SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER: PR-26-OTS-0145

PAGE 1 OF 33

2. CONTRACT NO.

3. AWARD/ EFFECTIVE DATE

4. ORDER NUMBER

5. SOLICITATION NUMBER: FRTIB1-26-Q-0027

6. SOLICITATION ISSUE DATE: 7/9/26

7. FOR SOLICITATION INFORMATION CALL:

a. NAME: frtibAMDoperations@frtib.gov

b. TELEPHONE NUMBER *(No collect calls)*: <<<< please email.

8. OFFER DUE DATE/LOCAL TIME: See Clause Section E.4.1.

9. ISSUED BY — CODE OCFO_ACQ_MGT_DIV ISS

FRTIB
77 K Street NE
Suite 1000
Washington DC 20002

10 THIS ACQUISITION IS ☒ UNRESTRICTED OR ☐ SET ASIDE: % FOR:

☐ SMALL BUSINESS
☐ HUBZONE SMALL BUSINESS
☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS (SDVOSB)
☐ WOMEN-OWNED SMALL BUSINESS (WOSB)
☐ ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB)
☐ 8(A)

NORTH AMERICAN INDUSTRY CLASSIFICATION STANDARD (NAICS): 423430

SIZE STANDARD: not applicable.

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 ☒ REQUEST FOR QUOTE (RFQ) ☐ INVITATION FOR BID (IFB) ☐ REQUEST FOR PROPOSAL (RFP)

15. DELIVER TO — CODE

FRTIB
77 K Street NE
Suite 1000
Washington DC 20002

16. ADMINISTERED BY — CODE OCFO_ACQ_MGT_DIV ADM

FRTIB
77 K Street NE
Suite 1000
Washington DC 20002

17a. CONTRACTOR/ OFFEROR — CODE — FACILITY CODE

TELEPHONE NO.

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

18a. PAYMENT WILL BE MADE BY — CODE

See Clause Section B.4.

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

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Security Awareness/Simulation Tool. See the clauses, provisions, and attachments for more info.				
	(Use Reverse and/or Attach Additional Sheets as Necessary)				

25. ACCOUNTING AND APPROPRIATION DATA

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

☒ 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 ☒ 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.

☐ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN zero 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)*

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

30c. DATE SIGNED

31b. NAME OF CONTRACTING OFFICER *(Type or print)*

31c. DATE SIGNED

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

Columns 19 to 24 of this page have been left intentionally blank.

32a. QUANTITY IN COLUMN 21 HAS BEEN

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

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

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

33. SHIP NUMBER	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

B. Continuation of SF-1449 (*per FAR 12.303 - Contract Format*)**.**

B.1 This document consists of the following sections:

SECTION	DESCRIPTION
A	Standard Form 1449
B	Continuation of the SF-1449
C	Contract Clauses
D	Any Contract Documents, Exhibits or Attachments
E	Solicitation Provisions

(End of Section)

B.2 SF-1449 Block 16: Contract Administration

To be provided at the time of the award.

(End of Text)

B.3 SF-1449 Block 17A: Contractor

System updates may lag policy updates. The System for Award Management (SAM) may continue to require entities to complete representations based on provisions that are not included in agency solicitations, including 52.223-22, Public Disclosure of Greenhouse Gas Emissions and Reduction Goals—Representation, and paragraph (t) of 52.212-3, Offeror Representations and Certifications—Commercial Products and Commercial Services. Agencies will not consider or use these representations. Entities are not required to, nor are they able to, update their entity registration to remove these representations in SAM.

(End of Text)

B.4 Block 18a Electronic Invoicing and Payment Requirements - Invoice Processing Platform (IPP) - Oct 2025)

Payment request must be submitted electronically through the U.S. Department of Treasury's Invoice Processing Platform (IPP) system using the "Bill to Agency" of Interior Business Center – FMD.

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. Any changes to submitted invoice (short-pay or withhold) will require resubmission of invoice with revised amount. To constitute a proper invoice, the payment request must comply with the requirements identified in the applicable Prompt Payment clause included in the contract, or the clause 52.212-4 Contract Terms and Conditions – Commercial Items include in commercial item contracts. The IPP website address is: https://www.ipp.gov.

The Contractor must use the IPP website to register, access and use IPP for submitting requests for payment. The Contractor must attach invoices in IPP. The Contractor Government Business Point of Contact (as listed in SAM) will receive enrollment instructions via email from the Federal Reserve prior to the contract award date, but no more than 3 – 5 business days of the contract award date.

Contractor assistance with enrollment can be obtained by contacting the IPP Production Helpdesk via email IPPCustomerSupport@fiscal.treasury.gov or phone (866) 973 – 3131.

If the Contractor is unable to comply with the requirements to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the Contracting Officer with its proposal or quotation.

(End of Text)

SECTION C - CONTRACT CLAUSES

C.1 FAR 52.252-2 Clauses Incorporated by Reference (FEB 1998)

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

(End of Clause)

C.2 Notice Listing Clauses Incorporated by Reference

The following clauses are hereby incorporated by reference (by Citation Number, Title, and Date) in accordance with the clause at FAR "52.252-2 CLAUSES INCORPORATED BY REFERENCE" contained in this document. See FAR 52.252-2 for an internet address (if specified) for electronic access to the full text of a clause.

FEDERAL ACQUISITION REGULATION (48 CFR Chapter 1)		
FAR Number	**Citation Title**	**Date**
52.204-24	Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment	Oct 2020
52.216-18	Ordering	Aug 2020
52.222-90	Addressing DEI Discrimination by Federal Contractors	Apr 2026
52.232-39	Unenforceability of Unauthorized Obligations	Jun 2013

(End of Text)

C.3 52.212-5 Contract Terms and Conditions Required to Implement Statutes or Executive Orders—Commercial Items (MAR 2026)

(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 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)).
(2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities (Dec 2023) (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) (Section 889(a)(1)(A) of Pub. L. 115-232).
(4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015).
(5) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (Mar 2023) (31 U.S.C. 3903 and 10 U.S.C. 3801).
(6) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).
(7) 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 as appropriate.]

__ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Jun 2020), with Alternate I (Nov 2021) (41 U.S.C. 4704 and 10 U.S.C. 4655).
__ (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Nov 2021) (41 U.S.C. 3509)).
__ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)
__ (4) 52.203-17, Contractor Employee Whistleblower Rights (Nov 2023) (41 U.S.C. 4712); this clause does not apply to contracts of DoD, NASA, the Coast Guard, or applicable elements of the intelligence community—see FAR 3.900(a).
__ (5) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Jun 2020) (Pub. L. 109-282) (31 U.S.C. 6101 note).
__ (6) [Reserved].
__ (7) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).
__ (8) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).
X (9) 52.204-27, Prohibition on a ByteDance Covered Application (Jun 2023) (Section 102 of Division R of Pub. L. 117-328).
__ (10) 52.204-28, Federal Acquisition Supply Chain Security Act Orders—Federal Supply Schedules, Governmentwide Acquisition Contracts, and Multi-Agency Contracts. (Dec 2023) (Pub. L. 115–390, title II).
__ (11)(i) 52.204-30, Federal Acquisition Supply Chain Security Act Orders—Prohibition. (Dec 2023) (Pub. L. 115–390, title II).
__ (ii) Alternate I (Dec 2023) of 52.204-30.
__ (12) 52.209-6, Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, Proposed for Debarment, or Voluntarily Excluded. (Jan 2025) (31 U.S.C. 6101 note).
__ (13) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).
__ (14) [Reserved].
__ (15) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Oct 2022) (15 U.S.C. 657a).
__ (16) 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).
__ (17) [Reserved]
__ (18)(i) 52.219-6, Notice of Total Small Business Set-Aside (Nov 2020) (15 U.S.C. 644).
__ (ii) Alternate I (Mar 2020) of 52.219-6.
__ (19)(i) 52.219-7, Notice of Partial Small Business Set-Aside (Nov 2020) (15 U.S.C. 644).
__ (ii) Alternate I (Mar 2020) of 52.219-7.
__ (20) 52.219-8, Utilization of Small Business Concerns (Jan 2025)(15 U.S.C. 637(d)(2) and (3)).
__ (21)(i) 52.219-9, Small Business Subcontracting Plan (Jan 2025) (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 (Jan 2025) of 52.219-9.
__ (22)(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.
__ (23) 52.219-14, Limitations on Subcontracting (Oct 2022) (15 U.S.C. 657s).
__ (24) 52.219-16, Liquidated Damages—Subcontracting Plan (Sep 2021) (15 U.S.C. 637(d)(4)(F)(i)).

__ (25) 52.219-27, Notice of Set-Aside for, or Sole-Source Award to, Service-Disabled Veteran-Owned Small Business (SDVOSB) Concerns Eligible Under the SDVOSB Program (Feb 2024) (15 U.S.C. 657f).
__ (26) (i) 52.219-28, Postaward Small Business Program Rerepresentation (Jan 2025) (15 U.S.C. 632(a)(2)).
__ (ii) Alternate I (Mar 2020) of 52.219-28.
__ (27) 52.219-29, Notice of Set-Aside for, or Sole-Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Oct 2022) (15 U.S.C. 637(m)).
__ (28) 52.219-30, Notice of Set-Aside for, or Sole-Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Oct 2022) (15 U.S.C. 637(m)).
__ (29) 52.219-32, Orders Issued Directly Under Small Business Reserves (Mar 2020) (15 U.S.C. 644(r)).
__ (30) 52.219-33, Nonmanufacturer Rule (Sep 2021) (15 U.S.C. 637(a)(17)).
__ (31) 52.222-3, Convict Labor (Jun 2003) (E.O. 11755).
__ (32) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Mar 2026)(E.O. 13126).
__ (33) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
__ (34) (i) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).
__ (ii) Alternate I (Feb 1999) of 52.222-26.
__ (35)
(i) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).
__ (ii) Alternate I (Jul 2014) of 52.222-35.
__ (36) (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.
__ (37) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212).
__ (38) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).
__ (39) (i) 52.222-50, Combating Trafficking in Persons (Oct 2025) (22 U.S.C. chapter 78 and E.O. 13627).
__ (ii) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).
__ (40) 52.222-54, Employment Eligibility Verification (Jan 2025) (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial products or commercial services as prescribed in FAR 22.1803.)
__ (41) (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.)
__ (42) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (May 2024) (42 U.S.C. 7671, et seq.).
__ (43) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (May 2024) (42 U.S.C. 7671, et seq.).
__ (44) 52.223-20, Aerosols (May 2024) (42 U.S.C. 7671, et seq.).
__ (45) 52.223-21, Foams (May 2024) (42 U.S.C. 7671, et seq.).
__ (46) 52.223-23, Sustainable Products and Services (May 2024) (E.O. 14057, 7 U.S.C. 8102, 42 U.S.C. 6962, 42 U.S.C. 8259b, and 42 U.S.C. 7671l).
__ (47) (i) 52.224-3 Privacy Training (Jan 2017) (5 U.S.C. 552 a).
__ (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).
__ (ii) Alternate I (Oct 2022) of 52.225-1.
__ (49) (i) 52.225-3, Buy American-Free Trade Agreements-Israeli Trade Act (NOV 2023) (19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, 19 U.S.C. chapter 29 (sections 4501-

4732), Public Law 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 [Reserved].
__ (iii) Alternate II (Jan 2025) of 52.225-3.
__ (iv) Alternate III (Feb 2024) of 52.225-3.
__ (v) Alternate IV (Oct 2022) of 52.225-3.
__ (50) 52.225-5, Trade Agreements (NOV 2023) (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 the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. Subtitle A, Part V, Subpart G 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).
X (55) 52.226-8, Encouraging Contractor Policies to Ban Text Messaging While Driving (May 2024) (E.O. 13513).
__ (56) 52.229-12, Tax on Certain Foreign Procurements (Feb 2021).
__ (57) 52.232-29, Terms for Financing of Purchases of Commercial Products and Commercial Services (Nov 2021) (41 U.S.C. 4505, 10 U.S.C. 3805).
__ (58) 52.232-30, Installment Payments for Commercial Products and Commercial Services (Nov 2021) (41 U.S.C. 4505, 10 U.S.C. 3805).
__ (59) 52.232-33, Payment by Electronic Funds Transfer-System for Award Management (Oct2018) (31 U.S.C. 3332).
__ (60) 52.232-34, Payment by Electronic Funds Transfer-Other than System for Award Management (Jul 2013) (31 U.S.C. 3332).
__ (61) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).
__ (62) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).
__ (63) 52.240-1, Prohibition on Unmanned Aircraft Systems Manufactured or Assembled by American Security Drone Act-Covered Foreign Entities (Nov 2024) (Sections 1821-1826, Pub. L. 118-31, 41 U.S.C. 3901 note prec.).
__ (64) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d)(13)).
__ (65)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) (46 U.S.C. 55305 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 products and commercial services:
[Contracting Officer check as appropriate.]
__ (1) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter67).
__ (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).
__ (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) (29U.S.C.206 and 41 U.S.C. chapter 67).

__ (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).
__ (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).
__ (7) 52.222-55, Minimum Wages for Contractor Workers Under Executive Order 14026 (Jan 2022).
__ (8) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2022) (E.O. 13706).
__ (9) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (Jun 2020) (42 U.S.C. 1792).
__ (10) 52.247-69, Reporting Requirement for U.S.-Flag Air Carriers Regarding Training to Prevent Human Trafficking (Jan 2025) (49 U.S.C. 40118(g)).
(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, as defined in FAR 2.101, on the date of award of this contract, 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 products or commercial services. 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) (41 U.S.C. 3509).
(ii) 52.203-17, Contractor Employee Whistleblower Rights (Nov 2023) (41 U.S.C. 4712).
(iii) 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)).
(iv) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities (Dec 2023) (Section 1634 of Pub. L. 115-91).
(v) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Section 889(a)(1)(A) of Pub. L. 115-232).
(vi) 52.204-27, Prohibition on a ByteDance Covered Application (Jun 2023) (Section 102 of Division R of Pub. L. 117-328).
(vii)(A) 52.204–30, Federal Acquisition Supply Chain Security Act Orders—Prohibition. (Dec 2023) (Pub. L. 115–390, title II).

(B) Alternate I (Dec 2023) of 52.204–30.
(viii) 52.219-8, Utilization of Small Business Concerns (Jan 2025) (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 the applicable threshold specified in FAR 19.702(a) on the date of subcontract award, the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.
(ix) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
(x) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).
(xi) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).
(xii) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).
(xiii) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212).
(xiv) 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.
(xv) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).
(xvi)(A) 52.222-50, Combating Trafficking in Persons (Oct 2025) (22 U.S.C. chapter 78 and E.O. 13627).
(B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).
(xvii) 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).
(xviii) 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).
(xix) 52.222-54, Employment Eligibility Verification (Jan 2025) (E.O. 12989).
(xx) 52.222-55, Minimum Wages for Contractor Workers Under Executive Order 14026 (Jan 2022).
(xxi) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2022) (E.O. 13706).
(xxii)(A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).
(B) Alternate I (Jan 2017) of 52.224-3.
(xxiii) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. Subtitle A, Part V, Subpart G Note).
(xxiv) 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.
(xxv) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (Mar 2023) (31 U.S.C. 3903 and 10 U.S.C. 3801). Flow down required in accordance with paragraph (c) of 52.232-40.
(xxvi) 52.240-1, Prohibition on Unmanned Aircraft Systems Manufactured or Assembled by American Security Drone Act-Covered Foreign Entities (Nov 2024) (Sections 1821-1826, Pub. L. 118-31, 41 U.S.C. 3901 note prec.).
(xxvii) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) (46 U.S.C. 55305 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)

Alternate I (Feb 2000). As prescribed in 12.301 (b)(4)(i), delete paragraph (d) from the basic clause, redesignate paragraph (e) as paragraph (d), and revise the reference to "paragraphs (a), (b), (c), or (d) of this clause" in the redesignated paragraph (d) to read "paragraphs (a), (b), and (c) of this clause".
Alternate II (Oct 2025). As prescribed in 12.301 (b)(4)(ii), substitute the following paragraphs (d)(1) and (e)(1) for paragraphs (d)(1) and (e)(1) of the basic clause as follows:
(d)(1) The Comptroller General of the United States, an appropriate Inspector General appointed under section 3 or 8 G of the Inspector General Act of 1978 (5 U.S.C. App.), or an authorized representative of either of the foregoing officials shall have access to and right to—
(i) Examine any of the Contractor's or any subcontractors' records that pertain to, and involve transactions relating to, this contract; and
(ii) Interview any officer or employee regarding such transactions.
(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), and (c), of this clause, the Contractor is not required to flow down any FAR clause in a subcontract for commercial products or commercial services, other than—
(i) Paragraph (d) of this clause. This paragraph flows down to all subcontracts, except the authority of the Inspector General under paragraph (d)(1)(ii) does not flow down; and
(ii) Those clauses listed in this paragraph (e)(1). Unless otherwise indicated below, the extent of the flow down shall be as required by the clause-
(A) 52.203-13, Contractor Code of Business Ethics and Conduct (Nov 2021) (41 U.S.C. 3509).
(B) 52.203-15, Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub. L. 111-5).
(C) 52.203-17, Contractor Employee Whistleblower Rights (Nov 2023) (41 U.S.C. 4712).
(D) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities (Dec 2023) (Section 1634 of Pub. L. 115-91).
(E) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Section 889(a)(1)(A) of Pub. L. 115-232).
(F) 52.204-27, Prohibition on a ByteDance Covered Application (Jun 2023) (Section 102 of Division R of Pub. L. 117-328).
(G)__(1) 52.204–30, Federal Acquisition Supply Chain Security Act Orders— Prohibition. (Dec 2023) (Pub. L. 115–390, title II).
__(2) Alternate I (Dec 2023) 52.204-30.
(H) 52.219-8, Utilization of Small Business Concerns (Jan 2025) (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 the applicable threshold specified in FAR 19.702(a) on the date of subcontract award, the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.
(I) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
(J) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).
(K) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).
(L) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).
(M) 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.
(N) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).
(O) **X** (1) 52.222-50, Combating Trafficking in Persons (Oct 2025) (22 U.S.C. chapter 78 and E.O. 13627).
__ (2) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).

(P) 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).
(Q) 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).
(R) 52.222-54, Employment Eligibility Verification (Jan 2025) (Executive Order 12989).
(S) 52.222-55, Minimum Wages for Contractor Workers Under Executive Order 14026 (Jan 2022).
(T) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2022) (E.O. 13706).
(U)__ (1) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).
__ (2) Alternate I (Jan 2017) of 52.224-3.
(V) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. Subtitle A, Part V, Subpart G Note).
(W) 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.
(X) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (MAR 2023) (31 U.S.C. 3903 and 10 U.S.C. 3801). Flow down required in accordance with paragraph (c) of 52.232-40.
(Y) 52.240-1, Prohibition on Unmanned Aircraft Systems Manufactured or Assembled by American Security Drone Act-Covered Foreign Entities (Nov 2024) (Sections 1821-1826, Pub. L. 118-31, 41 U.S.C. 3901 note prec.).
(Z) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) (46 U.S.C. 55305 and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(End of Clause)

C.4 FAR 52.252-6 Authorized Deviations in Clauses (Nov 2020)
(a)The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.
(b)The use in this solicitation or contract of Contract Terms and Conditions Required to Implement Statutes or Executive Orders—Commercial Items (MAR 2026) 48 CFR § 52.212-5 clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of clause)

C.5 Records Management Obligations Prescription:
“Federal record” as defined in 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.

- The term Federal record:
- Includes Agency records;
- Does not include personal materials;
- Applies to records created, received, or maintained by Contractors pursuant to their Agency contract;
- May include deliverables and documentation associated with deliverables.

Requirements

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, 33), NARA regulations at 36 CFR 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 records, regardless of form or characteristics, mode of transmission, or state of completion.

In accordance with 36 CFR 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.

In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and 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.

FRTIB and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of FRTIB or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. 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 of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to the FRTIB Contracting Officer and COR. The agency must report promptly to NARA in accordance with 36 CFR 1230.

The Contractor shall immediately notify the appropriate Contracting Officer and COR 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 the contract vehicle.

The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment are properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment are no longer required, it shall be returned to FRTIB control, or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer and COR or address prescribed in the contract vehicle. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) 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 sub-contractor) is required to abide by Government and FRTIB guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with FRTIB policy.

The Contractor shall not create or maintain any records containing any non-public Agency information that are not specifically tied to or authorized by the contract.

The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.
The FRTIB owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which FRTIB 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.
Training. All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take FRTIB 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.
[Note: To the extent an agency requires contractors to complete records management training, the agency must provide the training to the contractor.]
Flow down of requirements to subcontractors:
The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract vehicle, 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.

(End of Clause)

C.6 Recordkeeping & Proprietary Information Prescription:

Definitions. As used in this clause—
"Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.
The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract:
The Contractor shall protect the information against unauthorized access, modification, release, or disclosure.
The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.
All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take FRTIB provided Controlled Unclassified Information training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.
All Contractor employees assigned to this contract who create, work with, or otherwise handle FRTIB or TSP records using Government Furnished Property are required to take FRTIB provided Controlled Unclassified Information training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.
FRTIB safeguarding and use of contractor attributional/proprietary information. The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with the Cyber Incident Reporting clause. To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the

Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is released.
Use and release of contractor attributional/proprietary information not created by or for FRTIB. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for FRTIB is authorized to be released outside of FRTIB—
To entities with missions that may be affected by such information;
To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;
To Government entities that conduct counterintelligence or law enforcement investigations;
For national security purposes, including cyber situational awareness and defense purposes;
To a support services contractor ("recipient") that is directly supporting Government activities under a contract.
Use and release of contractor attributional/proprietary information created by or for FRTIB. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for FRTIB is authorized to be used and released outside of FRTIB for purposes and activities authorized by paragraph (f) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(End of Clause)

C.7 Advertising and Release of Information

The Contractor and any of its subcontractors shall not publicize or advertise in relation to this contract without the prior written approval of the Agency. Also, the Contractor and any of its subcontractors shall not release information or report on its performance under the contract without the prior written approval of the Agency.
Flow-down of requirements to subcontractors as follows:
The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract vehicle, 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.

(End Clause)

C.8 Federal Information Security Modernization Act (FISMA) Compliance

Definitions. As used in this clause—
"Continuous Diagnostics and Mitigation (CDM) agency dashboard" displays data about devices, users, privileges, and vulnerabilities. This dashboard collects and arranges detailed information on vulnerabilities gathered and provides an object-level view of an agency's cybersecurity posture.
"Covered contractor information system" means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits Controlled Unclassified Information. This system doesn't receive an agency authorization.
"Federal information system" means information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency. This system receives an agency authorization.
"Government data" means any information, document, media, or machine-readable material regardless of physical form or characteristics, that is created or obtained by the Government in the course of official Government business.

“Government-related data” means any information, document, media, or machine-readable material regardless of physical form or characteristics that is created or obtained by a contractor through the storage, processing, or communication of Government data. This does not include contractor’s business records, e.g. financial records, legal records etc. or data such as operating procedures, software coding or algorithms that are not uniquely applied to the Government data.
“High Value Asset” means designation of information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have serious impacts on the organization’s ability to perform its mission or conduct business.
“Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
“Privacy control” means the administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.
“Security controls” means the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
The Contractor shall comply with Federal Information Security Modernization Act (FISMA) in accordance with current versions of National Institute of Standards and Technology (NIST) Special Publication 800-53 series, 800-37 and the Cybersecurity Framework (CSF); as well as guidance issued in furtherance of FISMA that includes, but is not limited to, Executive Orders, Office of Management and Budget (OMB) guidance, other related NIST publications and guidance, Binding Operational Directives (BODs), and other guidance issued by the Cybersecurity and Infrastructure Security Agency (CISA). Contractor shall take actions to comply with revisions and/or new versions of FISMA that are part of routine operations at no additional cost to FRTIB.
Cybersecurity is a rapidly changing and evolving area governed by a variety of laws, regulations, directives, and guidance. Contractor shall be responsible for maintaining reasonable compliance with the cybersecurity requirements made applicable to this contract and Contractor’s own evolving cybersecurity best practices.
The Contractor shall select security controls according to the categorization approved by FRTIB, including applicable High Value Asset (HVA) controls.
FRTIB may accept system security controls other than those recommended by NIST. However, if other controls are used, they must be appropriately mapped to the NIST recommended controls and pass the assessment criteria outlined by NIST. Deviations from the agency’s FISMA policies and above-mentioned related guidance must be approved by the Contracting Officer.
Contractor’s security plan and implementation of its controls must be designed to support ongoing authorization requirements as defined by the FRTIB’s Information Security Continuous Monitoring (ISCM) program. The Contractor must have the ability to support real-time authorization decisions based on factors such as Continuous Diagnostics and Mitigation (CDM) agency dashboard data, automated control assessments, and agreed-upon assessments of non-automated controls. Contractor is required to implement the CDM tools and technologies as a part of the initial authorization process.
On a periodic basis, FRTIB reserves the right to evaluate any or all of the security controls, privacy controls, and other privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-days’ notice, at the request of the FRTIB, the Contractor shall fully cooperate and assist in an FRTIB-sponsored security and privacy controls assessment at each location wherein FRTIB information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of FRTIB. The FRTIB may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by FRTIB in the event of an incident or other circumstances indicating material non-compliance or urgent risk to agency information.

FRTIB or TSP information systems that support processing, transmitting, or storing of Agency data are to be used in support of FRTIB mission only. All data contained on FRTIB or TSP information systems in support of FRTIB is owned by the FRTIB and may be monitored, intercepted, recorded, read or captured. The Contractor shall provide the Government, or its authorized representatives, access to all Government data and Government-related data, access to contractor personnel involved in the performance of the contract, and physical access to any Contractor facility with Government data, for the purpose of audits, investigations, inspections, or other similar activities, as authorized by law or regulation.

Flow-down of requirements to subcontractors

The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract vehicle, 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.

(End Clause)

C.9 General Cybersecurity Compliance

Definitions. As used in this clause—

The Contractor shall establish, implement, and maintain a comprehensive cybersecurity program that adheres to cybersecurity best practices and addresses the risks associated with the information systems and data used to perform this contract.

The Contractor has no reasonable expectation of privacy while performing work in support of the contract on any Agency information system that processes, transmits, or stores FRTIB data.

All Contractors accessing a federal information system shall utilize a government-issued Personal Identity Verification (PIV) card or another agency approved phishing-resistant authenticator.

The contractor shall be responsible for properly protecting all information and data used, gathered, or developed as a result of work under this contract. All FRTIB information, data, and/or equipment shall only be disclosed to authorized personnel on a need-to-know basis in order to support the performance of the contract. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment shall be returned to the Government. Disposition of this information shall be followed in accordance with the A.3 Records Management Obligations clause and the current version of NIST SP 800-88, "Guidelines for Media Sanitization." The Contractor shall provide the confirmation of disposition to the Contracting Officer in accordance with contract closeout procedures

The Contractor shall use Government-related data only to manage the operational environment that supports the Government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.

The Contractor shall notify the Contracting Officer promptly of any requests from a third party for access to Government data or Government-related data, including any warrants, seizures, or subpoenas it receives, including those from another Federal, State, or local agency. The Contractor shall cooperate with the Contracting Officer to take all measures to protect Government data and Government-related data from any unauthorized disclosure.

Flow-down of requirements to subcontractors

The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract vehicle, 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.

(End Clause)

C.10 Cyber Incident Reporting

Definitions. As used in this clause—

"Breach" means 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 sensitive information (e.g., CUI, personally identifiable information, contract-sensible, etc.) or (2) an authorized user accesses or potentially accesses personally identifiable information for unauthorized purposes.

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

"Computer software" means computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae and related material that would enable the software to be reproduced, recreated, or recompiled. Computer software does not include computer databases or computer software documentation.

"Covered contractor information system" means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits Controlled Unclassified Information. This system doesn't receive an agency authorization.

"Controlled Unclassified Information (CUI)" means information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, and is—

Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of FRTIB in support of the performance of the contract; or

Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

"Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the confidentiality, integrity, or availability of information residing therein.

"Forensic analysis" means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

"Malicious software" means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

"Media" means physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system.

Cyber incident reporting requirement.

When the Contractor discovers a cyber incident or breach of an information system that stores or processes FRTIB information or data, the Contractor shall:

Immediately report all actual or potential cyber incidents to FRTIB at IncidentResponse@frtib.gov;

Require training for contractors and subcontractors on how to identify and report an incident or breach; and Conduct a review of their IT environment for evidence of compromise.

This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident or breach, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised Controlled Unclassified Information, or that affect the Contractor's ability to provide contractual services. The review shall include, but not be limited to, identifying any/all compromised computers, servers, specific data, and user accounts, for the purpose of identifying what information was or may have been accessed and by whom, creating timelines of unauthorized/malicious activity, determining methods and techniques used for system access, and identifying the attack vector.

The cyber incident report shall be treated as information created by or for FRTIB and shall include, at a minimum, the required elements in accordance with FRTIB Cyber Incident Response Policy and Procedures.

When the Contractor or subcontractor discovers and isolates malicious software in connection with a reported cyber incident, the Contractor shall coordinate the transfer, as requested by FRTIB, for a sample of the malicious software to IncidentResponse@frtib.gov. Contractor must not send the malicious software to the Contracting Officer or Contractor Officer's Representative (COR).

When a Contractor discovers a cyber incident or breach has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (b)(1)(iii) of this clause and all relevant monitoring/packet capture data for 90 days **from the date of discovery of the cyber incident** so that the Government can request and review them if needed.

The Contracting Officer will request that the Contractor provide all the damage assessment information gathered in accordance with paragraph (d) of this clause.

Upon request by FRTIB, the Contractor shall provide FRTIB with access to additional information or equipment that is necessary to conduct a forensic analysis.

The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations that govern the interception, monitoring, access, use, and disclosure of electronic communications and data.

The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

If Contractor's performance of services results in a breach of FRTIB data, the Contractor shall bear the losses and expenses (including attorneys' fees) associated with the breach including costs associated with (1) providing notice of the breach to affected individuals and to applicable regulatory bodies; (2) establishing call centers for affected individuals; and (3) providing individuals with credit and identity monitoring and credit and identity restoration services on an opt-in basis. The necessary remediation measures will be determined by FRTIB in accordance with FRTIB's Breach Response policy and procedures.

The Contractor agrees that the following conditions apply to cyber incident information it receives or creates in the performance of this contract, including information obtained from a third-party's reporting of a cyber incident:

The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to this clause and shall not be used for any other purpose.

The information is considered sensitive and is subject to protection and disclosure restrictions in accordance with OTS.1 General Cybersecurity clause.

The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.

The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure obligations and restrictions of this clause.
A breach of these obligations or restrictions may subject the Contractor to—
Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third-party beneficiary of this clause.
Flow-down of requirements to subcontractors
The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract vehicle, 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.
Require subcontractors to provide the incident report number assigned by the subcontractor's Security Operations Center or Computer Security Incident Response Team (CSIRT), to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber- incident to FRTIB as required in paragraph (b) of this clause.

(End of Clause)

C.11 Penetration Testing

Definitions. As used in this clause—
"Controlled Unclassified Information (CUI)" means information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, and is—
Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of FRTIB in support of the performance of the contract; or
Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.
The Contractor shall participate and assist FRTIB in its penetration testing program at the frequency agreed upon by the Contractor and Agency.
Rules of engagement for penetration testing shall be mutually agreed upon by the Contractor and the Agency prior to conducting penetration testing.
Penetration testing results shall be treated as Controlled Unclassified Information// Information Systems Vulnerability Information (CUI//ISVI) and shall be handled according to the Agency's CUI policies.
The Contractor shall remediate all identified vulnerabilities in keeping with the Agency's vulnerability management program.
For some cloud solutions, penetration testing conducted by previous penetration testing effort may be accepted at the sole discretion of the Agency.
Flow-down of requirements to subcontractors
The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract vehicle, 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.

(End of Clause)

C.12 Cloud Computing Services

Definitions. As used in this clause—

"Cloud computing" means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

"Government data" means any information, document, media, or machine-readable material regardless of physical form or characteristics, which is created or obtained by the Government in the course of official Government business.

The requirements of this clause are applicable when using cloud computing to provide information technology services in the performance of the contract.

If the Contractor indicated in its offer that it "does not anticipate the use of cloud computing services in the performance of a resultant contract," in response to provision A.11 Representation of Use of Cloud Computing, and after the award of this contract, the Contractor proposes to use cloud computing services in the performance of the contract, the Contractor shall obtain approval from the Contracting Officer prior to utilizing cloud computing services in performance of the contract.

All government data in transit and at rest must remain within the confines of the United States.

All cloud computing services must meet security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.

Flow-down of requirements to subcontractors

The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract vehicle, 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.

(End of Clause)

C.13 System Development/Engineering Lifecycle

Contractor shall implement a System Development Life Cycle (SDLC) or System Engineering Life Cycle (SELC) to manage systems, applying cyber resiliency design principles, constructs, and concepts from NIST Special Publication 800-160 and its associated volumes. Contractor shall attest that all systems have a documented SDLC and provide FRTIB with documentation upon request by the CO or COR.

The SDLC/SELC must be designed to receive and incorporate from FRTIB the necessary security requirements, including those outlined in the current version of NIST Special Publication 800-218 and related NIST guidance.

Flow-down of requirements to subcontractors

The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract
vehicle, 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.

(End of Clause)

C.14 Supply Chain Risk Management (SCRM):

Definitions. As used in this clause—

"High Value Asset" means designation of information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have serious impacts on the organization's ability to perform its mission or conduct business.

"Software Bill of Material (SBOM)" is a formal record containing the details and supply chain relationships of various components used in building software.

The Contractor shall maintain a trusted software supply chain by verifying the provenance of all third-party components used in the software.

The Contractor shall comply with the following Software Bill of Materials (SBOM) requirements:

The Contractor shall provide a Software Bill of Materials (SBOM) for all High Value Asset (HVA) software, software containing CUI/PII and other software that the Agency identifies ad critical software. The SBOM shall include details such as, but not limited to, component name, version, license information, and any known vulnerabilities.

The Contractor shall update the SBOM whenever there are changes to the software components, including updates, patches, or new versions. The updated SBOM must be provided to the customer within 30 days of the change.

The Contractor shall ensure that all software components listed in the SBOM are free from known vulnerabilities at the time of delivery.

The Contractor shall continuously monitor the SBOM for vulnerabilities and Known Exploited Vulnerabilities (KEVs) and report those that cannot be resolved within the defined timeline specified in the Agency's Vulnerability Management Procedures.

The Contractor shall comply with all applicable laws, regulations, and industry standards related to the creation and maintenance of SBOMs. This includes adherence to guidelines set forth by the National Telecommunications and Information Administration (NTIA), security and Infrastructure Security Agency (CISA), and other relevant authorities.

Flow-down of requirements to subcontractors

The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract vehicle, 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.

(End Clause)

C.15 Artificial Intelligence Use Across Multiple Agreements

This clause establishes standardized terms governing the development, deployment, and oversight of artificial intelligence (AI) systems in contractual relationships. It balances innovation with ethical, legal, and operational safeguards, drawing from emerging regulatory frameworks and industry best practices.

AI System Definition and Scope

For purposes of this Agreement, “AI System” is defined per section 7223 of the Advancing American AI Act which states that "[t]he term 'artificial intelligence system'- (A) means any data system, software, application, tool, or utility that operates in whole or in part using dynamic or static machine learning algorithms or other forms of artificial intelligence, whether-
(i) the data system, software, application, tool, or utility is established primarily for the purpose of researching, developing, or implementing artificial intelligence technology; or (ii) artificial intelligence capability is integrated into another system or agency business process, operational activity, or technology system; and (B) does not include any common commercial product within which artificial intelligence is embedded, such as a word processor or map navigation system. This includes but is not limited to:
Supervised, unsupervised, transfer learning, or reinforcement learning models
Generative AI tools (e.g., large language models, diffusion models)
Automated decision-making systems, fully autonomous, partially autonomous, and not autonomous, and it includes systems that operate both with and without human oversight.

Permitted Uses and Restrictions

Authorized Applications

The AI System may be used solely for:

- Operational Efficiency: Automating repetitive tasks in specify domain, e.g., customer service, data analysis
- Predictive Analytics: Generating insights from datasets related to define scope, e.g., market trends, equipment maintenance
- Content Creation: Producing draft materials in identified formats e.g., reports, marketing copy subject to human review

Prohibited Activities

Explicitly barred uses include:

- High-Risk Applications: Facial recognition in public spaces, social scoring, or real-time biometric identification without explicit opt-in consent
- Legal/Medical Decisions: Outputs that directly influence judicial rulings, medical diagnoses, or treatment plans without human validation
- Synthetic Media: Generating deepfakes or synthetic voices for deceptive purposes
- For High Impact AI as defined in OMB Memorandums M-25-21 and M-25-22, AI output that serves as a principal basis without human oversight for decisions or actions with legal, material, binding, or significant effect on:
    - an individual or entity's civil rights, civil liberties, or privacy
    - an individual or entity's access to education, housing, insurance, credit, employment, and other programs
    - an individual or entity's access to critical government resources or services
    - human health and safety
    - critical infrastructure or public safety
    - strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government.
    - ability to apply for, or adjudication of, requests for critical federal services, processes, and benefits to include loans and access to public housing; determination of continued eligibility for ongoing benefits; the control of access-through biometrics or other means (e.g., signature

matching)-to IT systems for accessing services for benefits; detection of fraudulent use or attempted use of government services; adjudication of penalties in the context of government benefits.

Data Governance Framework

Input/Output Ownership

Customer Data: All training data, prompts, and queries ("Inputs") remain the exclusive property of FRTIB
Derivative Works: Outputs generated by the AI System constitute joint intellectual property by FRTIB, unless otherwise negotiated. FRTIB retains unrestricted intellectual property rights to use Outputs generated by the AI System.

Usage Rights

Contractor grants FRTIB a non-exclusive, non-transferable right to:
Process Inputs through the AI System for the Agreement's stated purposes
Store Outputs for specified retention period. This retention period will be no less than 36 months with automatic encryption, unless otherwise agreed to by the parties.

Confidentiality Safeguards

Anonymization: Personal data must be de-identified using specified techniques, e.g., k-anonymity, differential privacy before processing
Re-Identification Ban: Parties warrant they will not attempt to reverse-engineer anonymized datasets

Transparency and Explainability

Disclosure Requirements

Contractor shall:

- Maintain publicly accessible documentation detailing the AI System's architecture, training data sources, and accuracy metrics
- Implement an API or dashboard enabling real-time monitoring of model drift and performance degradation

Right to Explanation

Upon request, Contractor must furnish:

- A plain-language summary of the factors influencing any material AI-driven decision affecting FRTIB
- Technical evidence demonstrating compliance with stated accuracy thresholds (e.g., ROC-AUC ≥ 0.85)
- Ethical and Operational Guardrails

Bias Mitigation

Contractor warrants that:

- Training datasets underwent statistical parity analysis across protected characteristics (race, gender, age, etc.)
- Models were audited using specified frameworks, e.g., IBM AI Fairness 360, Google What-If Tool

Human Oversight
FRTIB agrees to:

- Use best efforts to maintain a minimum 2:1 ratio between automated decisions and human validations during the first 12 months of deployment
- Coordinate with technical, legal, and/or any applicable compliance governance board to ensure the ethical use of AI.

Intellectual Property Allocation

Pre-Existing IP
Each party retains ownership of background IP contributed to the AI System. Contractor grants an unrestricted license to FRTIB to use algorithms/patents, unless otherwise agreed to by the parties Contractor shall clearly assert any limitations on Pre-Existing IP within their proposal that forms the basis for contract award.

Vendor Lock-In
Per OMB memorandums M-25-21 and M-25-22 to mitigate potential vendor lock-in of AI system, as soon as a decision is made by FRTIB not to extend a contract for an AI system or service or within 90 calendar days before the expiration of the contract's full performance period, the FRTIB retains ongoing rights and access to any data or derived products resulting from the services provided under the contract. FRTIB and Contractor shall come to a mutual understanding of format and usability of any data, and any circumstances that could result in expiration of access, as well as a plan for conducting any transfers of data or other derived assets necessary per the terms of the contract. The Contractor shall work in good faith with FRTIB to establish ongoing usability of data, including format and transferability of data upon expiration of contract. Any limitations on FRTIB's unrestricted use, access and transfer rights to all data shall be clearly defined by the Contractor within their proposal for award prior to contract execution and is subject to agreement by FRTIB.

Derivative Models
Fine-tuned models created using FRTIB data:
FRTIB retains unrestricted data rights
Any claims of Contractor data rights must be asserted in Contractor's proposal that forms the basis for contract award. Any Contractor data rights requires FRTIB's written consent for commercial exploitation and/or release to any third party.

Liability and Risk Allocation

Excluded Liabilities
Contractor is not responsible for:

1. Outputs modified by FRTIB without Contractor's written approval
2. Decisions made by FRTIB contrary to the AI System's documented limitations

Third-Party Indemnification
Contractor shall defend FRTIB against claims alleging:

1. Copyright infringement in training data, provided Contractor followed approved data sourcing protocols
2. Discriminatory impacts traceable to unmodified Contractor algorithms

Compliance and Audit Rights

Regulatory Alignment

The AI System shall comply with:

1. GDPR Articles 13–15 (transparency requirements for automated processing)
2. EU AI Act risk categorization protocols
3. Jurisdiction-specific mandates, e.g., NYC Local Law 144

Audit Mechanism

FRTIB may conduct regular audits through a certified third party to verify:

1. Training data provenance and consent documentation
2. Operational adherence to stated accuracy/ethics benchmarks

Dynamic Adaptation Clause

This clause automatically incorporates:
Technical Updates: Newly published IEEE/ISO standards for AI governance
Regulatory Changes: Finalized AI rules from specified agencies, e.g., EU Commission, NIST
Version Control: Provider will maintain a changelog accessible at URL

Implementation Notes

1. Modular Design: Sections may be adopted à la carte based on risk profiles (e.g., exclude Section_ for non-commercial AI uses)
2. Jurisdictional Tailoring: Replace bracketed terms with localized requirements (retention periods, damage caps)
3. Integration Protocol: Reference this clause as Exhibit _ in master service agreements with version control via blockchain timestamping this framework synthesizes technical safeguards from, compliance mandates from, and sector-specific adaptations from, creating a balanced contractual foundation for responsible AI deployment.

(End of Clause)

C.16 Artificial Intelligence (AI) Compliance and Ethics

Ethical AI Development:

1. The Contractor shall ensure that all AI technologies and systems are developed and deployed in accordance with ethical guidelines, including but not limited to fairness, accountability, transparency, and privacy.
2. The Contractor shall implement measures to prevent bias and discrimination in AI algorithms and ensure equitable treatment of all individuals.

Data Privacy and Security:

1. The Contractor shall adhere to all applicable data privacy and security regulations, including the Federal Information Security Management Act (FISMA) and the General Data Protection Regulation (GDPR), where applicable.
2. The Contractor shall implement robust data protection measures to safeguard sensitive information and prevent unauthorized access or data breaches.

Transparency and Explainability:

1. The Contractor shall ensure that AI systems are transparent and explainable, providing clear documentation on how AI decisions are made.
2. The Contractor shall provide mechanisms for users to understand and challenge AI-driven decisions, ensuring accountability and trust in AI systems.

Continuous Monitoring and Evaluation:

1. The Contractor shall establish processes for continuous monitoring and evaluation of AI systems to ensure ongoing compliance with ethical standards and regulatory requirements. Upon request by the FRTIB, the Contractor shall furnish their processes to FRTIB for verification of compliance. The Contractor shall promptly address any identified issues or concerns related to AI systems and report them to the FRTIB.
2. FRTIB shall retain the ability to regularly monitor and evaluate (based on the needs of the program) performance, risks, and effectiveness of an AI system or service.
3. FRTIB shall use in-house defined data (e.g., agency validation and testing datasets) when conducting any independent evaluations to ensure the AI system or service is fit for purpose. The data used when conducting independent evaluations will not be accessible to Contractor. The test data and validation set will be as similar as possible to the data used when the system is deployed.
4. Contractor must provide the access and time necessary for FRTIB to complete independent evaluation. FRTIB may allow Contractor to complete that testing when most appropriate, but must closely monitor such instances and require testing results detailed enough for the testing to be independently verified or reproduced, if practicable.

Training and Awareness:

1. The Contractor shall provide training and awareness programs for all personnel involved in the development, deployment, and use of AI technologies to ensure understanding of ethical guidelines and compliance requirements.
2. The Contractor shall promote a culture of ethical AI practices within the organization.

(End Clause)

C.17 Post Quantum Cryptography

Definitions. As used in this clause—

"Federal information system" means information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency. This system receives an agency authorization.

"Post-quantum Cryptography" ("PQC") means to develop cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks.

The Contractor shall comply with or provide a plan with a timeline on complying with EO 14028, EO 14144 and all applicable standards, directives and guidelines for post-quantum cryptography as published by the National Institute of Standards and Technology (NIST) and other relevant authorities. The Contractor shall ensure that all cryptographic implementations adhere to these standards. If the Contractor is not in full compliance as of the date of this contract award, the Contractor shall, within 30 days of award, submit to the Contracting Officer a plan and proposed timeline for achieving such compliance. The plan and timeline shall be subject to review and approval by the Contracting Officer.

The Contractor shall implement, or adopt and utilize, post-quantum cryptographic algorithms that meet the security requirements specified in NIST's PQC standards. Where a compliance plan and timeline have been approved by the Contracting Officer under paragraph (b), the Contractor shall implement such algorithms in accordance with that approved timeline.

Flow-down of requirements to subcontractors
The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract vehicle, 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.

(End Clause)

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS
Attachment A: Statement of Work.
Attachment B: Brand Name Justification
Attachment C: Price Schedule.

(End of Section)

Section E Solicitation Provisions
E.1 FAR 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): https://www.acquisition.gov/far/ and https://www.frtib.gov/pdf/procurement/Thrift_Federal_Acquisition_Supplement_T-FAS.pdf

(End of provision)

E.2 Notice Listing Provisions Incorporated by Reference
The following provisions are hereby incorporated by reference (by Citation Number, Title, and Date) in accordance with the clause at FAR "52.252- PROVISIONS INCORPORATED BY REFERENCE" contained in this document. See FAR 52.252-1 for an internet address (if specified) for electronic access to the full text of a clause.

FEDERAL ACQUISITION REGULATION (48 CFR Chapter 1)		
Title	**Citation Title**	**Date**
FAR 52.204-7	System for Award Management	OCT 2018
FAR 52.211-6	Brand Name or Equal	AUG 1999
FAR 52.212-3	Offeror Representations and Certifications—Commercial Items	FEB 2021

(End of provision)

E.3 52.216-1 TYPE OF CONTRACT (APR 1984)
The Government contemplates award of a Firm-Fixed-Price, requirements Purchase Order resulting from this solicitation.

(End of Provision)

E.4 EVALUATION FACTORS FOR AWARD.

The Government intends to make one award as a result of this requirement. Award selection will be based on the lowest price technically acceptable quote. A quote shall demonstrate a comprehension of the Statement of Work. The Government reserves the right to make award without discussion.

(End of Provision)

E.5 ADDITIONAL INSTRUCTIONS FOR OFFERORS.

1) The respondent shall submit a quote to ronald.rheinardt@frtib.gov and FRTIBAMDOperations@frtib.gov for receipt no later than the date set on this solicitation's SAM.gov posting.

2) The Offeror agrees to hold this offer firm, if accepted within 60 calendar days from the date for receipt of offers.

3) Any questions or comments regarding this solicitation shall be submitted through email to ronald.rheinardt@frtib.gov and FRTIBAMDOperations@frtib.gov by the date set on this solicitation's posting on SAM.gov.

(End of Provision)

Attachment A: Statement of Work.

Background
The Federal Retirement Thrift Investment Board (FRTIB); herein also stated as "the agency," was established as an independent agency of the United States Government by the Federal Employees Retirement System Act of 1986. The agency was established to administer the Thrift Savings Plan, which provides Federal employees the opportunity to save for additional retirement security.

Requirements/Scope/Objectives
FRTIB requires a Security Awareness and Simulation Tool that provides AI-powered security awareness training and phishing simulations to help organizations reduce human-related cyber risk. The platform delivers realistic, multi-channel attack simulations (email, SMS, and voice—including AI-generated deepfake scenarios) and combines them with personalized, role-based training and risk analytics. This enables organizations to train employees, identify vulnerabilities, and respond to phishing threats more effectively. This award is being recommended to Adaptive Security and executed under FAR 6.302-1, Only One Responsible Source.

The acquisition of the Adaptive Security platform (AI-driven phishing simulation, voice phishing (vishing) and SMS phishing (smishing) simulations) directly supports FRTIB's strategic objective of building a proactive, resilient, and high-performing organization by strengthening workforce readiness, improving decision-making, and enhancing operational effectiveness.

The contractor must be a United States of America (U.S.A.) business entity, and its primary business location must be within the U.S.A. The subscription services location will be on FRTIB IT network.

Period of Performance
Please see the price schedule for more information.

Contract Performance Location
Subscription services will be performed on the FRTIB IT network.

Deliverables
Please see the part list in Price Schedule

Security Requirements and Standards.
N/A

Information Technology
There are no information technology applications this vendor will have access to. The vendor will work with FRTIB IT to push application software updates as necessary.

Agency Specific IT Requirements
FRTIB IT (OTS) will install necessary vendor application, and all update pushes required to run software.

Contractor Specific IT Requirements
N/A

Agency Furnished Equipment (AFE) and Agency Furnished Information (AFI)
N/A

I. AGENCY & CONTRACTING DIVISION
Federal Retirement Thrift Investment Board
OCFO/Acquisition Management Division (AMD)
77 K Street N.E., Suite 1000
Washington, D.C. 20002

II. NATURE AND/OR DESCRIPTION OF THE ACTION BEING APPROVED
FRTIB requires a Security Awareness and Simulation Tool that provides AI-powered security awareness training and phishing simulations to help organizations reduce human-related cyber risk. The platform delivers realistic, multi-channel attack simulations (email, SMS, and voice—including AI-generated deepfake scenarios) and combines them with personalized, role-based training and risk analytics. This enables organizations to train employees, identify vulnerabilities, and respond to phishing threats more effectively. This award is being recommended to Adaptive Security and executed under FAR 6.302-1, Only One Responsible Source.

The acquisition of the Adaptive Security platform (AI-driven phishing simulation, voice phishing (vishing) and SMS phishing (smishing) simulations) directly supports FRTIB's strategic objective of building a proactive, resilient, and high-performing organization by strengthening workforce readiness, improving decision-making, and enhancing operational effectiveness.

The Agency currently utilizes the SANS End User Security Awareness Training and Phishing Bundle under Contract No. FRTIB1-26-P-0003 FE, which the base year will conclude February 4, 2027, for phishing training.

III. DESCRIPTION OF THE SUPPLIES/SERVICES REQUIRED TO MEET THE AGENCY'S NEEDS

<u>Training and Platform</u>
- Artificial Intelligence and Cyber security training modules
- Ability to use AI to create training content
- Ability to export in SCORM format
- Ability to create newsletters and posters
- Custom deepfake generation
- Ability to create reports

<u>Phishing Simulations</u>
- Ability to include QR codes in simulations
- Phishing templates including from popular vendors and companies
- Ability to use AI to create simulations

<u>Voice (Vishing) and SMS (Smishing) Simulations</u>
- Ability to create custom deepfakes
- Ability to handle incoming and outgoing calls
- Ability to handle outgoing SMS

IV. AUTHORITY PERMITTING OTHER THAN FULL AND OPEN COMPETITION
This template is for the following authority only:
- FAR 6.302-1, Only one responsible source and no other supplies or services will satisfy agency requirements.

- Use the agency-appropriate statutory citation required by FAR 6.301(b) (for example, 41 U.S.C. 3304(a)(1) for civilian agencies).

During our market research Adaptive Security was the only provider we found that satisfies all the agency's requirements, specifically phishing simulations, voice phishing simulations, SMS phishing simulations, deepfake simulations, open-source intelligence integration into campaigns, and spear phishing.

V. DEMONSTRATION THAT THE PROPOSED CONTRACTOR'S UNIQUE QUALIFICATIONS OR THE NATURE OF THE ACQUISITION REQUIRES USE OF THE AUTHORITY CITED

The Agency conducted a multi-faceted market research effort from September 2025 through June 2026 to identify and evaluate commercially available security awareness training and phishing simulation platforms capable of meeting evolving cybersecurity requirements. This effort included vendor demonstrations, conference participation, and direct vendor outreach to assess capabilities, market trends, and emerging technologies.

- Vendor Demonstrations

The Agency participated in multiple vendor-led demonstrations to evaluate platform functionality, integration capabilities, and alignment with operational needs. These demonstrations were conducted virtually via Microsoft Teams unless otherwise noted.

  - November 17, 2025 & June 11, 2026: Living Security – Product demonstrations.
  - May 26, 2026: Abnormal.AI – Product demonstration.
  - September 3, 2025, November 18, 2025 and June 15, 2026: Adaptive Security – Multiple demonstrations and deep-dive sessions.

These demonstrations enabled the Agency to assess user interface, phishing simulation realism (email, SMS, and voice), reporting capabilities, and integration with Microsoft 365 environments, which are critical to FRTIB operations.

- Industry Conferences and Expos

The Agency conducted in-person market research at RSA Conference 2026, held from March 23–26, 2026, a leading cybersecurity industry event that brings together solution providers and federal stakeholders. Vendors engaged In-Person: Adaptive Security, Arctic Wolf, and Proofpoint

During the conference, Agency representatives attended vendor booths, live demonstrations, and product briefings, allowing for direct comparison of vendor capabilities, particularly in AI-driven security awareness, managed detection and response (MDR), and phishing protection technologies. The event provided insight into emerging trends, including the increasing use of AI in social engineering attacks (e.g., deepfakes and voice phishing).

These engagements included email correspondence, product briefings, follow-up discussions, and review of vendor-provided documentation. Outreach efforts focused on:

- Capability clarification
- Pricing models and licensing structures
- Integration requirements with existing Agency infrastructure
- Roadmap discussions for future product enhancements

The Agency's Market Research Approach Leveraged/Summary of Methodology:

- Firsthand product evaluations through multiple vendor demonstrations
- Exposure to industry-leading solutions and trends through RSA Conference participation

- Direct vendor engagement and iterative discussions to validate capabilities and refine requirements.

This combination of activities provided a comprehensive understanding of available commercial solutions, enabling the Agency to assess both current capabilities and future trends in security awareness and phishing defense technologies.

The most suitable procurement method is a sole-source award to Adaptive Security. Based on our market research, Adaptive Security is the only vendor that fully meets all the agency's requirements. Among the vendors reviewed, Adaptive Security is the only vendor that offers e-mail phishing Platform, spear phishing, OSINT support, voice phishing, deep fake simulation, and SMS phishing. Please see the chart below for an overview of Adaptive Security and other vendors.

	SANs	Proofpoint	Arctic Wolf	Living Security	Abnormal	Adaptive Security
E-mail Phishing Platform	Yes	Yes	Yes	Yes	Yes	Yes
Spear phishing	No	Yes	Yes	No	Yes	Yes
OSINT Support	No	No	No	No	Yes	Yes
Voice Phishing	No	No	Yes	Yes	Yes	Yes
Deep Fake Simulation	No	No	No	No	No	Yes
SMS Phishing	No	Yes	No	Yes	No	Yes

VI. DESCRIPTION OF EFFORTS MADE TO ENSURE THAT OFFERS ARE SOLICITED FROM AS MANY POTENTIAL SOURCES AS PRACTICABLE
See section V.

VII. DETERMINATION BY THE CONTRACTING OFFICER THAT THE ANTICIPATED COST TO THE GOVERNMENT WILL BE FAIR AND REASONABLE
By analyzing the proposed prices, inclusive of any offered discounts, and comparing the submissions against prices previously paid for these memberships, the Contracting Officer will confirm that the proposed prices are fair and reasonable prior to acceptance.

VIII. DESCRIPTION OF MARKET RESEARCH CONDUCTED AND THE RESULTS, OR A STATEMENT OF THE REASONS MARKET RESEARCH WAS NOT CONDUCTED
See section V.

IX. ANY OTHER FACTS SUPPORTING THE USE OF OTHER THAN FULL AND OPEN COMPETITION
None.

X. LIST OF SOURCES, IF ANY, THAT EXPRESSED INTEREST IN THE PROCUREMENT
Not applicable.

XI. STATEMENT OF THE ACTIONS, IF ANY, THE AGENCY MAY TAKE TO REMOVE OR OVERCOME ANY BARRIERS TO COMPETITION BEFORE MAKING SUBSEQUENT PROCUREMENTS
OTS/ITSMD will re-evaluate Security Awareness and Simulation Tool future industry developments to determine if other options become available for future procurements

Attachment C: Price Schedule.

Adaptive Security's Real-Time Reporting And Analytics				
Adaptive Security's Description of Products/Services	**Period of Performance**	**Quantity**	Unit Price	**Quoted Price**
Voice Phishing	*Base Year Only.*	250	$	$
Adaptive Elite		425	$	$
SMS Phishing		250	$	$
			TOTAL	$