

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

SOLICITATION #D-23-HR-0023

52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions 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. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this address:

<https://www.acquisition.gov/far-smart-matrix>.

(End of provision)

CONTRACTING OFFICER: Check the corresponding box for the provisions and clauses applicable to this procurement.

- ☐ **52.204-6 UNIQUE ENTITY IDENTIFIER (OCT 2016)**
- ☒ **52.204-7 SYSTEM FOR AWARD MANAGEMENT (OCT 2018)**
- ☐ **52.204-7 ALT I SYSTEM FOR AWARD MANAGEMENT (OCT 2018) WITH ALTERNATE I (OCT 2018)**
- ☒ **52.204-16 COMMERCIAL AND GOVERNMENT ENTITY CODE REPORTING (JUL 2016)**
- ☐ **52.209-7 INFORMATION REGARDING RESPONSIBILITY MATTERS (OCT 2018)**
- ☐ **52.209-12 CERTIFICATION REGARDING TAX MATTERS (OCT 2020)**
- ☐ **52.211-6 BRAND NAME OR EQUAL (AUG 1999)**
- ☒ **52.212-1 INSTRUCTIONS TO OFFERORS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (NOV 2021)**
- ☒ **52.212-2 EVALUATION—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (NOV 2021)**

(a) The Government will award a contract resulting from this solicitation to the responsible offeror whose offer conforming to the solicitation will be most advantageous to the Government, price and other factors considered. The following factors shall be used to evaluate offers:

Factor 1-Technical Capability

Factor 2-Past Performance;

[Contracting Officer shall insert the significant evaluation factors, such as (i) technical capability of the item offered to meet the Government requirement; (ii) price; (iii) past performance (see FAR [15.304](#)); and include them in the relative order of importance of the evaluation factors, such as in descending order of importance.]

Technical and past performance, when combined, are significantly more important than price [Contracting Officer state, in accordance with FAR [15.304](#), the relative importance of all other evaluation factors, when combined, when compared to price.]

(b) Options. The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that an offer is unacceptable if the option prices are significantly unbalanced. Evaluation of options shall not obligate the Government to exercise the option(s).

(c) A written notice of award or acceptance of an offer, mailed or otherwise furnished to the successful offeror within the time for acceptance specified in the offer, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.

(End of provision)

- ☐ **52.225-7 WAIVER OF BUY AMERICAN STATUTE FOR CIVIL AIRCRAFT AND RELATED ARTICLES (FEB 2016)**
- ☐ **DEA-2852.209-75 NATIONAL SECURITY RISK ASSESSMENT (JUN 2014)**

(a) Any offeror responding to this solicitation acknowledges that before acquiring information technology equipment or software, the U.S. Department of Justice and its component entities will assess the supply chain risk of cyber-espionage or sabotage associated with the acquisition of such equipment or software, including any risk associated with such equipment or software being produced, manufactured, or assembled by one or more entities identified as posing a cyber-threat, including but not limited to, those that may be owned, directed, or subsidized by the People's Republic of China.

(b) By submitting an offer to this solicitation, the Offeror understands and agrees that the Government retains the right to reject any offer or response to this solicitation made by the Offeror, without any further recourse by, or explanation to, the Offeror, if the Government determines the Offeror or the equipment or software offered by the Offeror, in whole or in part, presents an unacceptable risk to national security.

(c) To assist the Government in assessing whether the acquisition poses a national security risk, offerors are required to complete and submit with its offer or quotation the National Security Acquisition Risk Assessment Questions, which are attached to this solicitation. Offerors must answer all questions completely and accurately to the best of their knowledge and belief. All answers are to be reflective of the parent and subsidiary levels of an organization.

(d) Offerors are also required to request, collect, and forward with its offer or quotation completed National Security Acquisition Risk Assessment Questions from all subcontractors that will provide any equipment or software in performance of the contract or order. Offerors are responsible for the thoroughness and completeness of each subcontractor's submission.

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

(e) Failure to provide any such requested information may render a proposal unacceptable.

(End of provision)

☐ **JAR 2852.233-70 PROTESTS FILED DIRECTLY WITH THE DEPARTMENT OF JUSTICE (NOV 2020)**

(a) The following definitions apply in this provision:

(1) “Agency Protest Official” (APO) means the Deciding Official for a procurement protest filed with a contracting activity of DOJ when the contracting officer will not be the Deciding Official because of the protestor’s election under JAR 2833.103(b).

(2) “Deciding Official” means the official who will review and decide a procurement protest filed with the agency. The Deciding Official will be the contracting officer unless the protestor requests pursuant to JAR 2833.103(b) that the protest be decided by an individual above the level of the contracting officer, in which case the HCA will designate an APO to serve as the Deciding Official.

(3) “Interested Party” means an actual or prospective offeror whose direct economic interest would be affected by the award of a contract or by the failure to award a contract.

(b) Only interested parties may file a protest.

(c) An interested party filing a protest with the DOJ has the choice of requesting either that the Contracting Officer or the APO decide the protest.

(d) A protest filed directly with the DOJ shall:

(1) Indicate that it is a protest to DOJ.

(2) Be filed with the Contracting Officer.

(3) State whether the protestor chooses to have the Contracting Officer or the Agency Protest Official decide the protest. If the protestor is silent on this matter, the Contracting Officer will decide the protest.

(4) Indicate whether the protestor prefers to make an oral or written presentation of arguments in support of the protest to the deciding official.

(5) Include the information required by FAR 33.103(d)(2):

(i) Name, address, facsimile number and telephone number of the protestor.

(ii) Solicitation or contract number.

(iii) Detailed statement of the legal and factual grounds for the protest, to include a description of resulting prejudice to the protestor.

(iv) Copies of relevant documents.

(v) Request for a ruling by the agency.

(vi) Statement as to the form of relief requested.

(vii) All information establishing that the protestor is an interested party for the purpose of filing a protest.

(viii) All information establishing the timeliness of the protest.

(e) The decision by the APO is an alternative to a decision by the Contracting Officer. The APO will not consider appeals from the Contracting Officer’s decision on an agency protest and a decision by the APO is final and not appealable.

(f) The Deciding Official may conduct a scheduling conference. The scheduling conference, if conducted, will establish deadlines for oral or written arguments in support of the agency protest and for agency officials to present information in response to the protest issues. The deciding official may hear oral arguments in support of the agency protest at the same time as the scheduling conference, depending on availability of the necessary parties.

(g) Oral conferences may take place either by telephone or in person.

(h) The protestor has only one opportunity to support or explain the substance of its protest. DOJ procedures do not provide for any discovery. The deciding official may request additional information from the agency or the protestor. The deciding official will resolve the protest through informal presentations or meetings to the maximum extent practicable.

(i) A protestor may represent itself or be represented by legal counsel. The DOJ will not reimburse the protestor for any legal fees related to the agency protest.

(j) The DOJ will stay award or suspend contract performance in accordance with FAR 33.103(f), unless the contract award is justified, in writing, for urgent and compelling reasons or is determined, in writing, to be in the best interest of the Government. The justification or determination shall be approved at a level above the Contracting Officer. The stay or suspension, unless over-ridden, remains in effect until the protest is decided, dismissed, or withdrawn.

(k) The deciding official will make a best effort to issue a decision on the protest within thirty-five (35) days after the filing date. The decision shall be written, and provided to the protestor using a method that provides for evidence of receipt.

(l) The DOJ may dismiss or stay proceedings on an agency protest if a protest on the same or similar basis is filed with a forum outside DOJ.

(End of Clause)

CONTINUED ON NEXT PAGE

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

SOLICITATION #:D-23-HR-0023

OFFERORS – COMPLETE THE REPRESENTATIONS BELOW AND RETURN THEM WITH YOUR OFFER OR QUOTE IF THE VERSIONS OF THESE PROVISIONS IN YOUR ANNUAL REPRESENTATIONS AND CERTIFICATIONS IN THE SYSTEM FOR AWARD MANAGEMENT ARE EARLIER THAN OCT 2020.

☒ 52.204-24 REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (NOV 2021)

The Offeror shall not complete the representation at paragraph (d)(1) of this provision if the Offeror has represented that it "does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument" in paragraph (c)(1) in the provision at [52.204-26](#), Covered Telecommunications Equipment or Services—Representation, or in paragraph (v)(2)(i) of the provision at [52.212-3](#), Offeror Representations and Certifications—Commercial Products and Commercial Services. The Offeror shall not complete the representation in paragraph (d)(2) of this provision if the Offeror has represented that it "does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services" in paragraph (c)(2) of the provision at [52.204-26](#), or in paragraph (v)(2)(ii) of the provision at [52.212-3](#).

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

Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in the clause [52.204-25](#), Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) *Prohibition.*

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

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

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

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

(c) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(d) *Representation.* The Offeror represents that—

(1) It ☐ will, ☐ will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation. The Offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the Offeror responds "will" in paragraph (d)(1) of this section; and

(2) After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that—

It ☐ does, ☐ does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the Offeror responds "does" in paragraph (d)(2) of this section.

(e) *Disclosures.*

(1) Disclosure for the representation in paragraph (d)(1) of this provision. If the Offeror has responded "will" in the representation in paragraph (d)(1) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(ii) For covered services—

SOLICITATION #:D-23-HR-0023

October 2022

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded "does" in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(End of provision)

☒ **52.212-3 OFFEROR REPRESENTATIONS AND CERTIFICATIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (OCT 2022)**

Attention is drawn to paragraph (b) of provision 52.212-3, which requests offeror-provided fill-in information in (b)(2), when applicable:

(b)(1) *Annual Representations and Certifications.* Any changes provided by the Offeror in paragraph (b)(2) of this provision do not automatically change the representations and certifications in SAM.

(2) The offeror has completed the annual representations and certifications electronically in SAM accessed through <http://www.sam.gov>. After reviewing SAM information, the Offeror verifies by submission of this offer that the representations and certifications currently posted electronically at FAR [52.212-3](#), Offeror Representations and Certifications—Commercial Products and Commercial Services, have been entered or updated in the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), at the time this offer is submitted and are incorporated in this offer by reference (see FAR [4.1201](#)), except for paragraphs _____.

[Offeror to identify the applicable paragraphs at (c) through (u) of this provision that the offeror has completed for the purposes of this solicitation only, if any. These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer. Any changes provided by the offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications posted electronically on SAM.]

***** Paragraph (i) Contracting Officer fill-in information: Paragraph (i)(1): The end products being acquired under this solicitation that are included in the List of Products Requiring Contractor Certification as to Forced or Indentured Child Labor are listed by Schedule of Supplies/Services Item Number as follows: **[when applicable, enter item numbers with country of origin in parentheses and separated by commas]**

***** Paragraph (k) Contracting Officer fill-in information: select applicable item when an exemption to the Service Contract Labor Standards statute applies.

☐ Paragraph k(1) is applicable. ☐ Paragraph k(2) is applicable.

(v) (2) The Offeror represents that—

(i) It ☐ does, ☐ does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(ii) After conducting a *reasonable inquiry** for purposes of this representation, that it ☐ does, ☐ does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

* *Reasonable inquiry* has the meaning provided in the clause [52.204-25](#), Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

CONTINUED ON NEXT PAGE

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

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 address: <https://www.acquisition.gov/far-smart-matrix>.
(End of clause)

CONTRACTING OFFICER: Check the appropriate box only for clauses that are applicable to this procurement.

- | | | |
|-------------------------------------|--------------------------------|--|
| <input type="checkbox"/> | 52.203-16 | PREVENTING PERSONAL CONFLICTS OF INTEREST (JUN 2020) |
| <input type="checkbox"/> | 52.203-17 | CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS (JUN 2020) |
| <input type="checkbox"/> | 52.204-4 | PRINTED OR COPIED DOUBLE-SIDED ON POSTCONSUMER FIBER CONTENT PAPER (MAY 2011) |
| <input type="checkbox"/> | 52.204-9 | PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (JAN 2011) |
| <input type="checkbox"/> | 52.204-12 | UNIQUE ENTITY IDENTIFIER MAINTENANCE (OCT 2016) |
| <input checked="" type="checkbox"/> | 52.204-13 | SYSTEM FOR AWARD MANAGEMENT MAINTENANCE (OCT 2018) |
| <input type="checkbox"/> | 52.204-18 | COMMERCIAL AND GOVERNMENT ENTITY CODE MAINTENANCE (AUG 2020) |
| <input checked="" type="checkbox"/> | 52.204-19 | INCORPORATION BY REFERENCE OF REPRESENTATIONS AND CERTIFICATIONS (DEC 2014) |
| <input type="checkbox"/> | 52.204-21 | BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (NOV 2021) |
| <input type="checkbox"/> | 52.204-23 | PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES, IN ALL SOLICITATIONS AND CONTRACTS (NOV 2021) |
| <input checked="" type="checkbox"/> | 52.204-25 | PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (NOV 2021) |
| <input type="checkbox"/> | 52.207-5 | OPTION TO PURCHASE EQUIPMENT (FEB 1995) |
| <input checked="" type="checkbox"/> | 52.212-4 | CONTRACT TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (NOV 2021) |
| <input type="checkbox"/> | 52.212-4 ALT I | CONTRACT TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (NOV 2021) WITH ALTERNATE I (NOV 2021) |
| <input type="checkbox"/> | 52.212-4 | CONTRACT TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (NOV 2021) |
| <input type="checkbox"/> | JAR 2852.212-4 | TERMS AND CONDITIONS—COMMERCIAL ITEMS (NOV 2020) (DEVIATION) |

When a commercial item is contemplated (using FAR part 12 procedures or otherwise) and the contract will include FAR 52.212-4, the following replaces subparagraph (g)(2); paragraph (h); subparagraph (i)(2); paragraph (s); and paragraph (u), Unauthorized Obligations, of the basic FAR clause, and adds paragraph (w), as follows:

(g)(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment act regulations at 5 CFR part 1315, as modified by subparagraph (i)(2), *Prompt payment*, of this clause.

(h) *Patent indemnity*. Contractor shall indemnify and hold harmless the Government and its respective affiliates, officers, directors, employees, agents, successors and assigns (collectively, "Indemnities") from and against any and all liability and losses incurred by the Indemnities that are (i) included in any settlement and/or (ii) awarded by a court of competent jurisdiction arising from or in connection with any third party claim of infringement made against Indemnities asserting that any product or service supplied under this contract constitutes infringement of any patent, copyright, trademark, service mark, trade name or other proprietary or intellectual right. This indemnity shall not apply unless Contractor shall have been informed within a reasonable time by the Government of the claim or action alleging such infringement and shall have been given such opportunity as is afforded by applicable laws, rules, or regulations to participate in its defense. This indemnity also shall not apply to any claim unreasonably settled by the Government which obligates Contractor to make any admission or pay any amount without written consent signed by an authorized officer of Contractor, unless required by final decree of a court of competent jurisdiction.

(i)(2) *Prompt payment*. The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations (5 CFR part 1315), with the following modification regarding the due date: For the sole purpose of computing an interest penalty due the Contractor, the Government agrees to inspect and determine the acceptability of any supply delivered or service performed specified in the invoice within thirty (30) days of receipt of a proper invoice from the Contractor, after which time, if no affirmative action has been taken by the Government to accept such supply or service, the supply or service will be deemed accepted and payment due thirty (30) days from the date of deemed acceptance. If the Government makes the determination that the item delivered or service performed is deficient or otherwise unacceptable, or the invoice is otherwise determined not to be a proper invoice, the terms and conditions of this paragraph regarding prompt payment will apply to the date the Contractor corrects the deficiency in the item delivered or service performed or submits a proper invoice. If actual acceptance occurs within the constructive acceptance period, the Government will base the determination of an interest penalty on the actual date of acceptance. The constructive acceptance requirement does not, however, compel Government officials to accept supplies or services, perform contract administration functions, or make payment prior to fulfilling their responsibilities.

(s) *Order of precedence*. Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:

- (1) The schedule of supplies/services.

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

(2) The Assignments, Payments, Invoice, Other Compliances, and Compliance with Laws Unique to Government Contracts provisions of the basic FAR clause at 52.212–4, and the Unauthorized Obligations and Contractor’s Commercial Supplier Agreements—Unenforceable Clauses provisions of JAR 2852.212–4.

(3) FAR 52.212–5.

(4) Other paragraphs of the basic FAR clause at 52.212–4, with the exception of paragraph (o), Warranty, and those paragraphs identified in this deviation of 52.212–4.

(5) Addenda to this solicitation, contract, or order, including contractor’s Commercial supplier agreements incorporated into the contract.

(6) Solicitation provisions if this is a solicitation.

(7) Paragraph (o), Warranty, of the basic FAR clause at 52.212–4.

(8) The Standard Form 1449.

(9) Other documents, exhibits, and attachments.

(10) The specification.

* * * * *

(u) *Unauthorized obligations.*

(1) Except as stated in paragraph (u)(2) of this clause, when any supply or service acquired under this contract or order is subject to any Commercial supplier agreement that includes any language, provision, or clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (see 31 U.S.C. 1341), the following shall govern:

(i) Any such language, provision, or clause is unenforceable against the Government.

(ii) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the commercial supplier agreement. If the commercial supplier agreement is invoked through an “I agree” click box or other similar mechanism (e.g., “clickwrap” or “browse-wrap” agreements), execution does not bind the Government or any Government authorized end user to such clause.

(iii) Any such language, provision, or clause is deemed to be stricken from the commercial supplier agreement and have no effect.

(2) Paragraph (u)(1) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

* * * * *

(w) *Commercial supplier agreements—unenforceable clauses.* When any supply or service acquired under this contract or order is subject to a contractor’s commercial supplier agreement, the following shall be deemed incorporated into such agreement and modifies and replaces any similar language, provision, or clause in such agreement. As used herein, “this agreement” means any contractor commercial supplier agreement:

(1) Notwithstanding any other provision of this agreement, when the end user is an agency or instrumentality of the U.S. Government, the following shall apply:

(i) *Applicability.* This agreement is a part of a contract between commercial supplier and the U.S. Government for the acquisition of the supply or service that necessitates a license or other similar legal instrument (including all contracts, task orders, and delivery orders under FAR part 12).

(ii) *End user.* This agreement shall bind the Government as end user but shall not operate to bind the Government employee or person acting on behalf of the Government in his or her personal capacity.

(iii) *Law and disputes.* This agreement is governed by Federal law.

(A) Any language, provision, or clause purporting to subject the U.S. Government to the laws of any U.S. state, territory, district, or municipality, or the laws of a foreign nation, except where Federal law expressly provides for the application of such laws, is hereby deleted and shall have no effect.

(B) Any language, provision, or clause requiring dispute resolution in a specific forum or venue that is different from that prescribed by applicable Federal law is hereby deleted and shall have no effect.

(C) Any language, provision, or clause prescribing a different time period for bringing an action than that prescribed by applicable Federal law in relation to a dispute is hereby deleted and shall have no effect.

(iv) *Continued performance.* Notwithstanding any other provision in this agreement, if the Contractor believes the Government to be in breach of this contract, order, or agreement, it shall pursue its rights under the Contract Disputes Act or other applicable Federal statute while continuing performance as set forth in subparagraph (d), Disputes, of FAR 52.212–4.

(v) *Arbitration; equitable or injunctive relief.* In the event of a claim or dispute arising under or relating to the contract, order, or this agreement,

(A) binding arbitration shall not be used unless otherwise specifically authorized by agency guidance, and

(B) equitable or injunctive relief, including the award of attorney fees, costs or interest, may be awarded against the Government only when explicitly provided by statute.

(vi) *Updating terms.*

(A) After award, the contractor may unilaterally revise terms if they are not material. Material terms are defined as:

(1) Terms that change Government rights or obligations;

(2) Terms that increase Government prices;

(3) Terms that decrease the overall level of service; or

(4) Terms that limit any other Government right addressed elsewhere in this contract.

(B) For revisions that materially change the terms of the contract, the revised commercial supplier agreement must be incorporated into the contract using a bilateral modification.

(C) Any agreement terms or conditions unilaterally revised subsequent to award that are inconsistent with any material term or provisions of this contract shall not be enforceable against the Government, and the Government shall not be deemed to have consented to them.

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

(vii) *Order of precedence.* Any Order of Precedence clause in any commercial supplier agreement is not enforceable against the Government. The applicable Order of Precedence for this contract, order, or agreement is FAR 52.212–4(s), as revised by JAR 2812.302 and 2852.212–4(s).

(viii) *No automatic renewals.* If any license or service tied to period payment is provided under this agreement (e.g., annual software maintenance or annual lease term), such license or service shall not renew automatically upon expiration of its current term without prior express consent by a properly warranted contracting officer, and any provision or term of any license or service purporting to provide for automatic renewal is unenforceable against the Government.

(ix) *Indemnification by the Government or end-user.* Any language, provision, or clause of this commercial supplier agreement requiring the Government or End-user to indemnify the commercial supplier or licensor is not enforceable against the Government.

(x) *Indemnification by the commercial supplier or licensor.* Any clause of this agreement requiring or permitting the commercial supplier or licensor to defend the Government as a condition of indemnifying the Government for any claim of infringement is hereby amended to provide that the U.S. Department of Justice has the sole right to represent the United States in any such action, in accordance with 28 U.S.C. 516.

(xi) *Audits.* Any language, provision, or clause of this commercial supplier agreement permitting Contractor to audit the end user's compliance with this agreement is not enforceable against the Government. To the extent any language, provision or clause of this agreement permits Contractor to audit the Government's compliance under this contract, order, or agreement, such language, provision, or clause of this agreement is hereby stricken and replaced as follows:

“(A) If Contractor reasonably believes that the Government has violated the terms of this agreement with regard to the restrictions on authorized use and/or the number of authorized users, upon written request from Contractor, including an explanation of the basis for the request, DOJ will provide a redacted version of the Government's most recent Security Assessment and Authorization package (SAA) to Contractor on a confidential basis, so that Contractor may reasonably verify the Government's compliance with its obligations under this agreement. Contractor understands and agrees that the Government will remove or redact any information from the SAA that it reasonably believes may compromise (a) the security of the Government's information technology environment; (b) the confidentiality of any third-party proprietary or confidential information; (c) any confidential, sensitive law enforcement information; and (d) any other information that the Government believes may compromise a past, current, or prospective investigation, prosecution, or litigation. Notwithstanding the preceding, and subject to the Government's policies and procedures for such review, including but not limited to complying with all Government security requirements prior to being granted access to the Government's facilities, including the execution of appropriate confidentiality and/or non-disclosure agreements, the Government will arrange, upon Contractor's written request, for Contractor to view an un-redacted version of the SAA on Government premises. Contractor understands that Contractor will be provided a copy of the un-redacted SAA on Government premises only and that no un-redacted copy of the SAA, or any medium containing information relating to it, will be permitted to be removed from Government premises.

(B) The Contractor also understands and agrees that the Contractor shall make a request under this paragraph no more than on an annual basis and only during the period of the contract, and that any activities performed by Contractor under this clause will be performed at Contractor's expense, without reimbursement by the Government.

(C) Discrepancies found with regard to the restrictions on authorized use and/or the number of authorized users may result in a charge by Contractor to the Government. Any resulting invoice must comply with the proper invoicing and payment requirements specified in the contract. This charge, if disputed by the Government, will be resolved through the Disputes clause at 52.212–4(d); no payment obligation shall arise on the part of the Government until the conclusion of the dispute process.”

(xii) *Taxes or surcharges.* Any taxes or surcharges which the Contractor seeks to pass along to the Government as end user will be governed by the terms of the underlying Government contract and, in any event, must be submitted to the Contracting Officer for a determination of applicability prior to invoicing unless specifically agreed to otherwise in the Government contract.

(xiii) *Non-assignment.* This agreement may not be assigned, nor may any rights or obligations thereunder be delegated, without the Government's prior approval, except as expressly permitted under FAR 52.212–4 (b), Assignment.

(xiv) *Confidential information.*

(A) During the term of this contract or order, either party may identify information as “confidential information,” and there shall be no disclosure, dissemination, or publication of any such information except to the extent required for the performance of this contract or order and otherwise provided in this clause or by statute or regulation. Specifically, the parties agree that the party receiving confidential information may only disclose such information to its employees and contractors on a “need-to-know” basis to carry out the obligations of this contract or order, and that subcontractors performing under this Agreement are subject to the same stipulations provided in this provision. The parties also agree that this provision shall survive the termination of this contract or order, and any confidential information obtained or received which comes within these restrictions shall remain confidential, provided that the obligation to treat information as confidential shall not apply to information which is or becomes publicly available through no improper action of the receiving party; is or comes to be in the receiving party's possession independent of its relationship with the disclosing party; is developed by or becomes known to the receiving party without use of any confidential information of the disclosing party; or is obtained rightfully from a third party not bound by an obligation of confidentiality. Additionally, nothing in this contract or order shall restrict disclosure by the receiving party pursuant to any applicable law, including but not limited to the Freedom of Information Act, 5 U.S.C. 552, *et seq.*, or an order of any court of competent jurisdiction, provided that in either such case the receiving party gives prompt notice to the disclosing party to allow the disclosing party to interpose an objection to such disclosure, take action to assure confidential handling of the confidential information, or take such other action as it deems appropriate to protect its confidential information.

(B) The Government considers and hereby identifies as confidential any and all information related to any inquiries and/or searches performed by the Government or by contractor at the Government's direction under this contract or order, including the subject of any such inquiry or search and any and all search terms, regardless of whether provided in writing or orally to Contractor, and Contractor agrees that it may only disclose such information to its employees and contractors on a “need-to-know” basis to carry out the obligations of this contract or order and that it will not share, reveal, divulge, disclose, disseminate, or publicize any such information to any third party except as provided in this provision without the prior written approval of the Contracting Officer. Contractor also understands and agrees that any subcontractors performing under this contract or order are subject to the same stipulations and that Contractor may be held responsible for any violations of confidentiality by a subcontractor.

(C) These provisions are consistent with and do not supersede, conflict with, or otherwise alter an employee's obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by Executive orders and statutory provisions relating to whistleblower protection are incorporated into this contract and are controlling.

(D) The Government may share the terms, conditions and prices set forth in this Order with, and provide a copy of the Order to, other Executive branch agencies of the U.S. Government, provided that the Government shall ensure that other Executive branch agencies to which it provides such information will be required to treat all such information consistent with terms and conditions set forth in this Order.

(E) Notwithstanding anything in this agreement, the Government may retain any confidential information as required by law, regulation, or its internal document retention procedures for legal, regulatory, or compliance purposes; provided, however, that all such retained confidential information will continue to be subject to the confidentiality obligations of this Order.

(xv) *Authorized users.* Authorized users may include full and part-time employees of the Government, including those working at or from remote locations, and contractors and contractor employees working within the scope of their contract with the Government, including those at or from remote locations.

(xvi) *Authorized use.* Authorized users are authorized to use the product or service acquired under this contract in performing business on behalf of the Government. Any information obtained or acquired by the Government under this contract may be used by the Government in the performance of Government business.

(2) If any language, provision, or clause of this agreement conflicts or is inconsistent with the preceding paragraph (w)(1), the language, provisions, or clause of paragraph (w)(1) shall prevail to the extent of such inconsistency.

(End of clause)

☒ **52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (OCT 2022)**

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

(1) [52.203-19](#), Prohibition on Requiring Certain 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)).

(2) [52.204-23](#), Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Nov 2021) (Section 1634 of Pub. L. 115-91).

(3) [52.204-25](#), Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Sec.889(a)(1)(A) of Pub. L. 115-232)

(4) [52.209-10](#), Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015) (Executive Order 13658).

(5) [52.233-3](#), Protest After Award (Aug 1996) ([31 U.S.C. 3553](#)).

(6) [52.233-4](#), Applicable Law for Breach of Contract Claim (Oct 2004)(Public Laws 108-77 and 108-78 ([19 U.S.C. 3805 note](#))).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

[CONTRACTING OFFICER: CHECK THE CORRESPONDING BOX FOR EACH CLAUSE THAT APPLIES TO THIS ORDER.]

☐ (1) [52.203-6](#), Restrictions on Subcontractor Sales to the Government (Jun 2020), with Alternate I (Oct 1995) ([41 U.S.C. 4704](#) and [10 U.S.C. 2402](#)).

☐ (2) [52.203-13](#), Contractor Code of Business Ethics and Conduct (Nov 2021) (Pub. L. 110-252, Title VI, Chapter 1 ([41 U.S.C. 3509](#))).

☐ (3) [52.203-15](#), Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (June 2010) (Section 1553 of Pub. L. 111-5).

(Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

☐ (4) [52.204-10](#), Reporting Executive Compensation and First-Tier Subcontract Awards (JUN 2020) (Pub. L. 109-282) ([31 U.S.C. 6101 note](#)).

☐ (5) [Reserved]

☐ (6) [52.204-14](#), Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

☐ (7) [52.204-15](#), Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

☒ (8) [52.209-6](#), Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Nov 2021) ([31 U.S.C. 6101 note](#)).

☐ (9) [52.209-9](#), Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) ([41 U.S.C. 2313](#)).

☐ (10) [Reserved]

☐ (11)(i) [52.219-3](#), Notice of HUBZone Set-Aside or Sole-Source Award (Oct 2022) ([15 U.S.C. 657a](#)).

☐ (12) [52.219-4](#), Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2022) (*if the offeror elects to waive the preference, it shall so indicate in its offer*) ([15 U.S.C. 657a](#)).

☐ (13) [Reserved]

☐ (14)(i) [52.219-6](#), Notice of Total Small Business Set-Aside (Mar 2020) ([15 U.S.C. 644](#)).

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

- ☐ (ii) Alternate I (Mar 2020).
- ☐ (15)(i) [52.219-7](#), Notice of Partial Small Business Set-Aside (Mar 2020) ([15 U.S.C. 644](#)).
 - ☐ (ii) Alternate I (Mar 2020) of [52.219-7](#).
- ☐ (16) [52.219-8](#), Utilization of Small Business Concerns (Oct 2022) ([15 U.S.C. 637\(d\)\(2\)](#) and (3)).
- ☐ (17)(i) [52.219-9](#), Small Business Subcontracting Plan (Oct 2022) ([15 U.S.C. 637\(d\)\(4\)](#)).
 - ☐ (ii) Alternate I (Nov 2016) of [52.219-9](#).
 - ☐ (iii) Alternate II (Nov 2016) of [52.219-9](#).
 - ☐ (iv) Alternate III (Jun 2020) of [52.219-9](#).
 - ☐ (v) Alternate IV (Sep 2021) of [52.219-9](#).
- ☐ (18)(i) [52.219-13](#), Notice of Set-Aside of Orders (Mar 2020) ([15 U.S.C. 644\(r\)](#)).
 - ☐ (ii) Alternate I (Mar 2020) of [52.219-13](#).
- ☐ (19) [52.219-14](#), Limitations on Subcontracting (Sep 2021) ([15 U.S.C. 637\(a\)\(14\)](#)).
- ☐ (20) [52.219-16](#), Liquidated Damages—Subcontracting Plan (Jan 1999) ([15 U.S.C. 637\(d\)\(4\)\(F\)\(i\)](#)).
- ☐ (21) [52.219-27](#), Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Oct 2022) ([15 U.S.C. 657 f](#)).
- ☐ (22)(i) [52.219-28](#), Post Award Small Business Program Rerepresentation (Oct 2022) ([15 U.S.C. 632\(a\)\(2\)](#)).
 - ☐ (ii) Alternate I (Mar 2020) of [52.219-28](#).
- ☐ (23) [52.219-29](#), Notice of Set-Aside for Economically Disadvantaged Women-Owned Small Business (EDWOSB) Concerns (Oct 2022) ([15 U.S.C. 637\(m\)](#)).
- ☐ (24) [52.219-30](#), Notice of Set-Aside for Women-Owned Small Business (WOSB) Concerns Eligible Under the WOSB Program (Oct 2022) ([15 U.S.C. 637\(m\)](#)).
- ☐ (25) [52.219-32](#), Orders Issued Directly Under Small Business Reserves (Mar 2020) ([15 U.S.C. 644\(r\)](#)).
- ☐ (26) [52.219-33](#), Nonmanufacturer Rule (Sep 2021) ([15 U.S.C. 637\(a\)\(17\)](#)).
- ☒ (27) [52.222-3](#), Convict Labor (Jun 2003) (E.O. 11755).
- ☒ (28) [52.222-19](#), Child Labor—Cooperation with Authorities and Remedies (Jan 2022) (E.O. 13126).
- ☒ (29) [52.222-21](#), Prohibition of Segregated Facilities (Apr 2015).
- ☒ (30)(i) [52.222-26](#), Equal Opportunity (Sept 2016) (E.O. 11246).
 - ☐ (ii) Alternate I (FEB 1999) of [52.222-26](#).
- ☒ (31)(i) [52.222-35](#), Equal Opportunity for Veterans (Jun 2020) ([38 U.S.C. 4212](#)).
 - ☐ (ii) Alternate I (Jul 2014) of [52.222-35](#).
- ☒ (32)(i) [52.222-36](#), Equal Opportunity for Workers with Disabilities (Jun 2020) ([29 U.S.C. 793](#)).
 - ☐ (ii) Alternate I (Jul 2014) of [52.222-36](#).
- ☐ (33) [52.222-37](#), Employment Reports on Veterans (Jun 2020) ([38 U.S.C. 4212](#)).
- ☐ (34) [52.222-40](#), Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).
- ☒ (35)(i) [52.222-50](#), Combating Trafficking in Persons (Nov 2021) (22 U.S.C. chapter 78 and E.O. 13627).
 - ☐ (ii) [Alternate I](#) (Mar 2015) of [52.222-50](#) (Nov 2021) (22 U.S.C. chapter 78 and E.O. 13627).
- ☐ (36) [52.222-54](#), Employment Eligibility Verification (May 2022). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in [22.1803](#).)
- ☐ (37)(i) [52.223-9](#), Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) ([42 U.S.C. 6962\(c\)\(3\)\(A\)\(ii\)](#)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
 - ☐ (ii) Alternate I (May 2008) of [52.223-9](#) ([42 U.S.C. 6962\(i\)\(2\)\(C\)](#)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
- ☒ (38) [52.223-11](#), Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O. 13693).
- ☐ (39) [52.223-12](#), Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693).
- ☐ (40)(i) [52.223-13](#), Acquisition of EPEAT®-Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514).
 - ☐ (ii) Alternate I (Oct 2015) of [52.223-13](#).
- ☐ (41)(i) [52.223-14](#), Acquisition of EPEAT®-Registered Televisions (Jun 2014) (E.O. 13423 and 13514).
 - ☐ (ii) Alternate I (Jun 2014) of [52.223-14](#).
- ☐ (42) [52.223-15](#), Energy Efficiency in Energy-Consuming Products (May 2020) ([42 U.S.C. 8259b](#)).
- ☐ (43)(i) [52.223-16](#), Acquisition of EPEAT®-Registered Personal Computer Products (Oct 2015) (E.O. 13423).

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

- ☐ (ii) Alternate I (Jun 2014) of [52.223-16](#).
- ☒ (44) [52.223-18](#), Encouraging Contractor Policies to Ban Text Messaging While Driving (Jun 2020) (E.O. 13513).
- ☐ (45) [52.223-20](#), Aerosols (Jun 2016) (E.O. 13693).
- ☐ (46) [52.223-21](#), Foams (Jun 2016) (E.O. 13693).
- ☐ (47)(i) [52.224-3](#), Privacy Training (Jan 2017) (5 U.S.C. 552a).
- ☐ (ii) Alternate I (Jan 2017) of [52.224-3](#).
- ☐ (48)(i) [52.225-1](#), Buy American—Supplies (Oct 2022) ([41 U.S.C. chapter 83](#)).
- ☐ (48)(ii) Alternate I (Oct 2022) of 52.225-1.
- ☐ (49)(i) [52.225-3](#), Buy American—Free Trade Agreements—Israeli Trade Act (Oct 2022) ([41 U.S.C. chapter 83](#), [19 U.S.C. 3301](#) note, [19 U.S.C. 2112](#) note, [19 U.S.C. 3805](#) note, [19 U.S.C. 4001](#) note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).
- ☐ (ii) Alternate I (Jan 2021) of [52.225-3](#).
- ☐ (iii) Alternate II (Jan 2021) of [52.225-3](#).
- ☐ (iv) Alternate III (Jan 2021) of [52.225-3](#).
- ☐ (v) Alternate IV (Oct 2022) of [52.225-3](#).
- ☐ (50) [52.225-5](#), Trade Agreements (Oct 2019) ([19 U.S.C. 2501](#), *et seq.*, [19 U.S.C. 3301](#) note).
- ☐ (51) [52.225-13](#), Restrictions on Certain Foreign Purchases (Feb 2021) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).
- ☐ (52) [52.225-26](#), Contractors Performing Private Security Functions Outside of the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; [10 U.S.C. 2302 Note](#)).
- ☐ (53) [52.226-4](#), Notice of Disaster or Emergency Area Set-Aside (Nov 2007) ([42 U.S.C. 5150](#)).
- ☐ (54) [52.226-5](#), Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) ([42 U.S.C. 5150](#)).
- ☐ (55) [52.229-12](#), Tax on Certain Foreign Procurements (Feb 2021).
- ☐ (56) [52.232-29](#), Terms for Financing of Purchases of Commercial Items (Nov 2021) ([41 U.S.C. 4505](#), [10 U.S.C. 2307\(f\)](#)).
- ☐ (57) [52.232-30](#), Installment Payments for Commercial Items (Nov 2021) ([41 U.S.C. 4505](#), [10 U.S.C. 2307\(f\)](#)).
- ☒ (58) [52.232-33](#), Payment by Electronic Funds Transfer—System for Award Management (Oct 2018) ([31 U.S.C. 3332](#)).
- ☐ (59) [52.232-34](#), Payment by Electronic Funds Transfer—Other than System for Award Management (Jul 2013) ([31 U.S.C. 3332](#)).
- ☐ (60) [52.232-36](#), Payment by Third Party (May 2014) ([31 U.S.C. 3332](#)).
- ☐ (61) [52.239-1](#), Privacy or Security Safeguards (Aug 1996) ([5 U.S.C. 552a](#)).
- ☐ (62) [52.242-5](#), Payments to Small Business Subcontractors (JAN 2017) ([15 U.S.C. 637\(d\)\(13\)](#)).
- ☐ (63)(i) [52.247-64](#), Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) ([46 U.S.C. Appx. 1241\(b\)](#) and [10 U.S.C. 2631](#)).
- ☐ (ii) Alternate I (Apr 2003) of [52.247-64](#).
- ☐ (iii) Alternate II (Nov 2021) of [52.247-64](#).

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

- ☐ (1) [52.222-41](#), Service Contract Labor Standards (Aug 2018) ([41 U.S.C. chapter 67](#)).
- ☐ (2) [52.222-42](#), Statement of Equivalent Rates for Federal Hires (May 2014) ([29 U.S.C. 206](#) and [41 U.S.C. chapter 67](#), *et seq.*).
- ☐ (3) [52.222-43](#), Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (Multiple Year and Option Contracts) (Aug 2018) ([29 U.S.C. 206](#) and [41 U.S.C. chapter 67](#)).
- ☐ (4) [52.222-44](#), Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (May 2014) ([29 U.S.C. 206](#) and [41 U.S.C. chapter 67](#), *et seq.*).
- ☐ (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) ([41 U.S.C. chapter 67](#), *et seq.*).
- ☐ (6) [52.222-53](#), Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (May 2014) ([41 U.S.C. chapter 67](#), *et seq.*).
- ☐ (7) [52.222-55](#), Minimum Wages for Contractor Workers Under Executive Order 14026 (Jan 2022). ([FAC 2022-04](#))
- ☐ (8) [52.222-62](#), Paid Sick Leave Under Executive Order 13706 (Jan 2022) (E.O. 13706). ([FAC 2022-04](#))
- ☐ (9) [52.226-6](#), Promoting Excess Food Donation to Nonprofit Organizations (JUN 2020) ([42 U.S.C. 1792](#)).

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

(d) *Comptroller General Examination of Record*. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at [52.215-2](#), Audit and Records—Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR [Subpart 4.7](#), Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

- (i) [52.203-13](#), Contractor Code of Business Ethics and Conduct (Nov 2021) (Pub. L. 110-252, Title VI, Chapter 1 ([41 U.S.C. 3509](#))).
- (ii) [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)).
- (iii) [52.204-23](#), Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Nov 2021) (Section 1634 of Pub. L. 115-91).
- (iv) [52.204-25](#), Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Sec. 889(a)(1)(A) of Pub. L. 115-232)
- (v) [52.219-8](#), Utilization of Small Business Concerns (Oct 2018) ([15 U.S.C. 637\(d\)\(2\)](#) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds \$700,000 (\$1.5 million for construction of any public facility), the subcontractor must include [52.219-8](#) in lower tier subcontracts that offer subcontracting opportunities.
- (vi) [52.222-21](#), Prohibition of Segregated Facilities (Apr 2015).
- (vii) [52.222-26](#), Equal Opportunity (Sept 2016) (E.O. 11246).
- (viii) [52.222-35](#), Equal Opportunity for Veterans (JUN 2020) ([38 U.S.C. 4212](#)).
- (ix) [52.222-36](#), Equal Opportunity for Workers with Disabilities (JUN 2020) ([29 U.S.C. 793](#)).
- (x) [52.222-37](#), Employment Reports on Veterans (JUN 2020) ([38 U.S.C. 4212](#)).
- (xi) [52.222-40](#), Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause [52.222-40](#).
- (xii) [52.222-41](#), Service Contract Labor Standards (Aug 2018) ([41 U.S.C. chapter 67](#)).
- (xiii) ☐ (A) [52.222-50](#), Combating Trafficking in Persons (Nov 2021) (22 U.S.C. chapter 78 and E.O. 13627).
☐ (B) Alternate I (Mar 2015) of [52.222-50](#) (Nov 2021) (22 U.S.C. chapter 78 and E.O. 13627).
- (xiv) [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) ([41 U.S.C. chapter 67](#)).
- (xv) [52.222-53](#), Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (May 2014) ([41 U.S.C. chapter 67](#)).
- (xvi) [52.222-54](#), Employment Eligibility Verification (May 2022) (E.O. 12989).
- (xvii) [52.222-55](#), Minimum Wages for Contractor Workers Under Executive Order 14026 (Jan 2022). (*FAC 2022-04*)
- (xiii) [52.222-62](#), Paid Sick Leave Under Executive Order 13706 (Jan 2022) (E.O. 13706). (*FAC 2022-04*)
- (xix)(A) [52.224-3](#), Privacy Training (Jan 2017) (5 U.S.C. 552a).
(B) Alternate I (Jan 2017) of [52.224-3](#).
- (xx) [52.225-26](#), Contractors Performing Private Security Functions Outside of the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; [10 U.S.C. 2302 Note](#)).
- (xxi) [52.226-6](#), Promoting Excess Food Donation to Nonprofit Organizations (JUN 2020) ([42 U.S.C. 1792](#)). Flow down required in accordance with paragraph (e) of FAR clause [52.226-6](#).

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

(xxii) [52.247-64](#), Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) ([46 U.S.C. Appx. 1241\(b\)](#) and [10 U.S.C. 2631](#)). Flow down required in accordance with paragraph (d) of FAR clause [52.247-64](#).

(2) While not required, the contractor may include in its subcontracts for commercial products and commercial services a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of clause)

☐ **52.223-2 AFFIRMATIVE PROCUREMENT OF BIOBASED PRODUCTS UNDER SERVICE AND CONSTRUCTION CONTRACTS (SEP 2013)**

***fill-in information in paragraph (d); enter agency point of contact name, phone #, and e-mail address ***

☐ **52.225-8 DUTY-FREE ENTRY (OCT 2010)**

☒ **52.232-18 AVAILABILITY OF FUNDS (APR 1984)**

☒ **52.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (JUN 2013)**

☒ **52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (NOV 2021)**

☐ **52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (NOV 2020)**

CONTRACTING OFFICER: List additional FAR clauses below, as needed, by entering the clause number, title, and date for each clause added.

The following clauses are also applicable as indicated below.

☒ **DEA-2852.203-70 FORMER EMPLOYMENT OR ASSIGNMENT WITH THE DEA (SEP 2021)**

(a) Any offeror or contractor who intends to employ any individual who either currently works for DEA, or had been employed with DEA as a Federal employee within the previous **five (5) years** for work supporting a prospective or active DEA contract must notify DEA of its intent as described in this clause.

(b) The offeror or contractor shall instruct any prospective or current employee meeting the criteria in paragraph (a), above, to complete and sign a DEA Contractor Ethics Questionnaire. The questionnaire is available for download at https://www.dea.gov/sites/default/files/2020-06/contractor_ethics_questionnaire_jan_2020.pdf. When the intent to employ such individual is known prior to the award of a new contract or order, the contractor shall submit the employee's completed questionnaire and résumé to DEA concurrently with its proposal. When the intent is to employ such individual under an existing contract or order, the contractor shall submit the completed questionnaire and résumé electronically to the cognizant DEA contracting officer **AND** ethicsFAC@usdoj.gov.

(c) The offeror or contractor understands that any such employees described in paragraph (a) are prohibited from appearing before, or communicating with, the Federal Government on behalf of a contractor regarding a Government contract, investigation or other particular matter that they participated in personally and substantially as a Federal employee with the intent to influence Government officials in those matters for the lifetime of those matters.

(d) The offeror or contractor further understands that for two (2) years after leaving the Federal Government, such employees described in paragraph (a) are prohibited from appearing before, or communicating with, the Government with the intent to influence on behalf of a contractor regarding a Government contract, investigation or other particular matter that they did not participate in personally and substantially as a Federal employee, but that was under their official responsibility during their last year in the Government. For purposes of this clause, an employee is defined as one appointed under Title 5, Section 2015 or Title 21, Section 878 of the United States Code.

(e) If DEA determines after reviewing questionnaire responses or conducting other inquiries that the prospective employee is disqualified for assignment to the contract based on an unfavorable suitability and/or security determination, or may violate the post-employment restrictions described in paragraphs (c) or (d), above, or other applicable laws if allowed to work on or support the contract/task order, at DEA's request, the offeror or contractor must not assign such employee to work under a prospective or active contract.

(f) If an offeror or contractor fails to provide a required Questionnaire, the prospective employee will not be approved to work under the DEA contract or order until such time as the Questionnaire is submitted, reviewed, and approved in accordance with established procedures.

(End of clause)

☐ **DEA-2852.203-72 WHISTLEBLOWER INFORMATION DISTRIBUTION (OCT 2021)**

Within 30 days of contract award, the contractor and its subcontractors must distribute the "Whistleblower Information for Employees of DOJ Contractors, Subcontractors, Grantees, or Sub-Grantees or Personal Services Contractors" ("Whistleblower Information") document to their employees performing work in support of the products and services delivered under this contract (<https://oig.justice.gov/sites/default/files/2020-04/NDAA-brochure.pdf>). By agreeing to the terms and conditions of this contract, the prime contractor acknowledges receipt of this requirement, in accordance with 41 U.S.C. § 4712 and FAR 3.908 & 52.203-17, and

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

commits to distribution. Within 45 days of award, the contractor must provide confirmation to the contracting officer verifying that it has distributed the whistleblower information as required. version includes all of the information in the English language document.

(End of clause)

☒ DEA-2852.209-70 ORGANIZATIONAL CONFLICTS OF INTEREST (SEP 2021)

(a) The Contractor warrants that, to the best of its knowledge and belief, there are no relevant facts or circumstances that would give rise to an organizational conflict of interest, as defined in FAR Subpart 9.5, or that the Contractor has disclosed all such relevant information.

(b) In the event that an actual, potential, or apparent organizational conflict of interest is discovered after award, the Contractor shall make full disclosure of the particular facts and circumstances to the Contracting Officer in writing. This disclosure shall include a description of the actions that the Contractor has taken, or proposes to take in order to avoid, mitigate, or neutralize the risk to the Government.

(c) Remedies. The Contracting Officer may terminate this contract for convenience, in whole or in part, if deemed necessary to avoid or mitigate an actual or apparent organizational conflict of interest. In the event that the Contractor failed to disclose in a timely manner, or misrepresented the facts and circumstances of, an actual, potential, or apparent organizational conflict of interest of which it had prior knowledge, the Contracting Officer may terminate this contract for default or cause, and pursue additional remedies, including debarment, as may be provided by law.

(d) In the event of repetitive failures to provide this report, the contract may be terminated for default.

(End of clause)

☐ DEA-2852.211-71 SCHEDULED AND UNSCHEDULED CLOSURES OF GOVERNMENT OFFICES (JUL 2021)

(a) In accordance with [5 U.S.C. 6103](#), Federal Government offices are closed for ordinary business in observance of the following holidays:

- New Year's Day
- Birthday of Martin Luther King, Jr.
- Washington's Birthday
- Memorial Day
- Juneteenth
- Independence Day
- Labor Day
- Columbus Day
- Veteran's Day
- Thanksgiving Day
- Christmas Day
- Inauguration Day (*Federal offices in the Washington DC metropolitan area only*)

(b) Federal offices may close at other times without advance notice due to emergencies, inclement weather, interruption of utilities, or other reasons. Such closures may be declared by the President, Office of Personnel Management, Office of Management and Budget, the Administrator of the DEA, or other appropriate executive authority. The duration of such closures may range from an early closure with normal operations expected on the next business day to a period of indeterminate length.

(c) At the time that a closure is declared, appropriate information, notifications, and instructions will be provided regarding the return to normal operations. The Contractor shall comply with all directives issued in regards to such closures. The Contractor shall follow agency procedures for registering emergency contact information and shall monitor appropriate broadcast mediums for receiving emergency information.

(d) When a closure is declared, contractor personnel must vacate the facility as directed except personnel designated in accordance with agency procedures by the contracting officer to remain onsite to continue performance. Evacuated personnel will not be allowed to reenter the facility for the duration of the closure. Performance of work at alternate sites is not permissible except in accordance with the terms of the contract and written authorization by the contracting officer.

(e) Whenever it is necessary for contractor employees to continue performance during such closures, the contracting officer will provide written authorization for such work. Such written authorization will designate the specific individuals authorized to continue performance, alternate work sites when applicable, work schedules, work dates, and special instructions and information. Telework may be authorized if permitted by the terms of the contract. Any services scheduled to be performed at Government facilities shall not be performed elsewhere unless specifically authorized in accordance with the terms of this contract.

(f) For firm fixed priced contracts, the terms for invoicing and payment in the contract will remain unchanged unless changed by a fully executed modification to the contract.

(g) For other than firm fixed priced contracts, the contractor shall invoice in accordance with the Payments and Prompt Payment clauses of the contract only for work performed. Employee compensation for the period of the closure shall be governed by corporate policy.

(h) Agency-sponsored events such as picnics or other social events are not considered to be official office closures. The Contractor shall not invoice for time spent by its employees attending or participating in such events.

(i) In no case will any compensable administrative leave, which might be approved for Federal employees in connection with official holidays or other events, extend to contractor personnel.

[End of clause]

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

☒ **DEA-2852.218-70 CONTINUING CONTRACT PERFORMANCE DURING A PANDEMIC INFLUENZA OUTBREAK OR OTHER BIOMEDICAL EMERGENCY OR CATASTROPHE (JUL 2021)**

(a) It has been determined that the services provided under this contract are mission-critical and essential to the ongoing operations of the Drug Enforcement Administration.

(b) In the event of a pandemic influenza outbreak or other biomedical emergency or catastrophe, the Contractor shall continue performance of this contract without delay or interruption.

(c) The Government will provide notice, information, and instructions to the Contractor regarding any such event. If it is determined that changes to the performance requirements are necessary, the Government will implement the necessary changes by the issuance of Change Orders in accordance with the Changes clause of the contract, and the Contractor may assert its right for an equitable adjustment accordingly. Additional information and guidance is provided in the attached notice entitled, "Continuing Contract Performance during a Pandemic Influenza or Other National Emergency."

(d) Additional information and guidance is provided in the notice entitled, "Continuing Contract Performance During a Pandemic Influenza or Other National Emergency," which may be viewed at <https://dojnet.doi.gov/jmd/seps/emergency/pio-plan/contract-performance.pdf>.

(End of clause)

☐ **DEA-2852.219-70 SECTION 8(a) DIRECT AWARD (MAY 2012)**

(a) Pursuant to the Partnership Agreement (PA) between the U.S. Small Business Administration (SBA) and the U.S. Department of Justice (DOJ), the U.S. Drug Enforcement Administration (DEA), a component of the DOJ, hereby executes a direct award to **[enter name of 8a concern]**, under the authority delegated to it by the SBA in accordance with 13 CFR 124.501 and the PA. DEA will perform all contract execution and review functions pertaining to this award in accordance with the delegation. The DEA will notify the SBA of this award, as required by 13 CFR 124.503(a)(4)(ii), and provide SBA with a copy of the award.

(b) Notwithstanding the identification of the parties on the award form, the prime Contractor for this award is the U.S. Small Business Administration, and **[enter name of 8a concern]** is the Subcontractor.

(c) The cognizant SBA district office is:

[SBA district office]

[street address]

[city, state, zip code]

(d) **[enter name of 8a concern]** shall:

(1) Notify the Contracting Officer, simultaneous with its notification to the SBA (as required by SBA's 8(a) regulations at 13 CFR 124.308), when the owner or owners upon whom 8(a) eligibility is based plan to relinquish ownership or control of the concern. Consistent with Section 407 of Public Law 100-656, transfer of ownership or control shall result in termination of the contract for convenience, unless the SBA waives the requirement for termination prior to the actual relinquishing of ownership and control;

(2) Comply with the applicable performance requirements of clause [52.219-14](#), Limitations on Subcontracting as checked below: *[Contracting officer: check only one performance standard based on the primary purpose of the contract.]*

- ☐ *Services (except construction)* — At least 50 percent of the cost of contract performance incurred for personnel shall be expended for employees of the concern.
- ☐ *Supplies (other than procurement from a nonmanufacturer of such supplies)* — The concern shall perform work for at least 50 percent of the cost of manufacturing the supplies, not including the cost of materials.
- ☐ *General construction* — The concern will perform at least 15 percent of the cost of the contract, not including the cost of materials, with its own employees.
- ☐ *Construction by special trade contractors* — The concern will perform at least 25 percent of the cost of the contract, not including the cost of materials, with its own employees.

(3) Provide the contracting officer with evidence of compliance with the applicable performance standard. This report shall show total dollars expended in the cost category specified in the performance standard both for the reporting period and cumulative to date along with the dollars and percentage of total dollars expended from the contractor's resources. This report shall be submitted annually. A final report covering the entire period of the contract shall be submitted upon expiration of the contract.

(4) Not subcontract the performance of any of the requirements of this contract without the prior written approval of the Contracting Officer.

(e) Compliance with the Limitation on Subcontracting clause is a mandatory performance requirement of this contract.

(End of clause)

☐ **DEA-2852.222-70 APPLICABLE WAGE DETERMINATION (SERVICE CONTRACT LABOR STANDARDS) (APR 2021)**

(a) In accordance with clause 52.222-41, Service Contract Labor Standards, the minimum monetary wages and fringe benefits applicable to this contract are

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

set forth in the attached Wage Determination(s):

Wage Determination #	Revision #	Date	Section J Attachment #

(b) The Contractor shall attach a copy of this (these) wage determination(s) to Wage and Hour Division (WHD) poster [WH-1313](#), Employee Rights on Government Contracts, and shall post both the publication and the wage determination(s) in a prominent and accessible location in the workplace as required by Federal Acquisition Regulation 22.1018(c). [WH-1313](#) is available for downloading at <http://www.dol.gov/whd/regs/compliance/posters/sca.htm> (Spanish language version available at <http://www.dol.gov/whd/regs/compliance/pdf/scaspan.pdf>).

(c) The Contractor shall classify each service employee who will perform under this contract by the applicable wage determination according to the work performed by the employee. If the applicable wage determination does not include an appropriate occupational code, title, and wage rate for a service employee employed under the contract, the Contractor shall initiate the conformance process in accordance with paragraph (c) of clause 52.222-41 and corresponding instructions provided by the WHD at https://www.dol.gov/sites/dolgov/files/WHd/legacy/files/SCA_Conformance_Guide.pdf.

(End of clause)

☐ **DEA-2852.237-70 PREVENTING PERSONAL SERVICES CONTRACTS AND PERFORMANCE OF INHERENTLY GOVERNMENT FUNCTIONS (JUN 2018)**

(a) A personal services contract is characterized by the employer-employee relationship it creates between the Government and the contractor's personnel. This contract action is for non-personal services and is not a personal services contract action. Due to the need for close interaction of government and contractor personnel, it is essential for all contractor personnel for this contract performing at Drug Enforcement Administration (DEA) designated worksites to receive supervision from their parent company and avoid employer-employee relationships with government officials. In addition, it is important for contractor personnel to recognize and avoid circumstances that may appear to be personal services. Federal Acquisition Regulation (FAR) subpart [37.104](#) provides important information to be aware of to avoid performing these types of duties. The contractor awarded this contract shall ensure their employees and subcontractors comply with this requirement and receive supervision from their parent company to avoid performance of a personal services contract.

(b) "[Inherently governmental function](#)" means, as a matter of policy, a function so intimately related to the public interest as to mandate performance by Government employees. An inherently governmental function includes activities requiring either the exercise of discretion in applying Government authority, or the making of value judgments in making decisions for the Government. Governmental functions normally fall into two categories: the act of governing, *i.e.*, the discretionary exercise of Government authority, and monetary transactions and entitlements. It is essential for all contractor personnel performing services at DEA designated worksites to recognize and understand what inherently government functions are. Federal Acquisition Regulation (FAR) [subpart 7.5 - Inherently Governmental Functions](#) and the Office of Management and Budget's (OMB) [Office of Federal Procurement Policy \(OFPP\) Policy Letter 11-01](#), Performance of Inherently Governmental and Critical Functions, provide important information regarding inherently governmental functions to be aware of to avoid performing these types of duties. The contractor awarded this contract shall ensure their employees and subcontractors comply with this requirement.

(c) Contractors providing personnel who perform services on-site at DEA offices must certify via the "Contractor Employee Certification Concerning Prohibition of Personal Services Contracts and Inherently Governmental Functions" form that its on-site employee(s) have read and understand FAR [37.104](#), Personal services contracts, and FAR [subpart 7.5](#) before they may begin work at an on-site DEA office. The Contractor on-site supervisor shall address any questions or concerns with the Contracting Officer's Representative (COR) or Contracting Officer.

(End of Clause)

☐ **DEA-2852.239-71 INFORMATION RESELLERS OR DATA BROKERS (MAY2012)**

(a) Under this contract, the Drug Enforcement Administration (DEA) obtains personally identifiable information about individuals from the contractor.

(b) The Contractor certifies that it has a security policy in place that contains procedures to promptly notify any individual whose personally identifiable information (as defined by OMB) was, or is reasonable believed to have been, breached. Any notification shall be coordinated with the DEA, and shall not proceed until the DEA has made a determination that notification would not impede a law enforcement investigation or jeopardize national security.

(c) The method and content of any notification by the contractor shall be coordinated with, and be subject to the approval of, the DEA/DOJ. The Contractor assumes full responsibility for taking corrective action consistent with the DEA's Guidelines for Data Breach Notification (December 2, 2011), which may include offering credit monitoring when appropriate.

(End of clause)

☐ **DEA-2852.239-73 SECURITY OF DOJ INFORMATION AND SYSTEMS (AUG 2020)**

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 U.S. Department of Justice (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, October 2022

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

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

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.

- A. 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.
- B. 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 0904](#), 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

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

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;
 11. 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;
 12. 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;
 13. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards;
 14. 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;
 15. 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;
 16. 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
 17. 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

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

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,

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

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.

(End of Clause)

☐ DEA-2852.239-74 CERTIFICATION OF OPERABILITY ON SYSTEMS USING THE FEDERAL DESKTOP CORE CONFIGURATION OR THE UNITED STATES GOVERNMENT CONFIGURATION BASELINE (MAY 2012)

(a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC) or the United States Government Configuration Baseline (USGCB). This includes Internet Explorer 7 and 8 configured to operate on Windows XP, Windows Vista, and Windows 7 (in Protected Mode on Windows Vista and Windows 7).

- For the Windows XP settings, see: http://csrc.nist.gov/itsec/guidance_WinXP.html.
- For the Windows Vista settings, see: http://csrc.nist.gov/itsec/guidance_vista.html.
- For Windows 7 settings, see: http://usgcb.nist.gov/usgcb_content.html.

(b) The standard installation, operation, maintenance, updating, and/or patching of software shall not alter the configuration settings from the approved FDCC or USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall.

(c) Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

(End of clause)

☐ DEA-2852.242-70 CONTRACTOR PERFORMANCE ASSESSMENT (MAR 2020)

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

(a) Pursuant to FAR [subpart 42.15](#), the Government will assess the Contractor's performance under this contract. Performance assessment information may be used by the Government for decision-making on exercise of options, source selection, and other purposes, and will be made available to other federal agencies for similar purposes.

(b) Performance will be assessed in the following areas:

- (1) Quality of product or service;
- (2) Schedule;
- (3) Cost control;
- (4) Business relations;
- (5) Management of key personnel; and
- (6) Other appropriate areas.

(c) For contracts that include the clause at [52.219-9](#), Small Business Subcontracting Plan, performance assessments will consider performance against, and efforts to achieve, small business subcontracting goals set forth in the small business subcontracting plan.

(d) For any contract with a performance period exceeding 18 months, inclusive of all options, the Government will perform interim performance assessments annually and a final performance assessment upon completion of the contract.

(e) The Government will prepare contractor performance assessment reports electronically using the Contractor Performance Assessment Reporting System (CPARS). Additional information on CPARS may be found at www.cpars.gov.

(f) The Contractor will be provided access to CPARS to review performance assessments. The Contractor shall designate a CPARS point-of-contact for each contract subject to performance assessment reporting. Upon setup of a contract in CPARS, the Contractor's CPARS point-of-contact will receive a system-generated e-mail with information and instructions for using CPARS. Prior to finalizing any contractor performance assessment, the Contractor shall be given 14 calendar days to review the report and submit comments, rebutting statements, or additional information. Disagreements between the Contractor and the Government performance assessment official will be resolved by a Government Reviewing Official, whose decision on the matter will be final.

(g) The Government will also report in the Federal Awardee Performance and Integrity Information System (FAPIIS) module of CPARS information related to:

- (1) A Contracting Officer's final determination that a contractor has submitted defective cost or pricing data;
- (2) Any subsequent change to a final determination concerning defective cost or pricing data pursuant to 15.407-1(d);
- (3) Any issuance of a final termination for default or cause notice; or
- (4) Any subsequent withdrawal or a conversion of a termination for default to a termination for convenience.

(End of clause)

☒ **DEA-2852.242-71 INVOICE REQUIREMENTS (MAY 2012)**

(a) The Contractor shall submit scanned or electronic images of invoice(s) to the following e-mail addresses:

- (1) Invoice.HR@dea.gov;
- (2) teresa.a.roshaudelgado@dea.gov; and
- (3) [enter COR's or Task Monitor's name & e-mail address, if applicable].

(b) The date of record for invoice receipt is established on the day of receipt of the e-mail if it arrives before the end of standard business hours (5 p.m. local), or the next business day if the invoice arrives outside of normal business hours. Scanned documents with original signatures in .pdf or other graphic formats attached to the e-mail are acceptable. Digital/electronic signatures and certificates cannot be processed by DEA and will be returned.

(c) In addition to the items required in FAR [32.905\(b\)](#), a proper invoice shall also include the following minimum additional information and/or attached documentation:

- (1) Total/cumulative charges for the billing period for each Contract Line Item Number (CLIN);
- (2) Dates upon which items/services were delivered; and
- (3) The Contractor's Taxpayer Identification Number (TIN).

(d) Invoices will be rejected if they are illegible or otherwise unreadable, or if they do not contain the required information or signatures.

(End of Clause)

☒ **DEA-2852.242-72 FINAL INVOICE AND RELEASE OF RESIDUAL FUNDS (MAY 2012)**

(a) The Contractor shall submit a copy of the final invoice to the Contracting Officer at the address listed in clause DEA-2852.242-71, Invoice Requirements. The final invoice must be marked "Informational Copy – Final Invoice."

(b) By submission of the final invoice and upon receipt of final payment, the Contractor releases the Government from any and all claims arising under, or by virtue of, this contract. Accordingly, the Government shall not be liable for the payment of any future invoices that may be submitted under the above referenced order.

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

(c) If residual funds on the contract total \$100 or less after payment of the final invoice, the Government will automatically deobligate the residual funds without further communication with the vendor.

(d) If funds greater than \$100 remain on this order after payment of the final invoice, the Government will issue a bilateral modification to deobligate the residual funds. The contractor will have up to **30** calendar days after issuance of the modification to sign and return it. The contractor's signature on the modification shall constitute a release of all claims against the Government arising by virtue of this contract, other than claims, in stated amounts, that the Contractor has specifically exempted from the operation of the release. If the contractor fails to sign the modification or assert a claim within the stated period, the Government will deobligate the residual balance and proceed with close-out of the contract.

(End of clause)

☐ **DEA-2852.242-80 CONTRACTOR TELEWORK (OCT 2018)**

(a) Definitions.

"Telework" means a work flexibility arrangement, including situational telework (weather or event-related) that allows Contractor and/or Subcontractors to perform the duties and responsibilities of their position from an approved alternative work site. The arrangement may not include hours that exceed the normal hours worked during an invoice pay period.

"Contracting Officer's Representative" (COR) means an individual designated and authorized in writing by the Drug Enforcement Administration (DEA) to perform specific technical or administrative functions.

"Contractor" means an employee of the Parent Company currently working onsite at a DEA facility.

"Contractor Program Manager" means the onsite supervisor or designated supervisor for Contractors.

"Parent Company" means a business entity holding a current contract with the DEA under which its employees (the Contractor) is performing.

"Program Office" includes the Office Head, Special Agent in Charge, Laboratory Director, Regional Director, Country Attaché or their designees.

"Task Monitor" means an individual designated and authorized in writing by DEA to conduct and document day to day contract administration functions in the field.

(b) The Program Office may approve a telework plan and have overall responsibility for the administration of this clause within their organizational jurisdiction.

(c) The COR/TM, in conjunction with the Program Office must make a written determination that:

- (1) Certain work functions or the missions of certain work units are suitable for a telework arrangement;
- (2) The Contractor is suitable for telework based on individual performance, program requirements and mission objectives;
- (3) Summary of work performed during teleworked hours is submitted to the COR/TM on a bimonthly basis;
- (4) The Contractor shall sign and submit the completed DEA Contractor Telework Agreement Form;
- (5) The COR/TM shall retain the signed DEA Contractor Telework Agreement Form in the contract file for record keeping;
- (6) The Contractor shall obtain the necessary technology prior to teleworking:

(i) Firebird Anywhere - <http://intranet/sites/si/Mobile/fba/Pages/default.aspx>; OR

(ii) DEA issued Laptop--If the contractor's current computer is a desktop, the Program Office may request a laptop using a DEA-19 form for the Contractor to take home when teleworking.

(7) The COR/TM and the Contractor shall review and re-sign, if approved, the DEA Contractor Telework Agreement on an annual basis.

(8) The Program Office or the Contractor reserves the right to terminate the Contractor Telework Agreement at any time.

(9) Within thirty (30) days of the date this clause is incorporated into the contract, the Program Office shall submit to the COR/TM and the cognizant Contracting Officer a plan for how it will implement authorizations for approved telework locations. The plan will describe the specific work and tasks that may be suitable for performance at a temporary work location, the personnel who may be assigned to perform the work, the methods the Program Office will use to manage, supervise, and perform quality control, and any other relevant information. Hours worked, as well as performance shall be tracked on a daily basis.

(d) Under no circumstance will the Contractor be authorized to perform any work requiring access to DOJ/DEA information or information systems unless such access will be made exclusively using DEA equipment or property issued for this purpose.

(e) No authorization for telework shall be construed as an indication of past performance, an increase in the price of the contract, an approval of overtime, a change in the contract schedule, or approval of an accelerated rate of expenditures.

(f) Local commuting expenses incurred in traveling to or from any approved telework location are not reimbursable. Any incidental costs incurred in performing work at approved telework locations will be reimbursable in accordance with the Allowable Cost and Payment clause and the Payments clause of the contract, provided that such costs are segregated and allocable to the contract.

(g) The contractor is responsible for protecting and using any DEA-owned or provided equipment or other property for official purposes only. DEA is

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

responsible for servicing, and maintaining any DEA-provided equipment issued to the Contractor. DEA is not liable for injuries or damages to the Contractor's personal or real property while the Contractor is working at the approved telework location.

End of clause

☐ **DEA-2852.242-81 CONTRACTOR RECORDS MANAGEMENT REQUIREMENTS (SEP 2020)**

A. Applicability

This clause applies to all contractors whose employees create, receive, or maintain federal records as defined below in Section B.

B. Definitions

"Federal record," 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a federal agency under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. DEA Federal Records include records created, received, or maintained by the contractor its employees, agents, or subcontractors pursuant to this contract; and, deliverables and documentation associated with deliverables. Personal materials are not considered federal records.

C. Requirements

1. The contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, and 33), NARA regulations at 36 C.F.R. Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. § 552a). These policies include the preservation of all DEA records, regardless of form or characteristics, mode of transmission, or state of completion.
2. In accordance with 36 C.F.R. § 1222.32, all data created for government use and delivered to, or falling under the legal control of the government are federal records subject to the provisions of 44 U.S.C. Chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. § 552), as amended, and the Privacy Act of 1974 (5 U.S.C. § 552a), as amended, and must be managed and scheduled for disposition only as permitted by statute or regulation.
3. In accordance with 36 C.F.R. § 1222.32, the contractor shall maintain all DEA records created for DEA use or created in the course of performing this contract and/or delivered to, or under the legal control of the government, and records must be managed in accordance with federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.
4. DEA and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records shall not be destroyed except in accordance with the provisions of the agency records schedules and with concurrence of the DEA Contracting Officer. Records may not be removed from the legal custody of DEA without the written concurrence of the Deputy Assistant Administrator, Office of Acquisition and Relocation Management. Willful and unlawful destruction, damage, or alienation of federal records is subject to the fines and penalties imposed by 18 U.S.C. § 2701. In the event that the contractor determines that there has been an unlawful or accidental unauthorized destruction, accidental removal, or alteration of federal records within its control, or within the control of its employees and agents, the contractor shall immediately report the incident to the DEA Contracting Officer of all facts and circumstances related to the discovered destruction or removal. The DEA Contracting Officer must advise DEA's Office of Administration, Freedom of Information and Records Management Section (FSR) of any such incidents and FSR must report promptly to NARA in accordance with 36 C.F.R. § 1230.
5. The contractor shall immediately notify the appropriate DEA Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records, or equipment. Disclosure of non-public information is limited to authorized personnel with a need to know as described in this contract. The contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of DEA information, data, documentary material, records, and/or equipment are properly protected. The contractor shall not remove material from DEA facilities or systems, or facilities or systems operated or maintained on the DEA's behalf, without the express written permission of the Deputy Assistant Administrator, Office of Acquisition and Relocation Management. When information, data, documentary material, records, and/or equipment is no longer required, it shall be returned to DEA's control or the contractor must hold it until otherwise directed. Items returned to DEA shall be hand carried, mailed, emailed, or securely electronically transmitted to the DEA Contracting Officer or address prescribed in this contract. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).
6. The contractor is required to obtain the DEA Contracting Officer's approval prior to engaging in any contractual relationship (sub-contract) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The contractor (and any subcontractor) is required to abide by government and DEA guidance for protecting sensitive, proprietary, classified, and controlled unclassified information. The contractor shall:
 - Incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under DEA awarded contracts, and require written subcontractor acknowledgment of same.
 - Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor
7. The contractor shall only use government-furnished equipment or resources for purposes specifically tied to or authorized by the contract.
8. The contractor shall not create or maintain any records containing any non-public DEA information that are not specifically tied to or authorized by the contract.
9. Notwithstanding the Rights in Data clause of the contract, the contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

information covered by the Privacy Act of 1974 or that is exempt from disclosure by the Freedom of Information Act.

10. In accordance with the Rights in Data clause of the contract, DEA reserves its rights to data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which DEA shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.
11. Training. All contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take DEA provided records management training. The contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

D. Flowdown of requirements to subcontractors

1. The contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract/order, and require written subcontractor acknowledgement of the requirements.
2. Violation by any subcontractor of any provision set forth in this clause will be attributed to the contractor.

(End of clause)

☒ DEA-2852.247-70 GENERAL PACKAGING AND MARKING REQUIREMENTS (MAY 2012)

(a) Packaging and packing for all items (includes written materials, reports, presentations, etc.) delivered hereunder shall be in accordance with common commercial practices, adequate to insure protection from possible damage resulting from improper handling, inclement weather, water damage, excessive heat and cold, and to insure acceptance by a common carrier for safe delivery to its final destination.

(b) All deliverables shall clearly indicate the contract number and/or task (delivery) order number, as appropriate, on or adjacent to the exterior shipping label.

(End of clause)

☒ 52.223-99 ENSURING ADEQUATE COVID-19 SAFETY PROTOCOLS FOR FEDERAL CONTRACTORS (OCT 2021) (DEVIATION)

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

United States or its outlying areas means—

- (1) The fifty States;
- (2) The District of Columbia;
- (3) The commonwealths of Puerto Rico and the Northern Mariana Islands;
- (4) The territories of American Samoa, Guam, and the United States Virgin Islands; and
- (5) The minor outlying islands of Baker Island, Howland Island, Jarvis Island, Johnston Atoll, Kingman Reef, Midway Islands, Navassa Island, Palmyra Atoll, and Wake Atoll.

(b) *Authority.* This clause implements Executive Order 14042, Ensuring Adequate COVID Safety Protocols for Federal Contractors, dated September 9, 2021 (published in the Federal Register on September 14, 2021, 86 FR 50985)

(c) *Compliance.* The Contractor shall comply with all guidance, including guidance conveyed through Frequently Asked Questions, as amended during the performance of this contract, for contractor or subcontractor workplace locations published by the Safer Federal Workforce Task Force (Task Force Guidance) at <https://www.saferfederalworkforce.gov/contractors/>.

(d) *Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (d), in subcontracts at any tier that exceed the simplified acquisition threshold, as defined in Federal Acquisition Regulation 2.101 on the date of subcontract award, and are for services, including construction, performed in whole or in part within the United States or its outlying areas.

(End of clause)

NOTE: “For existing DOJ contracts or contract-like instruments (hereinafter “contracts”) that contain a clause implementing requirements of EO 14042, the Department will take no action to enforce the clause implementing requirements of EO 14042, absent further written notice from the agency, where the place of performance identified in the contract is in a U.S. state or outlying area subject to a court order prohibiting the application of requirements pursuant to the EO (hereinafter, “Excluded State or Outlying Area”). In all other circumstances, the Department will enforce the clause, except for contractor employees who perform substantial work on or in connection with a covered contract in an Excluded State or Outlying Area, or in a covered contractor workplace located in an Excluded State or Outlying Area. A current list of such Excluded States and Outlying Areas is maintained at <https://www.saferfederalworkforce.gov/contractors/>.”

☐ DEA-2852.204-70 PERSONNEL SECURITY REQUIREMENTS FOR CONTRACTOR EMPLOYEES REQUIREMENTS (NOV 2021)

Work performed under this contract will involve any one or more of the following: access to DOJ Information, which may include Controlled Unclassified Information (CUI), i.e., unclassified, sensitive DOJ information, and/or access to DOJ Information Technology (IT) systems, and/or unescorted access to DOJ space or facilities. Contractor employees will occupy Public Trust Positions, unless clause alternates are applied.

☐ (Check if applicable) Access to/safeguarding of classified information will be required. ALTERNATE I sections also apply.

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

1. GENERAL REQUIREMENTS

(a) (1) All references to “contract(or) personnel” and “contract(or) employee” in this clause means all individuals, without limitation, to include individuals employed by the contractor, team member, subcontractor, consultant, and/or independent contractor, who will have access to information of the Department of Justice (DOJ) or information that is within the custody and control of the DOJ, access to DOJ IT systems, and/or unescorted access to DOJ facilities/space in connection with the performance of this contract. “Employment” as used herein does not create nor imply an employer/employee relationship between the DOJ and contractor employees.

(ALTERNATE I) [The following is added to the clause]: (2) Additionally, work performed under this contract will involve access to classified information [National Security Information (NSI)].

(b) (1) The type of security investigation required for each contractor employee will be governed by the type and risk level of information made available to the contractor employee. The contractor will not be permitted to commence performance under this contract until a sufficient number of its personnel, as determined by the Security Programs Manager (SPM), in consultation with the Contracting Officer’s Representative if one is appointed, have received the requisite security approval.

(ALTERNATE I) [The following is added to the Clause]: (2) All contractor employees requiring access to classified information will be processed by Defense Counterintelligence and Security Agency (DCSA) in accordance with the National Industrial Security Program (NISP). The contractor will not be permitted to commence performance under this contract until a sufficient number of its personnel, as determined by the SPM in consultation with the Contracting Officer’s Representative (COR) if one is appointed, have received the requisite NSI Clearance.

(c) Except where specifically noted otherwise, the federal government will be responsible for the cost and conduct of the investigation.

(d) The contractor shall ensure that no contractor employee commences performance prior to receipt of a written authorization from the contracting officer, COR, or the SPM that performance by the respective contractor employee is authorized.

(e) The data and other information to which the contractor may have access as a result of this contract is the property of, and/or within the custody and control of, the Department, and its disclosure to third parties is governed by various statutes and regulations, the violation of which may subject the discloser to criminal penalties.

2. CITIZENSHIP AND RESIDENCY REQUIREMENTS

(a) *Residency Requirement.* (1) Contractor employees in Public Trust positions, both U.S. citizens and non-U.S. citizens, must meet the Department’s residency requirement if they will require access to DOJ information, IT systems, or unescorted access to facilities. For three years (not necessarily consecutive years) out of the last five years immediately prior to employment under the Department contract the contractor employee must have: (i) resided in the U.S.; (ii) worked for the U.S. in a foreign country as either an employee or contractor in a federal civilian or military capacity; or, (iii) been a dependent of a federal civilian or military employee or contractor working for the U.S. in a foreign country. At the Department’s sole discretion, the residency requirement may be waived by the Department Security Officer (DSO) for contractor employees on a case-by-case basis where justified by extenuating circumstances. The residency requirement does not apply to contractor employees residing in foreign countries that are hired to work in American embassies/consulates/missions located outside of the United States and who require access to DOJ information, IT systems, or unescorted access *provided that* an adequate background investigation can be conducted, with favorable adjudication, as determined by the DSO.

(ALTERNATE I) [The following is added to the clause]: (2) The residency requirement does not apply to contractor employees working on the classified portion of this contract whose national security clearance has been processed by DCSA in accordance with the NISP.

(b) *Citizenship.* (1) Aside from the specific exceptions set forth in Section 1.2(b)(2), for Public Trust positions, the DOJ requires that contractor employees be U.S. citizens and nationals, or lawful permanent residents seeking U.S. citizenship. Any prospective non-U.S. citizen contractor employee who requires access to DOJ information systems, DOJ information, and/or unescorted facilities access must also have been granted a waiver as described below in paragraphs 1.2(d) and/or (e). The contractor is responsible for verifying that the non-U.S. citizens working under this contract are lawful permanent residents seeking U.S. citizenship.

(2) *Exception for Certain Non-U.S. Citizen Contractor Employees:* (i) Non-U.S. citizen expert witnesses, litigative consultants, and interpreters in rare foreign languages are not required to be lawful permanent residents seeking U.S. citizenship. However, they must be granted a waiver for access to unclassified DOJ information, whether CUI or not, DOJ IT systems, and/or unescorted facility access, as described below in paragraph 1.2(d) and (e), regardless of the duration of their duties. (ii) Non-U.S. Citizen contractor employees residing in foreign countries who are hired to work for the Department of Justice in American embassies/consulates/missions outside of the United States are not required to be lawful permanent residents seeking U.S. citizenship.

(ALTERNATE I) [The following is added to the clause]: (3) Contractor employees requiring access to classified information will be processed by DCSA in accordance with the NISP.

(c) *Dual Citizenship.* (1) U.S. citizens who hold dual citizenship with a foreign country are considered U.S. citizens within the meaning of this clause, and may be considered for, but are not entitled to, contract employment as U.S. citizens consistent with this clause. The means by which the contractor employee obtained or exercises his or her dual citizenship status will be a consideration in the Public Trust Investigation (PTI) adjudication, and/or waiver approval processes discussed in this clause.

(ALTERNATE I) [The following is added to the clause]: (2) Contractor employees requiring access to classified information will be processed by DCSA in accordance with the NISP.

(d) *Access to DOJ Information Technology Systems.* Non-U.S. citizens are not authorized to access DOJ information technology (IT) systems or assist in the development, operation, management, or maintenance of DOJ IT systems, including providing IT system support, unless a waiver has been granted by the Head of the DOJ component or designee, with the prior concurrence of both the DSO and the DOJ Chief Information Officer, allowing computer access by the non-U.S. citizen. Such a waiver will be granted only in exceptional and unique circumstances on a case-by-case basis. It should be noted that the Justice Consolidated Office Network (JCON) is a sensitive DOJ IT system and any contractor employee who will need access to JCON must be a U.S. citizen or have received a waiver. In order for a waiver to be considered for approval: (1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; (2) The type of personnel security vetting that has been conducted on the individual, and vetting results, that would mitigate risk; and (3) The waiver must be in the best interest of the federal government.

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

(e) *Access to Unclassified DOJ Information and Unescorted Access to DOJ Facilities or Space.* (1) Except as provided under 1.2(b)(2), non-U.S. citizens are not authorized to access DOJ information and/or unescorted access to DOJ facilities or space, unless a waiver has been granted by the DSO, allowing access by the non-U.S. citizen. Such a waiver will be granted on a case-by-case basis where justified at the discretion of the DSO.

3. BACKGROUND INVESTIGATION REQUIREMENTS

(a) (1) Unless otherwise stated below, all contractor personnel are subject to a Public Trust Investigation (PTI). The SPM will determine the type of investigation for each contractor employee based on the risk category (i.e., the nature of the position and degree of harm that could be caused by the individual in that position) and whether the position is long-term or short-term. The PTI risk categories are listed below.

- (i) High Risk Positions. The minimum background investigation required is a Tier 4 (T4) investigation, and the five-year reinvestigation required is a Tier 4R (T4R) investigation. The 2017 version of the Standard Form (SF) 85P, Questionnaire for Public Trust Positions, is required.
- (ii) Moderate Risk Positions. The minimum background investigation required is a Tier 2 (T2) investigation. The five-year reinvestigation required is a Tier 2R (T2R) investigation. The 2017 version of the SF-85P is required.
- (iii) Low Risk/Non-Sensitive Positions. The minimum background investigation required for Low Risk/Non-Sensitive positions is a Tier 1 (T1) investigation and the required five-year reinvestigation is also a Tier 1 (T1) investigation. The SF 85, Questionnaire for Non-Sensitive Positions, is required.

(ALTERNATE I) [The following is added to the clause]: (2). *Contractor employees requiring access to classified information will be processed by DCSA in accordance with the NISP.*

(b) *Exception for Expert Witnesses.* Expert Witnesses, litigative consultants, and interpreters in rare foreign languages may not be subject to full background investigation requirements if alternative security requirements are approved by the DSO.

(c) *Short-Term U.S. Citizen Contractor Employees.* Other than the exception in Section 1.3(b), short-term contractor employees (6 months or less) who are U.S. citizens are not subject to a full background investigation, however, must receive an approved pre-employment background investigation waiver. The required forms to complete and submit are listed in Section 1.4(b) and (c)(2).

(d) *Long-Term U.S. Citizen Contractor Employees.* Other than the exception in Section 1.3(b), all long-term U.S. citizen employees (longer than 6 months) are subject to a full background investigation in the risk category appropriate to the position they will hold.

(e) *Non-U.S. Citizen Contractor Employees.* Other than the exception in 1.3(b), all non-U.S. citizen contractor employees regardless of performance duration (short or long term) are subject to a full background investigation in the risk category appropriate to the position they will hold.

(f) *Reciprocity.* (1) A Public Trust Investigation will be accepted under reciprocity if it meets the following guidelines: (i) the investigation is current (investigations are considered current if completed within the last five years) and favorably adjudicated, or the reinvestigation has been deferred; (ii) the investigation meets or exceeds the level of investigation required for the DOJ contractual instrument; (iii) there has been no continuous (not cumulative) break in federal contract/service employment of two years or more; (iv) there is no derogatory information since the favorable fitness determination or adjudication that calls into question the individual's fitness based on character or conduct; and (v) the investigative record does not show conduct that is incompatible with the core duties of the new contract position. A "core duty" is a continuing responsibility that is of particular importance to the relevant covered position or the achievement of an agency's mission. Core duties will vary from position to position.

(ALTERNATE I) [The following is added to the clause]: (g) *National security investigations will be accepted from other federal agencies under reciprocity guidelines provided all of the following are true: (i) The new position does not require a higher eligibility than what the subject currently possesses; (ii) the existing eligibility is not granted on an interim or temporary basis, or limited or one-time basis; (iii) the covered individual's eligibility is not currently denied, revoked, or suspended; (iv) the favorable adjudication was based on the 13 Adjudicative Guidelines (SEAD 4) and E.O. 12968. Agencies may accept eligibility recorded with an exception based on their own risk assessment; (v) the most recent background investigation is not more than seven years old; (vi) there is no new derogatory information of national security adjudicative relevance that has been reported/developed since last investigation; (vii) the Bond Amendment disqualifier (SEAD 4) does not apply and individual requires SCI, SAP, or restricted access; and (viii) the subject does not have a break in federal service of 24 months or longer.*

4. BACKGROUND INVESTIGATION PROCESS

(a) *e-QIP (or its successor).* Public Trust background investigations/reinvestigations of contractor employees will be performed by the DCSA. The investigative process requires contractor employees to complete the Electronic Questionnaires for Investigations Processing (e-QIP) and provide additional information as specified in paragraph 1.4(b) below. Immediately after contract award, the contractor shall designate an employee as its "e-QIP Initiator" and provide the name of this person to the SPM. The e-QIP Initiator must have, at a minimum, a favorably adjudicated Tier 1 investigation and the appropriate DOJ security approval before being given access to e-QIP. After the e-QIP Initiator's security approval is granted, the Contractor will be configured in e-QIP as a sub-agency to DOJ. The contractor will then be responsible for initiating investigations for all contract personnel, whose previous investigation does not meet reciprocity, in e-QIP for completion of the security questionnaire form and forwarding the electronic form with the remainder of the security package to the SPM. Subject to the prior written approval of the SPM, the contractor may designate an e-QIP Initiator for each subcontractor. Subcontractor e-QIP Initiators must have, at a minimum, a favorably adjudicated Tier 1 investigation and the appropriate DOJ security approval before being provided access to e-QIP.

(b) *Additional Documentation.* (1) In addition to completing the e-QIP questionnaire (see 1.4(a), above), the contractor shall ensure that each contractor employee occupying Public Trust Positions, including short-term employees, completes and submits the following information through the contractor's Corporate Security Officer:

- (i) Digital Fingerprinting/FD-258 Applicant Fingerprint Card. Two sets are required per applicant. The contractor may schedule appointments with the SPM to be digitally fingerprinted; otherwise, fingerprinting by the FBI or other law enforcement entity, as approved by the SPM, is required to ensure the identity of the person being fingerprinted and for printing quality. All pertinent information must be completed by the individual taking the fingerprints (FBI or other). Use of the physical FD-258 Applicant Fingerprint Card should only be used in extenuating circumstances.
- (ii) DOJ-555 Fair Credit Reporting Act Disclosure. Authorizes DOJ to obtain one or more consumer/credit reports on the individual. This form will be required if the Component SPM determines a credit check is necessary for its Low Risk Level 1 contractor positions.

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

- (iii) OF-306, Declaration for Federal Employment.
- (iv) Foreign National Relatives or Associates Statement. This is only required if foreign national relatives or associates were not disclosed on the security questionnaire form.
- (v) Self-Reporting Requirements for All Contractor Personnel. This is an acknowledgement and acceptance statement that every contractor must sign.
- (vi) Additional information as may be required based on the review of the security questionnaire form.

The contractor shall review all forms/documents to ensure each is complete, accurate and meets all DOJ requirements, including applicable residency and citizenship requirements. The contractor shall resolve any issues or discrepancies with the contractor employee, including resubmission of corrected forms or documentation. Completed forms/documents shall be submitted to the SPM (or designee, which may include the COR) within five (5) calendar days after being finalized.

(c) *Adjudication and Pre-Employment Background Investigation Waivers*

(1) Except as set forth in this section, background investigations must be conducted and favorably adjudicated for each contractor employee prior to commencing their work on this contract. Where programmatic needs do not permit the federal government to wait for completion of the entire background investigation, a pre-employment background investigation waiver for public trust contractors can be granted by the SPM, in consultation with the cognizant COR. Pre-employment waivers cannot be used to circumvent delays in clearing classified contractors through the DCSA, if access to classified information is required.

(2) As directed by the SPM, the contractor shall initiate pre-employment waivers for Public Trust Positions when necessary. This may entail performing credit history checks and submission of these checks as part of the security package, including satisfactory resolution of any issues prior to submission to the federal government. A waiver will be disapproved if it develops derogatory information that cannot be resolved in the contractor employee's favor. When a waiver has been disapproved, the CO, in consultation with the SPM and COR, will determine (i) whether the contractor employee will no longer be considered for work on a DOJ contract or (ii) whether to wait for the completion and favorable adjudication of the background investigation before the contractor employee commences work on a Department contract. The pre-employment background investigation waiver requirements include:

1. Verification of citizenship (copy of a birth certificate, naturalization certificate, or U.S. passport);
2. Verification of compliance with the *DOJ Residency Requirement* of this Clause;
3. Favorable review of the security questionnaire form;
4. Favorable FBI fingerprint results;
5. Favorable credit report;
6. Favorable review of the OF-306 form, Declaration for Federal Employment;
7. Verification of the initiation of the appropriate background investigation (for long-term personnel); and
8. Receipt of the signed DOJ Self-Reporting Requirements for All Contractor Personnel (see Section 1.6, below).

(3) The investigating agency (DCSA) will provide the SPM with the results of each proposed contractor employee's Public Trust investigation. Upon receipt of the investigation and any other pertinent documents from the investigating agency, the SPM will determine whether each proposed contractor employee should be granted employment security approval.

(4) The COR will notify the contractor of the results of Public Trust background investigations as they are completed and adjudicated, including any individual who is found ineligible for employment security approval. For any individual found ineligible for employment on a Department contract, the contractor shall propose a replacement and initiate the background investigation process consistent with this clause.

(ALTERNATE I) *[The following is added to the clause]:*

(5) (1) For classified contracts, the contractor shall possess or be capable of obtaining a Department of Defense Central Adjudication Facility (DODCAF) Defense Industrial Security Clearance Facility Cage Code and the security clearance required to fully perform this contract. As directed by the COR or SPM, the contractor shall submit the information necessary to allow the Government to prepare and obtain for the Contractor a "Department of Defense Contract Security Classification Specification" (DD Form 254) for this contract. Where such clearance is required, the contractor agrees to provide information and access to contractor facilities as may be required by federal government investigators.

(2) Immediately after contract award (or post-award receipt of the required Facility Clearance), the contractor's Facility Security Officer (FSO) shall furnish to the COR a list of all personnel proposed to work under this contract who have been processed in accordance with the NISP by the DCSA. The contractor shall update this information as individuals are added or separated from the contract and the FSO shall provide the updated list to the COR.

(3) For each contractor employee who requires access to classified information under this contract, the contractor shall forward a Visit Authorization Request (VAR) indicating the current background investigation information and clearance level to the COR.

5. IDENTITY PROOFING AND BADGING

(a) Access to DOJ Information, federally-controlled IT systems, and/or unescorted access to federally-controlled facilities or space (regardless of whether the contractor employee will be issued a DOJ PIV card or building access badge) shall be made available after each respective contractor employee has (1) met the identity proofing requirements outlined below, and (2) completed all other security requirements stated elsewhere in this contract.

(b) (1) Public Trust contractor employees must appear in person at least once before a DOJ official or an official of a trusted contract company (i.e., has a facility security clearance) who is responsible for checking two forms of identification in original form prior to commencement of work by the contractor employee and PIV card or building access badge issuance (as applicable). Approval will be documented by the DOJ official or an official of a trusted contract company. (Acceptable documents are listed in Form I 9, Employment Eligibility Verification, and at least one document must be a valid state or federal government issued picture ID).

(c) **(ALTERNATE I)** *[The following is added to the clause]:* (2) All contractor employees requiring access to classified information must appear in person at least once before an official of the contractor possessing the facility clearance, who is responsible for checking the identification documents. (Acceptable documents are listed in Form I 9, Employment Eligibility Verification, and at least one document must be a valid state or federal government issued picture ID).

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

This identity proofing must be completed prior to commencement of work by the contractor employee under this contract and badge issuance (as applicable) and must be documented by the contractor official.

(d) All contractor employees requiring unescorted access to a DOJ controlled facility or space shall comply with the PIV card or building access badge requirements outlined below:

- (i) When any contractor employee enters a DOJ building for the first time, he/she shall allow one hour for security processing and the creation and issuance of a building access badge. PIV cards require additional processing time and will not likely be issued on the same day.
- (ii) Building access badges shall be subject to periodic review by the contractor employee's supervisor and checked against his/her personal identification. The contractor employees shall present themselves for the issuance of renewed badges when required by the government as scheduled by the COR or his/her designee. The contractor shall notify the COR when contractor employee badges are lost, and must immediately apply for reissuance of a replacement badge. The contractor shall pay for reissued building access badges at no cost to the government. It is the contractor employee's responsibility to return badges to the COR or his/her designee when a contractor employee is dismissed, terminated or assigned to duties not within the scope of this contract.

6. EMPLOYEE REPORTING REQUIREMENTS

(a) All contractor employees must sign the DOJ *Self-Reporting Requirements for All Contractor Personnel* statement acknowledging and accepting the DOJ requirement that they immediately self-report certain information using the Department's iReport system. The COR or SPM will provide the Self-Reporting statement as well as a list of reportable information, which varies by position sensitivity designation, to the contractor employee before commencing work under the contract. If the contractor employee does not have access to the DOJ iReport System, the COR or SPM will provide a fillable form for the contractor employee to complete and submit.

(b) The COR and SPM will review the written report and documentation and make a determination regarding continued employment on a DOJ contract.

(c) DOJ reporting requirements are in addition to the DCSA reporting requirements and the contractor's internal reporting requirements.

7. REPLACEMENT PERSONNEL

(a) The contractor shall make every effort to avoid costs to the government for security investigations for replacement of contractor employees, and in so doing shall ensure that otherwise satisfactorily performing and physically able contractor employees remain in contract performance for the duration of the contract. The contractor shall take all necessary steps to ensure that contractor personnel who are selected for assignment to this contract are professionally qualified and personally reliable, of reputable background and sound character, and able to meet all other requirements stipulated in the contract.

The fact that the government performs security investigations shall not in any manner relieve the contractor of its responsibility to ensure that all contract personnel are reliable and of reputable background and sound character. Should a security investigation conducted by the government and/or a contractor's self-report or failure to self-report render ineligible a contractor employee, the contracting officer will determine whether the contractor has violated this clause. The contracting officer may direct the contractor, at its own expense, to remove and replace any contractor personnel who fails to comply with or violates applicable requirements of this contract. Such action may be taken at the government's direction without prejudice to its rights under any other provision of this contract, including termination for default, and the contractor may be held liable, at a minimum, for all reasonable and necessary costs incurred by the government to (i) provide coverage (performance) through assignment of individuals employed by the government or third parties in those cases where absence of contractor personnel would cause either a security threat or DOJ program disruption and (ii) conduct security investigations in excess of those which would otherwise be required.

(b) Nothing in this clause shall require the contractor to bear costs involved in the conduct of security investigations for replacement of a contractor employee who separates from the contractor of his/her own accord, is incapacitated, or is deceased.

(c) The contractor shall comply with the terms and conditions set forth under this clause and assumes all liability for failure to comply. The rights and remedies conferred upon the government by this clause are in addition to all and other rights and remedies pursuant to the contract and as established by law.

(End of Clause)

☐ **DEA-2852.224-70 CONTRACTOR PRIVACY REQUIREMENTS (SEP 2022)**

A. Limiting Access to Privacy Act and Other Sensitive Information

1. *Privacy Act Information.* In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984) and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires Contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DOJ system of records notices (SORNs) applicable to this Privacy Act information may be found at <https://www.justice.gov/opcl/doj-systems-records>.¹ Applicable SORNs published by other agencies may be accessed through those agencies' websites or by searching the Federal Digital System (FDsys) available at <http://www.gpo.gov/fdsys/>. SORNs may be updated at any time.

2. *Prohibition on Performing Work Outside a Government Facility/Network/Equipment.* Except where use of Contractor networks, IT, other equipment, or Workplace as a Service (WaaS) is specifically authorized within this contract, the Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or WaaS and Government information shall remain within the confines of authorized Government networks at all times. Any handling of Government information on Contractor networks or IT must be approved by the Senior Component Official for Privacy of the component

¹ "[T]he term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." 5 U.S.C. § 552a(a)(4). "[T]he term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5).

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

entering into this contract. Except where remote work is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of remote work authorizations.

3. *Prior Approval Required to Hire Subcontractors.* The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

4. *Separation Checklist for Contractor Employees.*

(a) The Contractor shall complete and submit an appropriate separation checklist to the Contracting Officer before any employee or Subcontractor employee terminates working on the contract. The Contractor must submit the separation checklist on or before the last day of employment or work on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposition of personally identifiable information (PII)², in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to PII or other sensitive information.

(b) In the event of adverse job actions resulting in the dismissal of a Contractor or Subcontractor employee before the separation checklist can be completed, the Prime Contractor must notify the Contracting Officer within 24 hours and confirm receipt of the notification. In the case the Contractor is unable to notify the Contracting Officer, then the Contractor should notify the Contract Officer's Representative (COR).

(c) Contractors must complete the separation checklist with the Contracting Officer or COR by returning all Government-furnished property including, but not limited to, computer equipment, media, credentials and passports, smart cards, mobile devices, Personal Identity Verification (PIV) cards, calling cards, and keys and terminating access to all user accounts and systems. Unless the Contracting Officer requests otherwise, the relevant Program Manager or other Key Personnel designated by the Contracting Officer or COR may facilitate the return of equipment.

B. Privacy Training, Safeguarding, and Remediation

1. *Required Security and Privacy Training for Contractors.* The Contractor must ensure that all employees take appropriate privacy training, including Subcontractors who have access to PII as well as the creation, use, dissemination and/or destruction of PII at the outset of the employee's work on the contract and every year thereafter. Training must include procedures on how to properly handle PII, including heightened security requirements for the transporting or transmission of sensitive PII, and reporting requirements for a suspected breach or loss of PII. These courses, along with more information about DOJ security and training requirements for Contractors, are available at <https://www.justice.gov/jmd/learndojo>. The [Federal Information Security Modernization Act of 2014 \(FISMA\)](#) requires all individuals accessing DOJ information to complete training on records management, cybersecurity awareness, and information system privacy awareness. Contractor employees are required to sign the "Privacy Rules of Behavior," acknowledging and agreeing to abide by privacy law, policy, and certain privacy safeguards, prior to accessing DOJ information. These Rules of Behavior are made available to all new users of DOJ's computer network and to trainees at the conclusion of DOJ-OPCL-CS-0005. **The Contractor should maintain copies of certificates as a record of compliance and must submit an email notification annually to the COR verifying that all employees working under this contract have completed the required privacy and cybersecurity training.**

2. *Safeguarding PII Requirements.* Contractor employees must comply with DOJ Order 0904 and other guidance published to the publicly-available Office of Privacy and Civil Liberties (OPCL) Resources page³ relating to the safeguarding of PII, including the use of additional controls to safeguard sensitive PII (e.g., the encryption of sensitive PII). This requirement flows down from the Prime Contractor to all Subcontractors and lower tiered subcontracts.

3. *Non-Disclosure Agreement Requirement.* Prior to commencing work, all Contractor personnel that may have access to PII or other sensitive information shall be required to sign a Non-Disclosure Agreement (NDA) and the DOJ IT Rules of Behavior. The Non-Disclosure Agreement:

(a) prohibits the Contractor from retaining or divulging any PII or other sensitive information, or derivatives thereof, furnished by the Government or to which they may otherwise come in contact as a result of their performance of work under the contract/task order that is otherwise not publicly available, whether or not such information has been reduced to writing; and

(b) requires the Contractor to report any loss of control, compromise, unauthorized disclosure, or unauthorized acquisition of PII or other sensitive information to the component-level or headquarters Security Operations Center within one (1) hour of discovery.

The Contractor should maintain signed copies of the NDA for all employees as a record of compliance. The Contractor should also provide copies of each employee's signed NDA to the Contracting Officer before the employee may commence work under the contract/task order.

4. *Prohibition on Use of PII in Vendor Billing and Administrative Records.* The Contractor's invoicing, billing, and other financial or administrative records or

² As stated in FAR 52.224-3 and Office of Management and Budget (OMB) Circular A-130, Managing Federal Information as a Strategic Resource (2016), "personally identifiable information" means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Regarding "sensitive PII," "[t]he sensitivity level of the PII will depend on the context, including the purpose for which the PII is created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed. For example, the sensitivity level of a list of individuals' names may depend on the source of the information, the other information associated with the list, the intended use of the information, the ways in which the information will be processed and shared, and the ability to access the information." OMB Circular A-130, at App. II-2.

³ The DOJ OPCL Resources page is available at <https://www.justice.gov/opcl/resources>.

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

databases is not authorized to regularly store or include any sensitive PII or other confidential government information that is created, obtained, or provided during the performance of the contract without the written permission of the Senior Component Official for Privacy (SCOP). It is acceptable to list the names, titles and contact information for the Contracting Officer, COR, or other personnel associated with the administration of the contract in the invoices as needed.

5. *Reporting Actual or Suspected Data Breach.* Contractors must report any actual or suspected breach of PII within one hour of discovery.⁴ A “breach” is an incident or occurrence that involves the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. The report of a breach must be made to DOJ. The Contractor must cooperate with DOJ’s inquiry into the incident and efforts to minimize risks to DOJ or individuals, including remediating any harm to potential victims.

(a) The Contractor must develop and maintain an internal process by which its employees and Subcontractors are trained to identify and report the breach, consistent with DOJ Instruction 0900.00.01⁵, Reporting and Response Procedures for a Breach of Personally Identifiable Information.

(b) The Contractor must report any such breach by its employees or Subcontractors to the DOJ Security Operations Center (dojcert@usdoj.gov, 202-357-7000); Component-level Security Operations Center and Component-level Management Team, where appropriate; the COR; and the Contracting Officer within one (1) hour of the initial discovery.

(c) The Contractor must provide a written report to the DOJ Security Operations Center (dojcert@usdoj.gov, 202-357-7000) within 24 hours of discovery of the breach by its employees or Subcontractors. The report must contain the following information:

- (i) Narrative or detailed description of the events surrounding the suspected loss or compromise of information.⁶ Date, time, and location of the incident.
- (ii) Amount, type, and sensitivity of information that may have been lost or compromised, accessed without authorization, etc.
- (iii) Contractor’s assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.⁷
- (iv) Names and classification of person(s) involved, including victim, Contractor employee/Subcontractor and any witnesses.
- (v) Cause of the incident and whether the company’s security plan was followed and, if not, which specific provisions were not followed.⁸
- (vi) Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
- (vii) Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

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

(e) At the Government’s discretion, Contractor employees or Subcontractor employees may be identified as no longer eligible to access PII or to work on that contract based on their actions related to the loss or compromise of PII.

6. *Victim Remediation.* At DOJ’s request, the Contractor is responsible for notifying victims and providing victim remediation services in the event of a breach of PII held by the Contractor, its agents, or its Subcontractors, under this contract. Victim remediation services shall include at least 18 months of credit monitoring and, for serious or large incidents as determined by the Government, call center help desk services for the individuals whose PII was lost or compromised. When DOJ requests notification, the Department Chief Privacy and Civil Liberties Officer and SCOP will direct the Contractor on the method and content of such notification to be sent to individuals whose PII was breached. By performing this work, the Contractor agrees to full cooperation in the event of a breach. The Contractor should be self-insured to the extent necessary to handle any reasonably foreseeable breach, with another source of income, to fully cover the costs of breach response, including but not limited to victim remediation.

C. Government Records Training, Ownership, and Management

1. *Records Management Training and Compliance.*

(a) The Contractor must ensure that all employees and Subcontractors that have access to PII as well as to those involved in the creation, use, dissemination and/or destruction of PII take the [DOJ Records and Information Training for New Employees \(RIM\)](#) training course or another training approved by the Contracting Officer or COR. This training will be provided at the outset of the Subcontractor’s/employee’s work on the contract and every year thereafter. The Contractor shall maintain copies of certificates as a record of compliance and must submit an email notification annually to the COR verifying that all employees working under this contract have completed the required records management training.

⁴ As stated in DOJ Instruction 0900, “Contractors must notify the Contracting Officer, the Contracting Officer’s Representative, and JSOC (or component-level SOC) within 1 hour of discovering any incidents, including breaches, consistent with this Instruction, guidance issued by the CPCLO, NIST standards and guidelines, and the US-CERT notification guidelines.”

⁵ <https://www.justice.gov/file/4336/download>

⁶ As stated in DOJ Instruction 0900, the description should include the type of information that constitutes PII; purpose for which PII is collected, maintained, and used; extent to which PII identifies a peculiarly vulnerable population; the determination of whether the information was properly encrypted or rendered partially or completely inaccessible by other means; format of PII (e.g., whether PII was structured or unstructured); length of time PII was exposed; any evidence confirming that PII is being misused or that it was never accessed.

⁷ As stated in DOJ Instruction 0900, the report should include the nature of the cyber threat (e.g., Advanced Persistent Threat, Zero Day Threat, data exfiltration) for cyber incidents.

⁸ As stated in DOJ Instruction 0900, the report should include analysis on whether the data is accessible, usable, and intentionally targeted.

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

(b) The Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records containing PII and those covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format, mode of transmission, or state of completion.

2. *Records Creation, Ownership, and Disposition.*

(a) The Contractor shall not create or maintain any records not specifically tied to or authorized by the contract using Government IT equipment and/or Government records or that contain Government Agency information. The Contractor shall certify, in writing, the appropriate disposition or return of all Government information at the conclusion of the contract or at a time otherwise specified in the contract. In accordance with 36 CFR 1222.32, the Contractor shall maintain and manage all Federal records created in the course of performing the contract in accordance with Federal law. Records may not be removed from the legal custody of DOJ or destroyed except in accordance with the provisions of the agency records schedules.

(b) Except as stated in the Performance Work Statement and, where applicable, the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and may be considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

(c) The Contractor shall not retain, use, sell, disseminate, or dispose of any government data/records or deliverables without the express written permission of the Contracting Officer or Contracting Officer's Representative. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. § 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the Agency records schedules.

D. Data Privacy and Oversight

1. *Restrictions on Testing or Training Using Real Data Containing PII*

The use of real data containing PII from any source for testing or training purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for testing or training whenever feasible.

2. *Requirements for Contractor IT Systems Hosting Government Data*

The Contractor is required to obtain an Authority To Operate (ATO) for any IT environment owned or controlled by the Contractor or any Subcontractor on which Government data shall reside for the purposes of IT system development, design, data migration, testing, training, maintenance, use, or disposal.

3. *Requirement to Support Privacy Compliance*

(a) If this contract requires the development, maintenance or administration of information technology⁹, the Contractor shall support the completion of the Initial Privacy Assessment (IPA) document, if requested by Department personnel. An IPA is the first step in a process to identify potential privacy issues and mitigate privacy risks. The IPA asks basic questions to help components assess whether additional privacy protections may be needed in designing or implementing a project¹⁰ to mitigate privacy risks, and whether compliance work may be needed. Upon review of the IPA, the OPCL determines whether a Privacy Impact Assessment (PIA) document and/or SORN, or modifications thereto, are required. The Contractor shall provide adequate support to complete the applicable risk assessment and PIA document in a timely manner, and shall ensure that project management plans and schedules include the IPA, PIA, and SORN (to the extent required) as milestones. Additional information on the privacy compliance process at DOJ, including IPAs, PIAs, and SORNs, is located on the DOJ OPCL website (<https://dojnet.doi.gov/privacy/>), including DOJ Order 0601, Privacy and Civil Liberties. The Privacy Impact Assessment Guidance and Template outline the requirements and format for the PIA.

(b) If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy risk assessment and documentation, the Contractor shall provide adequate support to DOJ to ensure DOJ can complete any required assessment, and IPA, PIA, SORN, or other supporting documentation to support privacy compliance. The Contractor shall work with personnel from the program office, OPCL, the Office of the Chief Information Officer (OCIO), and the Office of Records Management and Policy to ensure that the privacy assessments and documentation are kept on schedule, that the answers to questions in the documents are thorough and complete, and that questions asked by the OPCL and other offices are answered in a timely fashion. The Contractor must ensure the completion of required PIAs and documentation of privacy controls consistent with federal law and standards, e.g. NIST

⁹ As defined in 40 U.S.C. § 11101, the term "information technology" means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use (i) of that equipment or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract.

¹⁰ In this instance, the term "project" is used to scope the activities (e.g., creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, or disposing of information) covered by an IPA. A project is intended to be technology-neutral, and may include an information system, a digital service, an information technology, a combination thereof, or some other activity that may create potential privacy issues or privacy risks that would benefit from an IPA. The scope of a project covered by an IPA is discretionary, but components should work with their SCOP and OPCL.

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

800-53, Rev. 5; and compliance with the Privacy Act of 1974, E-Government Act of 2002, Federal Information Security Modernization Act of 2014, and key OMB guidelines, e.g., OMB Circular A-130.

(End of Clause)

☐ **DEA-2852.231-70 TRAVEL REQUIREMENTS FOR CONTRACTORS (SEP 2022)**

(a) Contractor personnel may be required to conduct travel in the performance of this contract. All travel must be pre-approved in writing by the Contracting Officer's Representative (COR) or the Task Monitor (TM). Any expenses incurred by Contractor personnel without prior Government approval will be denied for payment. The Contractor will be reimbursed for travel costs in accordance with Part 31 of Federal Acquisition Regulation (FAR) and the Federal Travel Regulation (FTR).

(b) Travel requirements shall use the most cost effective and efficient means of transportation. All travel should be scheduled in advance in order to take advantage of discounted rates. The Contractor shall engage only the minimum number of travelers and vehicles needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible. Commuting expenses between an employee's residence and duty station are not reimbursable and will be disallowed.

(c) Domestic Travel. Contractors are authorized to use commercial air, commercial rail, rental vehicle, Government vehicle as a passenger, company authorized vehicle, or privately owned vehicle when travel is approved. When a mode other than commercial air is contemplated, the Contractor shall contact the COR to determine the mode of travel most advantageous to the Government. Domestic U.S. travel rates (i.e., per diem, mileage, etc.) can be found on the General Services Administration (GSA) website under the [Travel Resources](#) section.

(d) Overseas Non-Foreign Areas/International Travel.

(1) Maximum rates of per diem allowances and reimbursements for miscellaneous travel expenses for travel in Alaska, Hawaii, Guam, Puerto Rico and territories and possessions of the United States are prescribed by the Department of Travel Management Office (DTMO) located on DTMO's website at (<http://www.defensetravel.dod.mil/site/perdiem.cfm>).

(2) The Contractor shall be responsible for ensuring that all employees scheduled to travel to international locations have a valid passport. DEA will not request or authorize the issuance of a "US Official Government" passport for contractor personnel.

(3) International travel to specific countries and regions may be subject to additional DoS requirements, as well as host nation requirements, such as visas. The Contractor shall be responsible for complying with any applicable DoS and destination national requirements and notifying the COR/ TM of any matters that impact cost, schedule, or performance.

(4) Maximum rates of per diem allowance and reimbursements for miscellaneous travel expenses for travel in foreign areas, including the Trust Territory of the Pacific Islands, are established by the DoS (https://aoprals.state.gov/web920/per_diem.asp).

(e) Limitation of Government Liability for Contracts Performed Outside of the United States. This contract requires performance in whole or in part by contractor employees in one or more locations outside of the United States. By entering into the contract, the contractor assumes certain risks associated with performance including risks of injury to or death of its employees. The Contractor shall be responsible for notification of the employee-designated next of kin in the event of injury or death. The contractor may elect to obtain and maintain private insurance to cover those risks or cover the risks with its own resources. Any mandatory requirement for insurance will be specified in the contract in an appropriate insurance clause as prescribed in [FAR subpart 28.3](#). The Government assumes no liability for any costs associated with performance of the contract not expressly stipulated in the contract. In no event will the Government indemnify the contractor for any third-party liability.

(f) Travel Invoice.

(1) Travel expenses shall not include fees calculated as profit. General and Administrative (G&A) expenses shall be allowable on travel costs, provided that the Contractor's accounting system has been accepted by the Defense Contract Auditing Agency (DCAA). DEA reserves the right to negotiate a ceiling on all travel costs. Travel costs incurred by subcontractors may not be subsequently "marked up" by a prime Contractor's G&A prior to submission to DEA.

(2) The Contractor must submit a travel invoice upon the completion of travel. The travel invoice must be submitted to the COR in accordance with the invoice clause or the timetable specified in the subject contract. The invoice must contain all required documentation, including receipts supporting the travel costs and evidence of DEA pre-authorization to travel. The documentation shall include the following information: traveler's name(s), purpose of travel, destination, Contract Number, Task Order Number (if applicable), Contract Line Item Number (CLIN), name of DEA official authorizing the travel, date of authorization and a breakdown of actual travel costs. If applicable, the travel cost breakdown for per diem shall include: total number of travel days, lodging, miscellaneous and incidental expenses (including tolls, mileage, etc.), differential and allowances, with subtotals by category and a grand total. Vouchers and receipts shall be attached to invoices.

(End of clause)

☐ **DEA-2852.242-82 DOJ REPORTING SYSTEM FOR REPORTABLE PERSONNEL SECURITY RELATED ACTIVITIES (NOV 2021)**

This clause is applicable if the contract or order includes clause [DEA-2852.204-70](#), *Personnel Security Requirements for Contractor Employees*.

The Department of Justice (DOJ) [iReport](#) system is a secure, web-based application used by personnel to report activities as required by section 6 – *Employee Reporting Requirements* of clause [DEA-2852.204-70](#). Use of the [iReport](#) system is mandatory for contractor employees having access to it through Firebird. Employees who do not have access to [iReport](#) must submit reports directly to the cognizant Contracting Officer's Representative and to the DEA Security Program Manager by email to ISR.Correspondence@dea.gov. Additional guidance and instruction on the use of the [iReport](#) system may be viewed at <https://dojnet.doj.gov/jmd/seps/persg/ireport.php>.

(End of clause)

☐ **JAR 2852.201-70 CONTRACTING OFFICER'S REPRESENTATIVE (COR) (NOV 2020)**

(a) [name] of [organization], [address], [telephone number], [email address], is hereby designated to act as Contracting Officer's Representative (COR) under [award number], for the period of (specify the performance period of the contract that the designation covers).

(b) Performance of work under this contract is subject to the technical direction of the COR identified above, or another representative designated in writing by the Contracting Officer. The term "technical direction" includes, without limitation, the following:

DEA PROVISION & CLAUSE MATRIX – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Updated through FAC 2022-05 and 2022-08

- (i) Receiving all deliverables;
- (ii) Inspecting and accepting the supplies or services provided in accordance with the terms and conditions of this contract;
- (iii) Clarifying, directing, or redirecting the contract effort, including shifting work between work areas and locations, filling in details, or otherwise serving to accomplish the contractual statement of work to ensure the work is accomplished satisfactorily;
- (iv) Evaluating performance of the Contractor; and
- (v) Certifying all invoices/vouchers for acceptance of the supplies or services furnished for payment.

(c) The COR does not have the authority to issue direction that:

- (i) Constitutes a change of assignment or work outside the contract specification/work statement/scope of work.
- (ii) Constitutes a change as defined in the clause entitled “Changes” or other similar contract term.
- (iii) Causes, in any manner, an increase or decrease in the contract price or the time required for contract performance;
- (iv) Causes, in any manner, any change in a term, condition, or specification or the work statement/ scope of work of the contract;
- (v) Causes, in any manner, any change or commitment that affects price, quality, quantity, delivery, or other term or condition of the contract or that, in any way, directs the contractor or its subcontractors to operate in conflict with the contract terms and conditions;
- (vi) Interferes with the contractor’s right to perform under the terms and conditions of the contract; (vii) Directs, supervises, or otherwise controls the actions of the Contractor’s employees or a Subcontractor’s employees.

(d) The Contractor shall proceed promptly with performance resulting from the technical direction of the COR. If, in the opinion of the Contractor, any direction by the COR or the designated representative falls outside the authority of (b) above and/or within the limitations of (c) above, the Contractor shall immediately notify the Contracting Officer.

(e) Failure of the Contractor and Contracting Officer to agree that technical direction is within the scope of the contract is a dispute that shall be subject to the “Disputes” clause and/or other similar contract term.

(f) COR authority is not re-delegable.

(End of clause)

☒ **JAR 2852.222-70 DOMESTIC VIOLENCE, SEXUAL ASSAULT, AND STALKING (DEC 2014)**

(a) It is DOJ policy to enhance workplace awareness of and safety for victims of domestic violence, sexual assault, and stalking. This policy is summarized in “DOJ Policy Statement 1200.02, Federal Workforce Responses to Domestic Violence, Sexual Assault, and Stalking,” available in full for public viewing at: <http://www.justice.gov/sites/default/files/ovw/legacy/2013/12/19/federal-workplace-responses-to-domestic-violence-sexual-assault-stalking.pdf>. Vendor agrees, upon contract award, to provide notice of this Policy Statement, including at a minimum the above-listed URL, to all Vendor employees and employees of subcontractors who will be assigned to work on DOJ premises.

(b) Upon contract award, DOJ will provide the Contractor with the name and contact information of the point of contact for victims of domestic violence, sexual assault, and stalking for the component or components where the Contractor will be performing. The Contractor agrees to inform its employees and employees of subcontractors, who will be assigned to work on DOJ premises, with the name and contact information of the point of contact for victims of domestic violence, sexual assault, and stalking.

(End of Clause)

☐ **JAR 2852.223-70 UNSAFE CONDITIONS DUE TO THE PRESENCE OF HAZARDOUS MATERIAL (NOV 2020)**

(a) “Unsafe condition” as used in this clause means the actual or potential exposure of Contractor or Government employees to a hazardous material.

(b) “Hazardous Material” as used in this clause includes any material defined as hazardous under the latest version of Federal Standard No. 313 (including revisions adopted during the term of the contract), any other potentially hazardous material requiring safety controls, or any other material or working condition designated as hazardous by the Contracting Officer’s Representative (COR).

(c) 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.

(d) Prior to commencement of work, Contractors are required to inspect for and report to the Contracting Officer 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.

(e) 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.

(f) 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.

(g) 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)

CONTRACTING OFFICER: List the recommended security clause in the approved DD 254 in the space provided below by clause number, title, and date of clause.

CONTRACTOR: The full text of the clause may be found at <https://www.dea.gov/security-clauses>.