including both the Office of Personnel Management schedule date and position sensitivity/risk level; and
- 5) Favorable review of the National Agency Check (NAC) ⁴ portion of the applicable BI that is determined by position sensitivity/risk level.

A badge may be issued following approval of the above waiver requirements.

If the NAC is not received within five days of OPM's scheduling date, the badge can be issued based on a favorable review of the Security Questionnaire and the Federal Bureau of Investigation Criminal History Check (i.e., fingerprint check results).

e. Badge re-validation will occur once the investigation is completed and favorably adjudicated. If the BI results so justify, badges issued under these procedures will be suspended or revoked.

2. Short-Term Contractor Personnel:

It is the policy of the DOJ that short-term contractors having access to DOJ information systems and/or DOJ facilities or space for six months or fewer are subject to the identity proofing requirements listed in items 1a. and 1b. above. The pre-appointment waiver requirements for short-term contractors are:

- a. Favorable review of the security questionnaire form;
- b. Favorable fingerprint results;
- c. Favorable credit report, if required;⁵ and
- d. Waiver request memorandum indicating both the position sensitivity/risk level and the duration of the appointment. The commensurate BI does not need to be initiated.

A badge may be issued following approval of the above waiver requirements and the badge will expire six months from the date of issuance. This process can only be used once for a short-term contractor in a twelve month period. This will ensure that any consecutive short-term appointments are subject to the full PIV-I identity proofing process.

For example, if a contractor employee requires daily access for a three or four-week period, this contractor would be cleared according to the above short-term requirements. However, if a second request is submitted for the same contractor employee within a twelve-month period for the purpose of extending the initial contract or for employment under a totally different contract for another three or four-week period, this contractor would now be considered "long-term" and must be cleared according to the long-term requirements as stated in this interim policy.

3. Intermittent Contractors:

An exception to the above-mentioned short-term requirements would be intermittent contractors.

a. For purposes of this policy, "intermittent" is defined as those contractor employees needing access to DOJ information systems and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access. For example, the water delivery contractor that delivers water one time each week and is working on a one-year contract.

b. Contractors requiring intermittent access should follow the Department's escort policy. Please reference the August 11, 2004, and January 29, 2001, Department Security Officer policy memoranda that conveys the requirements for contractor facility escorted access.

c. Due to extenuating circumstances, if a component requests unescorted access or DOJ IT system access for an intermittent contractor, the same pre-employment background investigation waiver requirements that apply to short-term contractors are required.

d. If an intermittent contractor is approved for unescorted access, the contractor will only be issued a daily badge. The daily badge will be issued upon entrance into a DOJ facility or space and must be returned upon exiting the same facility or space.

e. If an intermittent contractor is approved for unescorted access, the approval will not exceed one year. If the intermittent contractor requires unescorted access beyond one year, the contractor will need to be re-approved each year.

4. An individual transferring from another department or agency shall not be re-adjudicated provided the individual has a current (within the last five years), favorably adjudicated BI meeting HSPD-12 and DOJ's BI requirements.

5. The DOJ's current escorted contractor policy remains unchanged by this acquisition notice.

Notes:

1. FIPS 201 is available at: www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf

2. Under HSPD-12, long-term contractors are contractors having access to DOJ information systems and/or DOJ facilities or space for six months or longer. The PIV-I identity proofing process, including initiation and adjudication of the required background investigation, is required for all new long-term contractors regardless of whether it is the current practice to issue a badge. The second phase of HSPD-12 implementation (PIV-II) requires badge issuance to all affected long-term contractors.

3. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.

4. In order to avoid a delay in the hiring process, components should request an Advance NAC Report when initiating investigations to OPM. Per OPM's instructions, to obtain an Advance NAC Report, a Code " 3" must be placed in block " B " of the " Agency Use Only " section of the investigative form. This report is available for all case types.

5. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.

#

[End of Clause]

52.218-000 CONTINUING CONTRACT PERFORMANCE DURING A PANDEMIC INFLUENZA OR OTHER NATIONAL EMERGENCY (May 2008)

During a Pandemic or other emergency we understand that our contractor workforce will experience the same high levels of absenteeism as our federal employees. Although the Excusable Delays and Termination for Default clauses used in Government contracts list epidemics and quarantine restrictions among the reasons to excuse delays in contract performance, we expect our contractors to make a reasonable effort to keep performance at an acceptable level during emergency periods.

The Office of Personnel Management (OPM) has provided guidance to federal managers and employees on the kinds of actions to be taken to ensure the continuity of operations during emergency periods. This guidance is also applicable to our contract workforce. Contractors are expected to have reasonable policies in place for continuing work performance, particularly those performing mission critical services, during a pandemic influenza or other emergency situation.

The types of actions a federal contractor should reasonably take to help ensure performance are:

- * Encourage employees to get inoculations or follow other preventive measures as advised by the public health service.
- * Cross-train workers as backup for all positions performing critical services. This is particularly important for work such as guard services where telework is not an option.

- * Implement telework to the greatest extent possible in the workgroup so systems are in place to support successful remote work in an emergency.
- * Communicate expectations to all employees regarding their roles and responsibilities in relation to remote work in the event of a pandemic health crisis or other emergency.
- * Establish communication processes to notify employees of activation of this plan.
- * Integrate pandemic health crisis response expectations into telework agreements.
- * With the employee, assess requirements for working at home (supplies and equipment needed for an extended telework period). Security concerns should be considered in making equipment choices; agencies or contractors may wish to avoid use of employees' personal computers and provide them with PCs or laptops as appropriate.
- * Determine how all employees who may telework will communicate with one another and with management to accomplish work.
- * Practice telework regularly to ensure effectiveness.
- * Make it clear that in emergency situations, employees must perform all duties assigned by management, even if they are outside usual or customary duties.
- * Identify how time and attendance will be maintained.

It is the contractor's responsibility to advise the Government Contracting Officer if they anticipate not being able to perform and to work with the Department to fill gaps as necessary. This means direct communication with the Contracting Officer or in his/her absence, another responsible person in the contracting office via telephone or email messages acknowledging the contractor's notification. The incumbent contractor is responsible for assisting the Department in estimating the adverse impacts of nonperformance and to work diligently with the Department to develop a strategy for maintaining the continuity of operations. The Department does reserve the right in such emergency situations to use Federal employees, employees of other agencies, contract support from other existing contractors, or to enter into new contracts for critical support services. Any new contracting efforts would be acquired following the guidance in the Office of federal Procurement Policy issuance "Emergency Acquisitions", May, 2007 and Subpart 18.2. Emergency Acquisition Flexibilities, of the Federal Acquisition Regulations.

[End of Clause]

52.21-603-70 Contracting Officer's Representative (COR) (June 2012)

(a) Renee Corriveau, BOP Education Central Office, Education Specialist, rjcorriveau@bop.gov, is hereby designated as the Contracting Officer's Representative (COR) under this contract.

(b) The COR is responsible, as applicable, for: receiving all deliverables, inspecting and accepting the supplies or services provided hereunder in accordance with the terms and conditions of this contract; providing direction to the contractor which clarifies the contractor effort, fills in details or otherwise serves to accomplish the contractual Scope of Work; evaluating performance; and certifying all invoices/vouchers for acceptance of the supplies or services furnished for payment.

(c) The COR does not have the authority to alter the contractor's obligations under the contract, and/or modify any of the expressed terms, conditions, specifications, or cost of the agreement. If as a result of technical discussions it is desirable to alter/change contractual obligations or the Scope of Work, the Contracting Officer shall issue such changes.

52.27-103-72 DOJ CONTRACTOR RESIDENCY REQUIREMENT BUREAU OF PRISONS (JUNE 2004)

For three of the five years immediately prior to submission of an offer/bid/quote, or prior to performance under a contract or commitment, individuals or contractor employees providing services must have:

1. Legally resided in the United States (U.S.);
2. worked for the U.S. overseas in a Federal or military capacity; or
3. been a dependent of a Federal or military employee serving overseas.

If the individual is not a U.S. citizen, they must be from a country allied with the U.S. The following website provides current information regarding allied countries: <http://www.opm.gov/employ/html/citizen.htm>

By signing this contract or commitment document, or by commencing performance, the contractor agrees to this restriction.

[End of Clause]

I. Applicability to Contractors and Subcontractors

This clause applies to all contractors and subcontractors, including cloud service providers (“CSPs”), and personnel of contractors, subcontractors, and CSPs (hereinafter collectively, “Contractor”) that may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information. It establishes and implements specific DOJ requirements applicable to this Contract. The requirements established herein are in addition to those required by the Federal Acquisition Regulation (“FAR”), including FAR 11.002(g) and 52.239-1, the Privacy Act of 1974, and any other applicable laws, mandates, Procurement Guidance Documents, and Executive Orders pertaining to the development and operation of Information Systems and the protection of Government Information. This clause does not alter or diminish any existing rights, obligation or liability under any other civil and/or criminal law, rule, regulation or mandate.

II. General Definitions

The following general definitions apply to this clause. Specific definitions also apply as set forth in other paragraphs.

- A. **Information** means any communication or representation of knowledge such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual. Information includes information in an electronic format that allows it be stored, retrieved or transmitted, also referred to as “data,” and “personally identifiable information” (“PII”), regardless of form.
- B. **Personally Identifiable Information (or PII)** means any information about an individual maintained by an agency, including, but not limited to, information related to education, financial transactions, medical history, and criminal or employment history and information, which can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.
- C. **DOJ Information** means any Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of the DOJ, including, without limitation, Information related to DOJ programs or personnel. It includes, without limitation, Information (1) provided by or generated for the DOJ, (2) managed or acquired by Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired in order to perform the contract.
- D. **Information System** means any resources, or set of resources organized for accessing, collecting, storing, processing, maintaining, using, sharing, retrieving, disseminating, transmitting, or disposing of (hereinafter collectively, “processing, storing, or transmitting”) Information.
- E. **Covered Information System** means any information system used for, involved with, or allowing, the processing, storing, or transmitting of DOJ Information.

III. Confidentiality and Non-disclosure of DOJ Information

- A. Preliminary and final deliverables and all associated working papers and material generated by Contractor containing DOJ Information are the property of the U.S. Government and must be submitted to the Contracting Officer (“CO”) or the CO’s Representative (“COR”) at the conclusion of the contract. The U.S. Government has unlimited data rights to all such deliverables and associated working papers and materials in accordance with FAR 52.227-14.
- B. All documents produced in the performance of this contract containing DOJ Information are the property of the U.S. Government and Contractor shall neither reproduce nor release to any third-party at any time, including during or at expiration or termination of the contract without the prior written permission of the CO.
- C. Any DOJ information made available to Contractor under this contract shall be used only for the purpose of performance of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this contract. In performance of this contract, Contractor assumes responsibility for the protection of the confidentiality of any and all DOJ Information processed, stored, or transmitted by the Contractor. When requested by the CO (typically no more than annually), Contractor shall provide a report to the CO identifying, to the best of Contractor’s knowledge and belief, the type, amount, and level of sensitivity of the DOJ Information processed, stored, or transmitted under the Contract, including an estimate of the number of individuals for whom PII has been processed, stored or transmitted under the Contract and whether such information includes social security numbers (in whole or in part).

IV. Compliance with Information Technology Security Policies, Procedures and Requirements

A. For all Covered Information Systems, Contractor shall comply with all security requirements, including but not limited to the regulations and guidance found in the Federal Information Security Management Act of 2014 ("FISMA"), Privacy Act of 1974, E-Government Act of 2002, National Institute of Standards and Technology ("NIST") Special Publications ("SP"), including NIST SP 800-37, 800-53, and 800-60 Volumes I and II, Federal Information Processing Standards ("FIPS") Publications 140-2, 199, and 200, OMB Memoranda, Federal Risk and Authorization Management Program ("FedRAMP"), DOJ IT Security Standards, including DOJ Order 2640.2, as amended. These requirements include but are not limited to:

1. Limiting access to DOJ Information and Covered Information Systems to authorized users and to transactions and functions that authorized users are permitted to exercise;
2. Providing security awareness training including, but not limited to, recognizing and reporting potential indicators of insider threats to users and managers of DOJ Information and Covered Information Systems;
3. Creating, protecting, and retaining Covered Information System audit records, reports, and supporting documentation to enable reviewing, monitoring, analysis, investigation, reconstruction, and reporting of unlawful, unauthorized, or inappropriate activity related to such Covered Information Systems and/or DOJ Information;
4. Maintaining authorizations to operate any Covered Information System;
5. Performing continuous monitoring on all Covered Information Systems;
6. Establishing and maintaining baseline configurations and inventories of Covered Information Systems, including hardware, software, firmware, and documentation, throughout the Information System Development Lifecycle, and establishing and enforcing security configuration settings for IT products employed in Information Systems;
7. Ensuring appropriate contingency planning has been performed, including DOJ Information and Covered Information System backups;
8. Identifying Covered Information System users, processes acting on behalf of users, or devices, and authenticating and verifying the identities of such users, processes, or devices, using multifactor authentication or HSPD-12 compliant authentication methods where required;
9. Establishing an operational incident handling capability for Covered Information Systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, and tracking, documenting, and reporting incidents to appropriate officials and authorities within Contractor's organization and the DOJ;
10. Performing periodic and timely maintenance on Covered Information Systems, and providing effective controls on tools, techniques, mechanisms, and personnel used to conduct such maintenance;
12. Protecting Covered Information System media containing DOJ Information, including paper, digital and electronic media; limiting access to DOJ Information to authorized users; and sanitizing or destroying Covered Information System media containing DOJ Information before disposal, release or reuse of such media;
13. Limiting physical access to Covered Information Systems, equipment, and physical facilities housing such Covered Information Systems to authorized U.S. citizens unless a waiver has been granted by the Contracting Officer ("CO"), and protecting the physical facilities and support infrastructure for such Information Systems;
14. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards;
15. Assessing the risk to DOJ Information in Covered Information Systems periodically, including scanning for vulnerabilities and remediating such vulnerabilities in accordance with DOJ policy and ensuring the timely removal of assets no longer supported by the Contractor;
16. Assessing the security controls of Covered Information Systems periodically to determine if the controls are effective in their application, developing and implementing plans of action designed to correct deficiencies and eliminate or reduce vulnerabilities in such Information Systems, and monitoring security controls on an ongoing basis to ensure the continued effectiveness of the controls;

17. Monitoring, controlling, and protecting information transmitted or received by Covered Information Systems at the external boundaries and key internal boundaries of such Information Systems, and employing architectural designs, software development techniques, and systems engineering principles that promote effective security; and
18. Identifying, reporting, and correcting Covered Information System security flaws in a timely manner, providing protection from malicious code at appropriate locations, monitoring security alerts and advisories and taking appropriate action in response.
- B. Contractor shall not process, store, or transmit DOJ Information using a Covered Information System without first obtaining an Authority to Operate (“ATO”) for each Covered Information System. The ATO shall be signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under this contract. The DOJ standards and requirements for obtaining an ATO may be found at DOJ Order 2640.2, as amended. (For Cloud Computing Systems, see Section V, below.)
- C. Contractor shall ensure that no Non-U.S. citizen accesses or assists in the development, operation, management, or maintenance of any DOJ Information System, unless a waiver has been granted by the by the DOJ Component Head (or his or her designee) responsible for the DOJ Information System, the DOJ Chief Information Officer, and the DOJ Security Officer.
- D. When requested by the DOJ CO or COR, or other DOJ official as described below, in connection with DOJ’s efforts to ensure compliance with security requirements and to maintain and safeguard against threats and hazards to the security, confidentiality, integrity, and availability of DOJ Information, Contractor shall provide DOJ, including the Office of Inspector General (“OIG”) and Federal law enforcement components, (1) access to any and all information and records, including electronic information, regarding a Covered Information System, and (2) physical access to Contractor’s facilities, installations, systems, operations, documents, records, and databases. Such access may include independent validation testing of controls, system penetration testing, and FISMA data reviews by DOJ or agents acting on behalf of DOJ, and such access shall be provided within 72 hours of the request. Additionally, Contractor shall cooperate with DOJ’s efforts to ensure, maintain, and safeguard the security, confidentiality, integrity, and availability of DOJ Information.
- E. The use of Contractor-owned laptops or other portable digital or electronic media to process or store DOJ Information covered by this clause is prohibited until Contractor provides a letter to the DOJ CO, and obtains the CO’s approval, certifying compliance with the following requirements:
1. Media must be encrypted using a NIST FIPS 140-2 approved product;
 2. Contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;
 3. Where applicable, media must utilize antivirus software and a host-based firewall mechanism;
 4. Contractor must log all computer-readable data extracts from databases holding DOJ Information and verify that each extract including such data has been erased within 90 days of extraction or that its use is still required. All DOJ Information is sensitive information unless specifically designated as non-sensitive by the DOJ; and,
 5. A Rules of Behavior (“ROB”) form must be signed by users. These rules must address, at a minimum, authorized and official use, prohibition against unauthorized users and use, and the protection of DOJ Information. The form also must notify the user that he or she has no reasonable expectation of privacy regarding any communications transmitted through or data stored on Contractor-owned laptops or other portable digital or electronic media.
- F. Contractor-owned removable media containing DOJ Information shall not be removed from DOJ facilities without prior approval of the DOJ CO or COR.
- G. When no longer needed, all media must be processed (sanitized, degaussed, or destroyed) in accordance with DOJ security requirements.
- H. Contractor must keep an accurate inventory of digital or electronic media used in the performance of DOJ contracts.
- I. Contractor must remove all DOJ Information from Contractor media and return all such information to the DOJ within 15 days of the expiration or termination of the contract, unless otherwise extended by the CO, or waived (in part or whole) by the CO, and all such information shall be returned to the DOJ in a format and form acceptable to the DOJ. The removal and return of all DOJ Information must be accomplished in accordance with DOJ IT Security Standard requirements, and an official of the Contractor shall provide a written certification certifying the removal and return of all such information to the CO within 15 days of the removal and return of all DOJ Information.

J. DOJ, at its discretion, may suspend Contractor's access to any DOJ Information, or terminate the contract, when DOJ suspects that Contractor has failed to comply with any security requirement, or in the event of an Information System Security Incident (see Section V.E. below), where the Department determines that either event gives cause for such action. The suspension of access to DOJ Information may last until such time as DOJ, in its sole discretion, determines that the situation giving rise to such action has been corrected or no longer exists. Contractor understands that any suspension or termination in accordance with this provision shall be at no cost to the DOJ, and that upon request by the CO, Contractor must immediately return all DOJ Information to DOJ, as well as any media upon which DOJ Information resides, at Contractor's expense.

V. Cloud Computing

A. **Cloud Computing** means an Information System having the essential characteristics described in NIST SP 800-145, The NIST Definition of Cloud Computing. For the sake of this provision and clause, Cloud Computing includes Software as a Service, Platform as a Service, and Infrastructure as a Service, and deployment in a Private Cloud, Community Cloud, Public Cloud, or Hybrid Cloud.

B. Contractor may not utilize the Cloud system of any CSP unless:

1. The Cloud system and CSP have been evaluated and approved by a 3PAO certified under FedRAMP and Contractor has provided the most current Security Assessment Report ("SAR") to the DOJ CO for consideration as part of Contractor's overall System Security Plan, and any subsequent SARs within 30 days of issuance, and has received an ATO from the Authorizing Official for the DOJ component responsible for maintaining the security confidentiality, integrity, and availability of the DOJ Information under contract; or,

2. If not certified under FedRAMP, the Cloud System and CSP have received an ATO signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under the contract.

C. Contractor must ensure that the CSP allows DOJ to access and retrieve any DOJ Information processed, stored or transmitted in a Cloud system under this Contract within a reasonable time of any such request, but in no event less than 48 hours from the request. To ensure that the DOJ can fully and appropriately search and retrieve DOJ Information from the Cloud system, access shall include any schemas, meta-data, and other associated data artifacts.

VI. Information System Security Breach or Incident

A. Definitions

1. **Confirmed Security Breach** (hereinafter, "Confirmed Breach") means any confirmed unauthorized exposure, loss of control, compromise, exfiltration, manipulation, disclosure, acquisition, or accessing of any Covered Information System or any DOJ Information accessed by, retrievable from, processed by, stored on, or transmitted within, to or from any such system.

2. **Potential Security Breach** (hereinafter, "Potential Breach") means any suspected, but unconfirmed, Covered Information System Security Breach.

3. **Security Incident** means any Confirmed or Potential Covered Information System Security Breach.

B. **Confirmed Breach.** Contractor shall immediately (and in no event later than within 1 hour of discovery) report any Confirmed Breach to the DOJ CO and the CO's Representative ("COR"). If the Confirmed Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call DOJ-CERT at 1-866-US4-CERT (1-866-874-2378) immediately (and in no event later than within 1 hour of discovery of the Confirmed Breach), and shall notify the CO and COR as soon as practicable.

C. Potential Breach.

1. Contractor shall report any Potential Breach within 72 hours of detection to the DOJ CO and the COR, unless Contractor has (a) completed its investigation of the Potential Breach in accordance with its own internal policies and procedures for identification, investigation and mitigation of Security Incidents and (b) determined that there has been no Confirmed Breach.

2. If Contractor has not made a determination within 72 hours of detection of the Potential Breach whether an Confirmed Breach has occurred, Contractor shall report the Potential Breach to the DOJ CO and COR within one-hour (i.e., 73 hours from

detection of the Potential Breach). If the time by which to report the Potential Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call the DOJ Computer Emergency Readiness Team (DOJ-CERT) at 1-866-US4-CERT (1-866-874-2378) within one-hour (i.e., 73 hours from detection of the Potential Breach) and contact the DOJ CO and COR as soon as practicable.

D. Any report submitted in accordance with paragraphs (B) and (C), above, shall identify (1) both the Information Systems and DOJ Information involved or at risk, including the type, amount, and level of sensitivity of the DOJ Information and, if the DOJ Information contains PII, the estimated number of unique instances of PII, (2) all steps and processes being undertaken by Contractor to minimize, remedy, and/or investigate the Security Incident, (3) any and all other information as required by the US-CERT Federal Incident Notification Guidelines, including the functional impact, information impact, impact to recoverability, threat vector, mitigation details, and all available incident details; and (4) any other information specifically requested by the DOJ. Contractor shall continue to provide written updates to the DOJ CO regarding the status of the Security Incident at least every three (3) calendar days until informed otherwise by the DOJ CO.

E. All determinations regarding whether and when to notify individuals and/or federal agencies potentially affected by a Security Incident will be made by DOJ senior officials or the DOJ Core Management Team at DOJ's discretion.

F. Upon notification of a Security Incident in accordance with this section, Contractor must provide to DOJ full access to any affected or potentially affected facility and/or Information System, including access by the DOJ OIG and Federal law enforcement organizations, and undertake any and all response actions DOJ determines are required to ensure the protection of DOJ Information, including providing all requested images, log files, and event information to facilitate rapid resolution of any Security Incident.

G. DOJ, at its sole discretion, may obtain, and Contractor will permit, the assistance of other federal agencies and/or third party contractors or firms to aid in response activities related to any Security Incident. Additionally, DOJ, at its sole discretion, may require Contractor to retain, at Contractor's expense, a Third Party Assessing Organization (3PAO), acceptable to DOJ, with expertise in incident response, compromise assessment, and federal security control requirements, to conduct a thorough vulnerability and security assessment of all affected Information Systems.

H. Response activities related to any Security Incident undertaken by DOJ, including activities undertaken by Contractor, other federal agencies, and any third-party contractors or firms at the request or direction of DOJ, may include inspections, investigations, forensic reviews, data analyses and processing, and final determinations of responsibility for the Security Incident and/or liability for any additional response activities. Contractor shall be responsible for all costs and related resource allocations required for all such response activities related to any Security Incident, including the cost of any penetration testing.

VII. Personally Identifiable Information Notification Requirement

Contractor certifies that it has a security policy in place that contains procedures to promptly notify any individual whose Personally Identifiable Information ("PII") was, or is reasonably determined by DOJ to have been, compromised. Any notification shall be coordinated with the DOJ CO and shall not proceed until the DOJ has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by Contractor shall be coordinated with, and subject to the approval of, DOJ. Contractor shall be responsible for taking corrective action consistent with DOJ Data Breach Notification Procedures and as directed by the DOJ CO, including all costs and expenses associated with such corrective action, which may include providing credit monitoring to any individuals whose PII was actually or potentially compromised.

VIII. Pass-through of Security Requirements to Subcontractors and CSPs

The requirements set forth in the preceding paragraphs of this clause apply to all subcontractors and CSPs who perform work in connection with this Contract, including any CSP providing services for any other CSP under this Contract, and Contractor shall flow down this clause to all subcontractors and CSPs performing under this contract. Any breach by any subcontractor or CSP of any of the provisions set forth in this clause will be attributed to Contractor.

52.204-18 Commercial and Government Entity Code Maintenance (Aug 2020)

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

"Commercial and Government Entity (CAGE) code" means--

(1) An identifier assigned to entities located in the United States or its outlying areas by the Defense Logistics Agency (DLA) Commercial and Government Entity (CAGE) Branch to identify a commercial or government entity by unique location; or

(2) An identifier assigned by a member of the North Atlantic Treaty Organization (NATO) or by the NATO Support and Procurement Agency (NSPA) to entities located outside the United States and its outlying areas that the DLA Commercial and Government Entity (CAGE) Branch records and maintains in the CAGE master file. This type of code is known as a NATO CAGE (NCAGE) code.

(b) Contractors shall ensure that the CAGE code is maintained throughout the life of the contract for each location of contract, including subcontract, performance. For contractors registered in the System for Award Management (SAM), the DLA Commercial and Government Entity (CAGE) Branch shall only modify data received from SAM in the CAGE master file if the contractor initiates those changes via update of its SAM registration. Contractors undergoing a novation or change-of-name agreement shall notify the contracting officer in accordance with subpart 42.12. The contractor shall communicate any change to the CAGE code to the contracting officer within 30 days after the change, so that a modification can be issued to update the CAGE code on the contract.

(c) Contractors located in the United States or its outlying areas that are not registered in SAM shall submit written change requests to the DLA Commercial and Government Entity (CAGE) Branch. Requests for changes shall be provided at <https://cage.dla.mil>. Change requests to the CAGE master file are accepted from the entity identified by the code.

(d) Contractors located outside the United States and its outlying areas that are not registered in SAM shall contact the appropriate National Codification Bureau (points of contact available at <http://www.nato.int/structur/AC/135/main/links/contacts.htm>) or NSPA at <https://eportal.nspa.nato.int/AC135Public/scage/CageList.aspx> to request CAGE changes.

(e) Additional guidance for maintaining CAGE codes is available at <https://cage.dla.mil>.

(f) If the contract includes Federal Acquisition Regulation clause 52.204-2, Security Requirements, the contractor shall ensure that subcontractors maintain their CAGE code(s) throughout the life of the contract.

(End of clause)

52.203-13 Contractor Code of Business Ethics and Conduct (Jun 2020)

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

"Agent" means any individual, including a director, an officer, an employee, or an independent Contractor, authorized to act on behalf of the organization.

"Full cooperation"--

(1) Means disclosure to the Government of the information sufficient for law enforcement to identify the nature and extent of the offense and the individuals responsible for the conduct. It includes providing timely and complete response to Government auditors' and investigators' request for documents and access to employees with information;

(2) Does not foreclose any Contractor rights arising in law, the FAR, or the terms of the contract. It does not require--

(i) A Contractor to waive its attorney-client privilege or the protections afforded by the attorney work product doctrine; or

(ii) Any officer, director, owner, or employee of the Contractor, including a sole proprietor, to waive his or her attorney client privilege or Fifth Amendment rights; and

(3) Does not restrict a Contractor from--

(i) Conducting an internal investigation; or

(ii) Defending a proceeding or dispute arising under the contract or related to a potential or disclosed violation.

"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).

"Subcontract" means any contract entered into by a subcontractor to furnish supplies or services for performance of a prime contract or a subcontract.

"Subcontractor" means any supplier, distributor, vendor, or firm that furnished supplies or services to or for a prime contractor or another subcontractor.

"United States," means the 50 States, the District of Columbia, and outlying areas.

(b) *Code of business ethics and conduct.* (1) Within 30 days after contract award, unless the Contracting Officer establishes a longer time period, the Contractor shall--

(i) Have a written code of business ethics and conduct; and

(ii) Make a copy of the code available to each employee engaged in performance of the contract.

(2) The Contractor shall--

(i) Exercise due diligence to prevent and detect criminal conduct; and

(ii) Otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

(3) (i) The Contractor shall timely disclose, in writing, to the agency Office of the Inspector General (OIG), with a copy to the Contracting Officer, whenever, in connection with the award, performance, or closeout of this contract or any subcontract thereunder, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed--

(A) A violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the United States Code; or

(B) A violation of the civil False Claims Act (31 U.S.C. 3729-3733).

(ii) The Government, to the extent permitted by law and regulation, will safeguard and treat information obtained pursuant to the Contractor's disclosure as confidential where the information has been marked "confidential" or "proprietary" by the company. To the extent permitted by law and regulation, such information will not be released by the Government to the public pursuant to a Freedom of Information Act request, 5 U.S.C. Section 552, without prior notification to the Contractor. The Government may transfer documents provided by the Contractor to any department or agency within the Executive Branch if the information relates to matters within the organization's jurisdiction.

(iii) If the violation relates to an order against a Governmentwide acquisition contract, a multi-agency contract, a multiple-award schedule contract such as the Federal Supply Schedule, or any other procurement instrument intended for use by multiple agencies, the Contractor shall notify the OIG of the ordering agency and the IG of the agency responsible for the basic contract.

(c) Business ethics awareness and compliance program and internal control system. This paragraph (c) does not apply if the Contractor has represented itself as a small business concern pursuant to the award of this contract or if this contract is for the acquisition of a commercial item as defined at FAR 2.101. The Contractor shall establish the following within 90 days after contract award, unless the Contracting Officer establishes a longer time period:

(1) An ongoing business ethics awareness and compliance program.

(i) This program shall include reasonable steps to communicate periodically and in a practical manner the Contractor's standards and procedures and other aspects of the Contractor's business ethics awareness and compliance program and internal control system, by conducting effective training programs and otherwise disseminating information appropriate to an individual's respective roles and responsibilities.

(ii) The training conducted under this program shall be provided to the Contractor's principals and employees, and as appropriate, the Contractor's agents and subcontractors.

(2) An internal control system.

(i) The Contractor's internal control system shall--

(A) Establish standards and procedures to facilitate timely discovery of improper conduct in connection with Government contracts; and

(B) Ensure corrective measures are promptly instituted and carried out.

(ii) At a minimum, the Contractor's internal control system shall provide for the following:

(A) Assignment of responsibility at a sufficiently high level and adequate resources to ensure effectiveness of the business ethics awareness and compliance program and internal control system.

(B) Reasonable efforts not to include an individual as a principal, whom due diligence would have exposed as having engaged in conduct that is in conflict with the Contractor's code of business ethics and conduct.

(C) Periodic reviews of company business practices, procedures, policies, and internal controls for compliance with the Contractor's code of business ethics and conduct and the special requirements of Government contracting, including--

(1) Monitoring and auditing to detect criminal conduct;

(2) Periodic evaluation of the effectiveness of the business ethics awareness and compliance program and internal control system, especially if criminal conduct has been detected; and

(3) Periodic assessment of the risk of criminal conduct, with appropriate steps to design, implement, or modify the business ethics awareness and compliance program and the internal control system as necessary to reduce the risk of criminal conduct identified through this process.

(D) An internal reporting mechanism, such as a hotline, which allows for anonymity or confidentiality, by which employees may report suspected instances of improper conduct, and instructions that encourage employees to make such reports.

(E) Disciplinary action for improper conduct or for failing to take reasonable steps to prevent or detect improper conduct.

(F) Timely disclosure, in writing, to the agency OIG, with a copy to the Contracting Officer, whenever, in connection with the award, performance, or closeout of any Government contract performed by the Contractor or a subcontract thereunder, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed a violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 U.S.C. or a violation of the civil False Claims Act (31 U.S.C. 3729-3733).

(1) If a violation relates to more than one Government contract, the Contractor may make the disclosure to the agency OIG and Contracting Officer responsible for the largest dollar value contract impacted by the violation.

(2) If the violation relates to an order against a Governmentwide acquisition contract, a multi-agency contract, a multiple-award schedule contract such as the Federal Supply Schedule, or any other procurement instrument intended for use by multiple agencies, the contractor shall notify the OIG of the ordering agency and the IG of the agency responsible for the basic contract, and the respective agencies' contracting officers.

(3) The disclosure requirement for an individual contract continues until at least 3 years after final payment on the contract.

(4) The Government will safeguard such disclosures in accordance with paragraph (b)(3)(ii) of this clause.

(G) Full cooperation with any Government agencies responsible for audits, investigations, or corrective actions.

(d) *Subcontracts.* (1) The Contractor shall include the substance of this clause, including this paragraph (d), in subcontracts that exceed the threshold specified in FAR 3.1004(a) on the date of subcontract award and a performance period of more than 120 days.

(2) In altering this clause to identify the appropriate parties, all disclosures of violation 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.

(End of clause)

52.213-4 Terms and Conditions-Simplified Acquisitions (Other Than Commercial Items) (Aug 2020)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses that are incorporated by reference:

(1) The clauses listed below implement provisions of law or Executive order:

- (i) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).
- (ii) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).
- (iii) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2020) (Section 889(a)(1)(A) of Pub. L. 115-232).
- (iv) 52.222-3, Convict Labor (Jun 2003) (E.O. 11755).
- (v) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
- (vi) 52.222-26, Equal Opportunity (Sept 2016) (E.O. 11246).
- (vii) 52.225-13, Restrictions on Certain Foreign Purchases (Jun 2008) (E.O.s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).
- (viii) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).
- (ix) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004) (Pub. L. 108-77, 108-78 (19 U.S.C. 3805 note)).

(2) Listed below are additional clauses that apply:

- (i) 52.232-1, Payments (Apr 1984).
- (ii) 52.232-8, Discounts for Prompt Payment (Feb 2002).
- (iii) 52.232-11, Extras (Apr 1984).
- (iv) 52.232-25, Prompt Payment (Jan 2017).
- (v) 52.232-39, Unenforceability of Unauthorized Obligations (Jun 2013).
- (vi) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (Dec 2013)
- (vii) 52.233-1, Disputes (May 2014).
- (viii) 52.244-6, Subcontracts for Commercial Items (Aug 2020).
- (ix) 52.253-1, Computer Generated Forms (Jan 1991).

(b) The Contractor shall comply with the following FAR clauses, incorporated by reference, unless the circumstances do not apply:

(1) The clauses listed below implement provisions of law or Executive order:

- (i) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Jun 2020) (Pub. L. 109-282) (31 U.S.C. 6101 note) (Applies to contracts valued at or above the threshold specified in FAR 4.1403(a) on the date of award of this contract).
- (ii) 52.222-19, Child Labor--Cooperation with Authorities and Remedies (Jan 2020) (E.O. 13126) (Applies to contracts for supplies exceeding the micro-purchase threshold, as defined in FAR 2.101 on the date of award of this contract).
- (iii) 52.222-20, Contracts for Materials, Supplies, Articles, and Equipment (Jun 2020) (41 U.S.C. chapter 65) (Applies to supply contracts over the threshold specified in FAR 22.602 on the date of award of this contract, in the United States, Puerto Rico, or the U.S. Virgin Islands).
- (iv) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212) (Applies to contracts valued at or above the threshold specified in FAR 22.1303(a) on the date of award of this contract).

(v) 52.222-36, Equal Employment for Workers with Disabilities (Jun 2020) (29 U.S.C. 793) (Applies to contracts over the threshold specified in FAR 22.1408(a) on the date of award of this contract, unless the work is to be performed outside the United States by employees recruited outside the United States). (For purposes of this clause, "United States" includes the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the U.S. Virgin Islands, and Wake Island.)

(vi) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212) (Applies to contracts valued at or above the threshold specified in FAR 22.1303(a) on the date of award of this contract).

(vii) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67) (Applies to service contracts over \$2,500 that are subject to the Service Contract Labor Standards statute and will be performed in the United States, District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the U.S. Virgin Islands, Johnston Island, Wake Island, or the outer Continental Shelf).

(viii)(A) 52.222-50, Combating Trafficking in Persons (Jan 2019) (22 U.S.C. chapter 78 and E.O 13627) (Applies to all solicitations and contracts).

(B) Alternate I (Mar 2015) (Applies if the Contracting Officer has filled in the following information with regard to applicable directives or notices: Document title(s), source for obtaining document(s), and contract performance location outside the United States to which the document applies).

(ix) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015) (Applies when 52.222-6 or 52.222-41 are in the contract and performance in whole or in part is in the United States (the 50 States and the District of Columbia)).

(x) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2017) (E.O. 13706) (Applies when 52.222-6 or 52.222-41 are in the contract and performance in whole or in part is in the United States (the 50 States and the District of Columbia).))

(xi) 52.223-5, Pollution Prevention and Right-to-Know Information (May 2011) (E.O. 13423) (Applies to services performed on Federal facilities).

(xii) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O. 13693) (applies to contracts for products as prescribed at FAR 23.804(a)(1)).

(xiii) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693) (Applies to maintenance, service, repair, or disposal of refrigeration equipment and air conditioners).

(xiv) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b) (Unless exempt pursuant to 23.204, applies to contracts when energy-consuming products listed in the ENERGY STAR® Program or Federal Energy Management Program (FEMP)) will be--

(A) Delivered;

(B) Acquired by the Contractor for use in performing services at a Federally-controlled facility;

(C) Furnished by the Contractor for use by the Government; or

(D) Specified in the design of a building or work, or incorporated during its construction, renovation, or maintenance).

(xv) 52.223-20, Aerosols (Jun 2016) (E.O. 13693) (Applies to contracts for products that may contain high global warming potential hydrofluorocarbons as a propellant or as a solvent; or contracts for maintenance or repair of electronic or mechanical devices).

(xvi) 52.223-21, Foams (Jun 2016) (E.O. 13693) (Applies to contracts for products that may contain high global warming potential hydrofluorocarbons or refrigerant blends containing hydrofluorocarbons as a foam blowing agent; or contracts for construction of buildings or facilities).

(xvii) 52.225-1, Buy American--Supplies (May 2014) (41 U.S.C. chapter 67) (Applies to contracts for supplies, and to contracts for services involving the furnishing of supplies, for use in the United States or its outlying areas, if the value of the supply contract or supply portion of a service contract exceeds the micro-purchase threshold, as defined in FAR 2.101 on the date of award of this contract, and the acquisition--

(A) Is set aside for small business concerns; or

(B) Cannot be set aside for small business concerns (see 19.502-2), and does not exceed \$25,000).

(xviii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (Jun 2020) (42 U.S.C. 1792) (Applies to contracts greater than the threshold specified in FAR 26.404 on the date of award of this contract, that provide for the provision, the service, or the sale of food in the United States).

(xix) 52.232-33, Payment by Electronic Funds Transfer--System for Award Management (Oct 2013) (Applies when the payment will be made by electronic funds transfer (EFT) and the payment office uses the System for Award Management (SAM) as its source of EFT information).

(xx) 52.232-34, Payment by Electronic Funds Transfer--Other than System for Award Management (Jul 2013) (Applies when the payment will be made by EFT and the payment office does not use the SAM database as its source of EFT information).

(xxi) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. App. 1241) (Applies to supplies transported by ocean vessels (except for the types of subcontracts listed at 47.504(d)).

(2) Listed below are additional clauses that may apply:

(i) 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (Jun 2016) (Applies to contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system.

(ii) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Jun 2020) (Applies to contracts over the threshold specified in FAR 9.405-2(b) on the date of award of this contract).

(iii) 52.211-17, Delivery of Excess Quantities (Sept 1989) (Applies to fixed-price supplies).

(iv) 52.247-29, F.o.b. Origin (Feb 2006) (Applies to supplies if delivery is f.o.b. origin).

(v) 52.247-34, F.o.b. Destination (Nov 1991) (Applies to supplies if delivery is f.o.b. destination).

(c) FAR 52.252-2, *Clauses Incorporated by Reference (Feb 1998)*. This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

[#www.acquisition.gov](http://www.acquisition.gov)

[Insert one or more Internet addresses]

(d) *Inspection/Acceptance*. The Contractor shall tender for acceptance only those items that conform to the requirements of this contract. The Government reserves the right to inspect or test any supplies or services that have been tendered for acceptance. The Government may require repair or replacement of nonconforming supplies or reperformance of nonconforming services at no increase in contract price. The Government must exercise its postacceptance rights--

(1) Within a reasonable period of time after the defect was discovered or should have been discovered; and

(2) Before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item.

(e) *Excusable delays*. The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence, such as acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.

(f) *Termination for the Government's convenience*. The Government reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid a percentage of the contract price reflecting the percentage of the work performed prior to the notice of termination,

plus reasonable charges that the Contractor can demonstrate to the satisfaction of the Government, using its standard record keeping system, have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred that reasonably could have been avoided.

(g) *Termination for cause.* The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government, upon request, with adequate assurances of future performance. In the event of termination for cause, the Government shall not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If it is determined that the Government improperly terminated this contract for default, such termination shall be deemed a termination for convenience.

(h) *Warranty.* The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.

(End of clause)

52.247-21 Contractor Liability for Personal Injury and/or Property Damage (Apr 1984)

(a) The Contractor assumes responsibility for all damage or injury to persons or property occasioned through the use, maintenance, and operation of the Contractor's vehicles or other equipment by, or the action of, the Contractor or the Contractor's employees and agents.

(b) The Contractor, at the Contractor's expense, shall maintain adequate public liability and property damage insurance during the continuance of this contract, insuring the Contractor against all claims for injury or damage.

(c) The Contractor shall maintain Workers' Compensation and other legally required insurance with respect to the Contractor's own employees and agents.

(d) The Government shall in no event be liable or responsible for damage or injury to any person or property occasioned through the use, maintenance, or operation of any vehicle or other equipment by, or the action of, the Contractor or the Contractor's employees and agents in performing under this contract, and the Government shall be indemnified and saved harmless against claims for damage or injury in such cases.

(End of clause)

Section 4 - List of Attachments

This Section Is Intentionally Left Blank