# SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

*NOTE: OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24 AND 30.*

1. REQUISITION NUMBER

PAGE 1 OF 16

2. CONTRACT NUMBER

3. AWARD/EFFECTIVE DATE: 08/11/2026

4. ORDER NUMBER

5. SOLICITATION NUMBER: 15B41126Q00000012

6. SOLICITATION ISSUE DATE: 08/11/2026

**7. FOR SOLICITATION INFORMATION CALL:**

a. NAME: Hans Frei hfrei@bop.gov

b. TELEPHONE NUMBER (*No collect calls*): 309-346-8588 x1055

8. OFFER DUE DATE / LOCAL TIME: 08/21/2026 03:00 CT

9. ISSUED BY CODE 15B411
Federal Bureau of Prisons
FCI Pekin
2600 S. 2ND STREET
Pekin, IL 61554

10. THE ACQUISITION IS
[X] SMALL BUSINESS
[ ] HUBZONE SMALL BUSINESS
[ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS (SDVOSB)
[ ] UNRESTRICTED OR
[ ] WOMEN-OWNED SMALL BUSINESS (WOSB)
[ ] ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB)
[ ] 8(A)
[X] SET ASIDE: 100.00 % FOR
NORTH AMERICAN INDUSTRY CLASSIFICATION STANDARD (NAICS): 311999
SIZE STANDARD: 700 Employees

11. DELIVERY FOR FREE ON BOARD (FOB) DESTINATION UNLESS BLOCK IS MARKED
[ ] SEE SCHEDULE

12. DISCOUNT TERMS

[ ] 13a. THIS CONTRACT IS A RATED ORDER UNDER THE DEFENSE PRIORITIES AND ALLOCATIONS SYSTEM - DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION
[X] REQUEST FOR QUOTE (RFQ)
[ ] INVITATION FOR BID (IFB)
[ ] REQUEST FOR PROPOSAL (RFP)

15. DELIVER TO CODE 15B411
Federal Bureau of Prisons
FCI Pekin
2600 S. 2ND STREET
Pekin, IL 61554

16. ADMINISTERED BY CODE 15B411
Federal Bureau of Prisons
FCI Pekin
2600 S. 2ND STREET
Pekin, IL 61554

17a. CONTRACTOR/ OFFEROR CODE ____ FACILITY CODE ____

TELEPHONE NUMBER

[ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY CODE 15B411
PEK-BusinessOffice-S@bop.gov
Federal Bureau of Prisons
FCI Pekin
2600 S. 2ND STREET
Pekin, IL 61554

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED [ ] SEE ADDENDUM

| 19. ITEM NUMBER | 20. SCHEDULE OF SUPPLIES/SERVICES | 21. QUANTITY | 22. UNIT | 23. UNIT PRICE | 24. AMOUNT |
|---|---|---|---|---|---|
| | **Delivery Date:** 10/30/2026<br>INCLUDE THE FOLLOWING:<br><br>UEI_____<br>TIN_____<br>Phone_____<br>E-Mail_____<br>Firm Fixed Price<br><br>See Continuation Sheet(s)<br>(*Use Reverse and/or Attach Additional Sheets as Necessary*) | | | | |

25. ACCOUNTING AND APPROPRIATION DATA

26. TOTAL AWARD AMOUNT (*For Government Use Only*)

[X] 27a. SOLICITATION INCORPORATES BY REFERENCE (FEDERAL ACQUISITION REGULATION) FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA [X] ARE [ ] ARE NOT ATTACHED

[ ] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

[X] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

[ ] 29. AWARD OF CONTRACT: REFERENCE _____ OFFER DATED _____ . YOUR OFFER ON SOLICITATION (BLOCK 5) INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA (*SIGNATURE OF CONTRACTING OFFICER*)
HANS FREI
Digitally signed by HANS FREI
Date: 2026.08.11 08:57:17 -05'00'

30b. NAME AND TITLE OF SIGNER (*Type or print*)

30c. DATE SIGNED

31b. NAME OF THE CONTRACTING OFFICER (*Type or print*)
Hans P Frei

31c. DATE SIGNED
08/11/2026

| 19. ITEM NUMBER | 20. SCHEDULE OF SUPPLIES/SERVICES | 21. QUANTITY | 22. UNIT | 23. UNIT PRICE | 24. AMOUNT |
|---|---|---|---|---|---|
| | | | | | |

32a. QUANTITY IN COLUMN 21 HAS BEEN

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

| 32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE | 32c. DATE | 32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE |
|---|---|---|
| 32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE | | 32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE<br>32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE |

| 33. SHIP NUMBER | 34. VOUCHER NUMBER | 35. AMOUNT VERIFIED CORRECT FOR | 36. PAYMENT | 37. CHECK NUMBER |
|---|---|---|---|---|
| PARTIAL FINAL | | | ☐ COMPLETE ☐ PARTIAL ☐ FINAL | |
| 38. S/R ACCOUNT NUMBER | 39. S/R VOUCHER NUMBER | 40. PAID BY | | |

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

## Table of Contents


| Section | Description | Page Number |
|---|---|---|
| | Solicitation/Contract Form | 1 |
| 1 | Commodity or Services Schedule | 4 |
| | B.1 Delivery Information | 4 |
| | B.2 Variation in Quantity | 5 |
| 2 | Contract Clauses | 6 |
| | 52.203-17 Contractor Employee Whistleblower Rights (Nov 2023) | 6 |
| | 52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) | 6 |
| | 52.204-13 (DEV) System for Award Management-Maintenance (Oct 2018) (DEVIATION NOV 2025) | 6 |
| | 52.209-6 (DEV) Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, Proposed for Debarment, or Voluntarily Excluded (Jan 2025) (DEVIATION NOV 2025) | 6 |
| | 52.209-10 (DEV) Prohibition on Contracting With Inverted Domestic Corporations (Nov 2015) (DEVIATION NOV 2025) | 6 |
| | 52.212-4 (DEV) Terms and Conditions-Commercial Products and Commercial Services (Nov 2023) (DEVIATION NOV 2025) | 6 |
| | 52.219-6 (DEV) Notice of Total Small Business Set-Aside (Nov 2020) (DEVIATION DEC 2025) | 6 |
| | 52.222-3 (DEV) Convict Labor (June 2003) (DEVIATION DEC 2025) | 6 |
| | 52.222-19 (DEV) Child Labor-Cooperation with Authorities and Remedies (Jan 2025) (DEVIATION MAR 2026) | 6 |
| | 52.222-36 (DEV) Equal Opportunity for Workers with Disabilities (Jun 2020) (DEVIATION DEC 2025) | 7 |
| | 52.222-50 (DEV) Combating Trafficking in Persons (Oct 2025) (DEVIATION DEC 2025) | 7 |
| | 52.222-90 Addressing DEI Discrimination by Federal Contractors (APR 2026) | 7 |
| | 52.225-3 (DEV) Buy American-Free Trade Agreements-Israeli Trade Act (Nov 2023) (DEVIATION DEC 2025) | 7 |
| | 52.226-8 Encouraging Contractor Policies To Ban Text Messaging While Driving (May 2024) | 7 |
| | 52.232-18 Availability of Funds (Apr 1984) | 7 |
| | 52.232-33 Payment by Electronic Funds Transfer-System for Award Management (Oct 2018) | 7 |
| | 52.232-40 Providing Accelerated Payments to Small Business Subcontractors (Mar 2023) | 7 |
| | 52.233-3 (DEV) Protest after Award (Aug 1996) (DEVIATION NOV 2025) | 7 |
| | 52.233-4 (DEV) Applicable Law for Breach of Contract Claim (Oct 2004) (DEVIATION NOV 2025) | 7 |
| | 52.244-6 (DEV) Subcontracts for Commercial Products and Commercial Services (Jan 2025) (DEVIATION APR 2026) | 7 |
| | 52.247-34 F.o.b. Destination (Nov 1991) | 7 |
| | DOJ-02 Contractor Privacy Requirements (JAN 2022) | 8 |
| | DOJ-08 Continuing Contract Performance During a Pandemic Influenza or other National Emergency (OCT 2007) | 13 |
| 3 | List of Attachments | 15 |
| 4 | Solicitation Provisions | 16 |
| | 52.204-7 (DEV) System for Award Management-Registration (Nov 2024) (DEVIATION NOV 2025) | 16 |

**Section 1 - Commodity or Services Schedule**

## SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

| ITEM NO. | SUPPLIES/SERVICES | QUANTITY | UNIT | UNIT PRICE | AMOUNT |
|---|---|---|---|---|---|
| 0001 | Firm Fixed Price<br>*SEE ATTACHED BID SHEETS FOR REQUIRED SUBSISTENCE ITEMS AND QUANTITIES. SUBMIT COMPLETED BID SHEETS WITH RFQ FOR AWARD CONSIDERATION.<br><br>*PLEASE NOTE MANY ITEMS REQUIRE THE BIDDER TO IDENTIFY "SIZE", "TYPE", "BRAND", ETC. OF THE PRODUCT BEING BID. FAILURE TO ADDRESS THESE REQUIREMENTS WILL RESULT IN THE CONTRACTOR BEING CONSIDERED NONRESPONSIVE AND THE LINE ITEM WILL NOT BE CONSIDERED FOR AWARD.<br><br>PSC: 8940<br><br>**Line Period of Performance:** 08/11/2026 - 08/21/2026<br><br>**Delivery Schedule:**<br><br>**Delivery Description:**<br>Delivery Number: 1<br>Delivery Period: 10/19/2026 - 10/30/2026<br>Quantity: 1.000000<br><br>Delivery Address:<br>Federal Bureau of Prisons<br>FCI Pekin<br>2600 S. 2ND STREET<br>Pekin, IL 61554 | 1 | LT | $_____ | $_____ |

B.1 Delivery Information

**DELIVERY ARRANGEMENTS WILL BE MADE WITH THE FOOD WAREHOUSE SUPERVISOR AT: 309-346-8588 x4769.**
Warehouse hours are from 7:00 a.m. to 1:30 p.m. (CST), Monday through Friday (excluding Federal Holidays). Warehouse phone number: 309-346-8588 x4769. A single payment will be made by Electronic Funds Transfer (EFT), in accordance with the Prompt Payment Act upon delivery of all Contract Line Item Numbers (CLINS) or credit card. Award will be based upon best value to the U.S. Government. Best value is determined by evaluating price and past delivery performance. Multiple awards may be made at the discretion of the Government. Some line items may not be awarded.

Delivery time-frame of all items is **October 19, 2026 to October 30, 2026, between the hours of 7:00 a.m. and 1:30 p.m. CST.**

**It is incumbent on vendors to request a delivery extension by contacting the Contracting Officer at hfrei@bop.gov or 309-346-8588 x1055. Extensions may be granted on case by case basis.**

***Any line items not received by the delivery deadline WILL BE CANCELLED unless the Contracting Officer authorizes a delivery extension.***

**A payment will be made for all product received during the specified delivery time frame.**

**All food items bearing manufacturer-assigned date labels, including "Best if Used By/Before", "Sell By", "Use By", and "Freeze By", must have a minimum 6-month date range extending beyond the date in which it is received by the institution. Food items with manufacturer-assigned date labels that are not in compliance with these standards will be rejected upon delivery.**

## B.2 Variation in Quantity

A variation in the quantity of any item called for by this contract will not be accepted unless the variation has been caused by conditions of loading, shipping, or packing, or allowances in manufacturing processes, and then only to the extent, if any, specified below:
The permissible variation shall be limited to:
5 Percent increase
5 Percent decrease
This increase or decrease shall apply to EACH LINE ITEM.

**Section 2 - Contract Clauses**

**A.1 ADDENDUM TO FAR 52.212-4, Terms and Conditions-Commercial Products and Commercial Services (Nov 2023) (DEVIATION NOV 2025)**

The terms and conditions for the following clauses are hereby incorporated into this solicitation and resulting contract as an addendum to FAR clause 52.212-4.

**Clauses By Reference**

| **52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)** | | |
|---|---|---|
| This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): www.acquisition.gov | | |
| Clause | Title | Fill-ins (if applicable) |
| 52.203-17 | Contractor Employee Whistleblower Rights (Nov 2023) | |
| 52.203-19 | Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) | |
| 52.204-13 (DEV) | System for Award Management-Maintenance (Oct 2018) (DEVIATION NOV 2025) | |
| 52.209-6 (DEV) | Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, Proposed for Debarment, or Voluntarily Excluded (Jan 2025) (DEVIATION NOV 2025) | |
| 52.209-10 (DEV) | Prohibition on Contracting With Inverted Domestic Corporations (Nov 2015) (DEVIATION NOV 2025) | |
| 52.212-4 (DEV) | Terms and Conditions-Commercial Products and Commercial Services (Nov 2023) (DEVIATION NOV 2025) | |
| 52.219-6 (DEV) | Notice of Total Small Business Set-Aside (Nov 2020) (DEVIATION DEC 2025) | |
| 52.222-3 (DEV) | Convict Labor (June 2003) (DEVIATION DEC 2025) | |

| Clause | Title | Fill-ins (if applicable) |
|---|---|---|
| 52.222-19 (DEV) | Child Labor-Cooperation with Authorities and Remedies (Jan 2025) (DEVIATION MAR 2026) | |
| 52.222-36 (DEV) | Equal Opportunity for Workers with Disabilities (Jun 2020) (DEVIATION DEC 2025) | |
| 52.222-50 (DEV) | Combating Trafficking in Persons (Oct 2025) (DEVIATION DEC 2025) | |
| 52.222-90 | Addressing DEI Discrimination by Federal Contractors (APR 2026) | |
| 52.225-3 (DEV) | Buy American-Free Trade Agreements-Israeli Trade Act (Nov 2023) (DEVIATION DEC 2025) | |
| 52.226-8 | Encouraging Contractor Policies To Ban Text Messaging While Driving (May 2024) | |
| 52.232-18 | Availability of Funds (Apr 1984) | |
| 52.232-33 | Payment by Electronic Funds Transfer-System for Award Management (Oct 2018) | |
| 52.232-40 | Providing Accelerated Payments to Small Business Subcontractors (Mar 2023) | |
| 52.233-3 (DEV) | Protest after Award (Aug 1996) (DEVIATION NOV 2025) | |
| 52.233-4 (DEV) | Applicable Law for Breach of Contract Claim (Oct 2004) (DEVIATION NOV 2025) | |
| 52.244-6 (DEV) | Subcontracts for Commercial Products and Commercial Services (Jan 2025) (DEVIATION APR 2026) | |
| 52.247-34 | F.o.b. Destination (Nov 1991) | |

**Clauses By Full Text**

52.252-2 Clauses Incorporated by Reference (Feb 1998)

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

www.acquisition.gov

_____

_____
*[Insert one or more Internet addresses]*

(End of clause)

DOJ-02 Contractor Privacy Requirements (JAN 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 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*

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.

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).

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/learndoj. 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 page[3] 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 therefrom, 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 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 0900.00.01[5], 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. <u>Government Records Training, Ownership, and Management</u>

*(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.

(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. <u>Data Privacy and Oversight</u>

*(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 technology[9], 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 project[10] 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.doj.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 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.

[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).
[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.
[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.
[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.

(End of Clause)

DOJ-08 Continuing Contract Performance During a Pandemic Influenza or other National Emergency (OCT 2007)

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

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

- Encourage employees to get inoculations or follow other preventive measures as advised by the public health service.
- Contractors should cross-train workers as backup for all positions performing critical services. This is particularly important for work such as guard services where telework is not an option.
- Implement telework to the greatest extent possible in the workgroup so systems are in place to support successful remote work in an emergency.
- Communicate expectations to all employees regarding their roles and responsibilities in relation to remote work in the event of a pandemic health crisis or other emergency.
- Establish communication processes to notify employees of activation of this plan.
- Integrate pandemic health crisis response expectations into telework agreements.
- With the employee, assess requirements for working at home (supplies and equipment needed for an extended telework period). Security concerns should be considered in making equipment choices; agencies or contractors may wish to avoid use of employees' personal computers and provide them with PCs or laptops as appropriate.
- Determine how all employees who may telework will communicate with one another and with management to accomplish work.
- Practice telework regularly to ensure effectiveness.
- Make it clear that in emergency situations, employees must perform all duties assigned by management, even if they are outside usual or customary duties.
- Identify how time and attendance will be maintained.

It is the contractor's responsibility to advise the government contracting officer if they anticipate not being able to perform and to work with the Department to fill gaps as necessary. This means direct communication with the contracting officer or in his/her absence, another responsible person in the contracting office via telephone or email messages acknowledging the contractor’s notification. The incumbent contractor is responsible for assisting the Department in estimating the adverse impacts of nonperformance and to work diligently with the Department to develop a strategy for maintaining the continuity of operations.

The Department does reserve the right in such emergency situations to use federal employees. employees of other agencies, contract support from other existing contractors, or to enter into new contracts for critical support services. Any new contracting efforts would be acquired following the guidance in the Office of federal Procurement Policy issuance "Emergency Acquisitions", May, 2007 and Subpart 18.2. Emergency Acquisition Flexibilities, of the Federal Acquisition Regulations.

(End of Clause)

**[END OF ADDENDUM TO FAR 52.212-4]**

## Section 3 - List of Attachments

| Identifier | Title | Number of Pages |
|---|---|---|
| 1 | FY27Q1 Halal Religious Diet Menu Specifications.xlsx | |

## Section 4 - Solicitation Provisions

### Provisions By Reference

| **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/these address(es): www.acquisition.gov | | |
| Provision | Title | Fill-ins (if applicable) |
| 52.204-7 (DEV) | System for Award Management-Registration (Nov 2024) (DEVIATION NOV 2025) | |