SOLICITATION DOCUMENT

American Consulate General
Jeddah, Saudi Arabia
Contracting and Procurement Office

FCS VPN DIA Dedicated Internet Services

Solicitation No. 19SA4026R0011

American Consulate General, Jeddah
PO Box 149
Jeddah 21411
Saudi Arabia

TABLE OF CONTENTS

Section 1 - The Schedule

- SF 1449 cover sheet
- Continuation To SF-1449, RFP Number 19SA4026R0011**,** Prices, Block 23
- Continuation To SF-1449, RFP Number 19SA4026R0011*,* Schedule Of Supplies/Services, Block 20 Description/Specifications/Work Statement

Section 2 - Contract Clauses

- Contract Clauses
- Addendum to Contract Clauses - FAR and DOSAR Clauses not Prescribed in Part 12

Section 3 - Solicitation Provisions

- Solicitation Provisions
- Addendum to Solicitation Provisions - FAR and DOSAR Provisions not Prescribed in Part 12
- Cybersecurity Supply Chain Risk Management (C-SCRM) Software Producer Attestation Form

Section 4 - Evaluation Factors

- Evaluation Factors
- Addendum to Evaluation Factors - FAR and DOSAR Provisions not Prescribed in Part 12

Section 5 - Offeror Representations and Certifications

- Offeror Representations and Certifications
- Addendum to Offeror Representations and Certifications - FAR and DOSAR Provisions not Prescribed in Part 12

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

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

1. REQUISITION NUMBER	PAGE 1 OF
PR16129995	98

2. CONTRACT NUMBER	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
			19SA4026R0011	7/30/2026

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER *(No collect calls)*	8. OFFER DUE DATE/ LOCAL TIME
	Steven Workoff	+966(12)220 5000	8/20/2026 5PM

9. ISSUED BY — CODE 19SA40

Contracting Officer
American Consulate General
Jeddah, Saudi Arabia
Tel: +966- 12-2205000

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): 517111 - 532490
SIZE STANDARD:

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 19SA40

American Consulate General
Jeddah, Saudi Arabia

16. ADMINISTERED BY — CODE 19SA40

Same as Block 9.

17a. CONTRACTOR/ OFFEROR — CODE ____ FACILITY CODE ____

TELEPHONE NUMBER

18a. PAYMENT WILL BE MADE BY — CODE 19SA40

American Consulate General
Management Office
Jeddah, Saudi Arabia
Email: JeddahDBO@state.gov

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

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

19. ITEM NUMBER	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	FCS Dedicated Internet VPN Circuit Service See details below. *(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 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

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

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED
		Steven Workoff	7/30/2026

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 11/2021)
Prescribed by GSA - FAR (48 CFR) 53.212

SECTION 1 - THE SCHEDULE

CONTINUATION TO SF-1449, RFP NUMBER 19SA4026R0011
PRICES BLOCK 23

I. SCOPE OF SERVICES

The Contractor shall complete all work, including furnishing all labor, material, equipment, and services, unless otherwise specified herein, required under this contract for stated services within the time specified herein. The price listed below shall include all labor, materials, overhead, and profit. In consideration of satisfactory performance of all scheduled services required under this contract, the Contractor shall be paid a firm fixed-price for all services.

II. PERIOD

The contract will be for a one-year period from the date of the contract award and a notice to proceed with ***2*** option years.

1. The Contractor shall furnish all engineering, labor, tools, equipment, materials, supplies and services to provide the required circuit as specified under Section 1, hereof:

2. Prices. In consideration of satisfactory performance of the services required under this contract, the Contractor shall be paid a firm fixed-price (FFP) per month as stated in the schedule below in SAR (Saudi Arabian Riyals). Carrier shall be responsible for payment end-to-end circuit billing.

2.1 VALUE ADDED TAX

VALUE ADDED TAX. Value Added Tax (VAT) is not included in the CLIN rates. Instead, it will be priced as a separate Line Item in the contract and on Invoices. Local law dictates the portion of the contract price that is subject to VAT; this percentage is multiplied only against that portion. It is reflected for each performance period. The portions of the solicitation subject to VAT are:

2.2 The firm fixed-prices are in ***SAR (Saudi Arabian Riyals) OR USD (United States Dollar***

2.2.1 BASE YEAR:

CLIN 0001	Sub CLIN #	Description of Services	Number of Months	Monthly Price	Total Firm-Fixed Price
	1 (NAICS 517111 532490)	**FCS - VPN** DIA (VPN through the Internet) at the US Consulate Compound at Mohammedia District in Jeddah, Saudi Arabia. One (1) dedicated Internet channel at minimum **10240 Kbps (10 Mbps)** providing fault tolerance in the last mile.. HSRP protocol is required. **Price shall include ISP and Lease circuit.**	12		
	2	**Initial Installation** (once off)			
				SUB-TOTAL	
				VAT 15%	
				CLIN 0001 GRAND TOTAL	

2.2.2 OPTION YEAR 1:

CLIN 1001	Sub CLIN #	Description of Services	Number of Months	Monthly Price	Total Firm-Fixed Price
	1 (NAICS 517111 532490)	**FCS - VPN** DIA (VPN through the Internet) at the US Consulate Compound at Mohammedia District in Jeddah, Saudi Arabia. One (1) dedicated Internet channel at minimum **10240 Kbps (10 Mbps)** providing fault tolerance in the last mile.. HSRP protocol is required. **Price shall include ISP and Lease circuit.**	12		
	2	**Initial Installation** (once off)			
				SUB-TOTAL	
				VAT 15%	
				CLIN 1001 GRAND TOTAL	

2.2.3 OPTION YEAR 2:

CLIN 2001	Sub CLIN #	Description of Services	Number of Months	Monthly Price	Total Firm-Fixed Price
	1 (NAICS 517111 532490)	**FCS - VPN** DIA (VPN through the Internet) at the US Consulate Compound at Mohammedia District in Jeddah, Saudi Arabia. One (1) dedicated Internet channel at minimum **10240 Kbps (10 Mbps)** providing fault tolerance in the last mile.. HSRP protocol is required. **Price shall include ISP and Lease circuit.**	12		
	2	**Initial Installation** (once off)			
				SUB-TOTAL	
				VAT 15%	
				CLIN 2001 GRAND TOTAL	

2.2.4 52-217-8 OPTION TO EXTEND SERVICES:

Offerors are encouraged to complete the following pricing table for FAR Clause 52.217-8 Option to Extend Services for 6 months. The cost/price information provided will also be used to evaluate total price for all options (52.217-5) to the total price for the basic requirement ONLY. The price offered in the table below will not be included in the total contract award amount; however, if you choose not to provide any cost/price information for each line item below, your Price Proposal will be considered incomplete, labeled as failure to follow instructions, and no further consideration will be given.

CLIN 3001	Sub CLIN #	Description of Services	Number of Months	Monthly Price	Total Firm-Fixed Price
	1 (NAICS 517111 532490)	**FCS - VPN** DIA (VPN through the Internet) at the US Consulate Compound at Mohammedia District in Jeddah, Saudi Arabia. One (1) dedicated Internet channel at minimum **10240 Kbps (10 Mbps)** providing fault tolerance in the last mile.. HSRP protocol is required. **Price shall include ISP and Lease circuit.**	6		
	2	**Initial Installation** (once off)			
				SUB-TOTAL	
				VAT 15%	
				CLIN 3001 GRAND TOTAL	

2.2.5 GRAND TOTAL:

GRAND TOTAL CONTRACT PRICE, INCLUDING ALL OPTION YEARS	
Base Period Total Price (CLIN 0001)	
First Option Year Total Price (CLIN 1001)	
Second Option Year Total Price (CLIN 2001)	
52.217-8 (6 Months) (CLIN 3001)	
GRAND TOTAL FIRM-FIXED PRICE FOR BASE YEAR PLUS ALL OPTIONS	

End of Price Table

CONTINUATION TO SF-1449, RFP NUMBER 19SA4026R0011
SCHEDULE OF SUPPLIES/SERVICES, BLOCK 20 DESCRIPTION/SPECIFICATIONS/WORK STATEMENT

I SCOPE OF WORK

The purpose of this firm fixed price contract is to obtain VPN, DIA Internet Services, and Circuitry for **FCS office** (Foreign Commercial Services) located at the **U.S. Consulate General in Jeddah.**

The local Telecommunication's Internet Service Provider (ISP) contracting firm must provide internet services and dedicated leased line channels and circuitry for connecting American Consulate General in **Jeddah** and remote U.S. Consulate Annex locations data links as shown below in this technical paper.

CLIN#1 DIA – FCS Office

SERVICE: FCS VPN	
NAME:	**FCS** (VPN through the Internet) at the **U.S. Consulate General Jeddah**
DESCRIPTION:	One (1) dedicated Internet channel at minimum 10 MBPS, providing fault tolerance in the last mile. HSRP protocol is required.
TYPE OF SERVICE:	Dedicated Internet Channel Fiber
LOCATION:	**American Consulate General, Al Safa Street, Jeddah**

THE PROVIDED INTERNET SERVICE SHALL COMPLY WITH THE FOLLOWING REQUIREMENTS:

Internet Services Quality

Internet Service Provider (ISP) shall provide dedicated (not shared or bundled) leased channel high-speed access to the Internet; data transport media must be fiber optic, terrestrial connectivity. Twenty-four (24) hours uplink. Post Internet Service Provider (ISP) connection must be "always on" with unlimited usage, and must not require the installation of any custom software on the client side.

Internet Service Provider (ISP) digital bandwidth is the amount or volume of data that may be sent through the channel, measured in kilobits per second (Kbps), without distortion. Required Bandwidth connection is defined in each service description.

For Internet Services the Internet Service Provider (ISP) must guarantee full contracted bandwidth availability 24X7X365 from the originator side to the ISP's internet gateway. Bandwidth sharing between other non-Consulate customers is not allowed. Connection Ratio must be 1/1.

Internet Service or data service transmission from the originating information server towards an end server is referred to as downstream; and a transmission from an end user towards the remote server is referred as upstream; Post Internet Service Provider (ISP) Contention Ratio (downstream / upstream) must be 1:1 /1:1.

Internet Service Provider (ISP) must provide excellent Quality of Service (QOS) for the connection, that represents the level of consistent download capacity provided, must be the higher QOS percentage possible but, at minimum, greater than 99.97% or the highest possible quality of service connection reaching 100%.

The ISP must provide a symmetrical internet connection, allowing upload and download data transfers simultaneously at the same speed.

Internet Service Provider (ISP) connection must NOT, *repeat*, NOT use Network Address Translation (NAT).

Internet Service Provider (ISP) Round Trip Time (RTT) reports the total time in milliseconds (ms) time to send a small data packet and obtain a reply back; must be the faster than 100ms for the Round Trip Time (RTT) for internet service. Also, RTT must be faster than 7ms for local data services (for instance: point-to-point channels or web pages accessed through the **Saudi** Network Access Point (NAP).

Internet Service Provider (ISP) must permit the transit of all Internet Protocol (IP) protocols (especially IPSec), including but not limited to, User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and IPSEC to transit without filters or proxies. Unfiltered access to the Internet is required without ISP firewall blocking. Filters or sniffers must not be established, connected, or introduced by the ISP for any Consulate channels. If there are any existing filters, sniffers, restrictions, or proxies, they must be identified, and removed prior lease line circuit installation.

Internet Service Provider (ISP) must permit installation of Customer VPN encryption devices on circuit.

Internet Service Provider (ISP) must provide detailed network topology map that shows all possible paths ISP use for the internet traffic between ISP hub in **Jeddah** and the ISP hub in United States of America (USA).

Internet Service Provider (ISP) must have redundancy in the Internet backbone between **Saudi Arabia** and USA. For instance, If NAP of the host country's backbone fail, NAP Americas, NAP Sprint, or any other alternate backbone paths shall be available.

Internet Service Provider (ISP) must provide fault-tolerance Fiber Optic connectivity to the very end at the **U.S. Consulate General compound** Telecommunications Service Entrance Facilities (TSEF) Room.

Network Identification

Internet Service Provider (ISP) must provide a block of sixteen (16) public internet IP addresses on a single subnet for Internet services.

Internet Service Provider (ISP) must provide IP addresses used to identify the single subnet address in Classless Inter-Domain Routing address specification (Network IP address / 28) or, equivalently, its subnet mask 255.255.255.240, and ISP Gateway IP addresses (virtual IP addresses).

Network Devices
The network devices shall comply with the following characteristics:

Internet Service Provider (ISP) must permit ping and trace route traffic from 169.252.0.0/16 and 169.253.0.0/16 to the ISP connection RJ45 10/100BaseT router interface which terminates Customer VPN encryption device.

Services provided by the Internet Service Provider (ISP) must be delivered with RJ-45 interface connectors with a 10/100baseT interface.

Internet Service Provider (ISP) must provide routers and Data media converters or transmission devices in all cases.

Power standard sources must be dual voltage (110v/60hz and 220v/50hz)

Devices must be Rack mountable in a standard Commercial off-the-shelf (COTS) rack.

One separate or individual physical interface connector is required per service.

Service Support and Contingencies
The awarded ISP must warrant service support 7X24X365.

The vendor must warrant service support on site if necessary 7X24X365, services must be coordinated directly with Consulate's Contracting Office Representative (COR) or Information Technology (IT) representative from the Consulate Information Systems Center (ISC).

Expected service availability and reliability must be at minimum 99.97%.

The awarded ISP must have direct connection capability with major United States of America (U.S.A) telecommunication providers (ISPs) at Internet tier 1 level, having alternative line channels or backups in case of main Internet path malfunctioning.

The awarded ISP must provide on line web access data traffic analysis graphs capabilities. Graphs must be updated on a daily basis. Graphs must retain traffic history behavior for at least one year.

The awarded ISP must provide a central Information Technology (IT) point of contact (POC) in order to promptly coordinate technical issues during the initial installation.

II. GENERAL:

The Department of State has a requirement for one full period, full duplex, clear channels, and digital circuits capable of supporting synchronous traffic. Open net plus 46080 Kbps (45Mbps) & ITC 51200 Kbps (50Mbps), between the Main Distribution Frame [MDF] of U.S Consulate Jeddah and the Main Distribution Frame (MDF) STC (Saudi Telecom Company). For clear channel circuits, they shall be completely transparent to Open net plus 46080 Kbps (45Mbps) & ITC 51200 Kbps (50Mbps) data, with no bits added to or deleted from the bit stream provided to the interface of the Department of State equipment. The circuit shall be supplied for the transmission of a multiplexed aggregate bit stream for telegraphic and data signals.

These digital services shall be via Optic Fiber. The service shall be for the exclusive use of the Department of State, 24-hours per day, 7 days per week, and 52 weeks per year.

C. The Contractor shall coordinate the service and shall be responsible for the technical sufficiency of the circuit, including services necessary to establish, operate, and restore the circuit. Except for modems and terminal equipment furnished by the Government, the Contractor shall provide all equipment, materials, and supplies required to provide the service which includes the Data Service Unit (DSU) configured with Data Communications Equipment
(DCE) interface. If required, signal element timing shall be provided by the Contractor's facility.

D. The Contractor shall provide sufficient technical support to ensure uninterrupted End-to-end service between such terminal points as are covered in this contract. The Contractor shall provide, properly adjust, and maintain the circuit for continuous Department of State use. The Contractor shall ensure that the circuit complies with service changes, additions, or deletions as required under this contract.

E. RESERVE

F. RESERVE

G. The Contractor shall supply a Data Service Unit(s) (DSUs) configured with a Data Communications Equipment (DCE) interface. Signal element timing shall be provided as follows: (1) timing to the American Consulate will be provided by the Contractor's facility.

H. The Contractor shall use the following for interface standards:

OVERSEAS: RS-530 electrical/mechanical where available, or RS-422 electrical interface and RS-449 mechanical interface will be required between the DSU/CSU and the Department of State furnished equipment located at the **American Consulate Jeddah**

NOTE: Where applicable for digital service and for information purposes:

I. Services. This is a firm fixed-price contract for the lease of one full period, full duplex, clear channel, digital circuit capable of supporting synchronous data transfer. The circuit shall be completely transparent to 46080 Kbps (45Mbps) data, with no bits added to or deleted from the bit stream provided to the interface of the Department of State equipment. The circuit shall be supplied for the transmission of a multiplexed aggregate bit stream for telegraphic and data signals.

J. Bit Error Rate Test (BERT) The bit error rate (BER) for the service shall not be greater than 1 in 10 to the 6 bits for 99.7% of the time, for all time.

K. Acceptable Level of Performance. The Standard of Performance (SP) for this contract is 99.7% percent availability per month (100 percent less 0.3 percent each month for corrective and preventive maintenance).

L. Inspection and Acceptance. Unless specified in the Contract, the Government shall require a period not to exceed 24 hours in order to perform testing to determine acceptance of the required circuit under Section C. The U.S. destination point or the U.S. foreign post shall conduct the testing.

M. Term of Contract: The required circuits shall be installed and delivered to the Destination Point on or before 60 Days after Contract Award. Upon successful installation and acceptance by the Government of the required circuit under Section C, the Contractor shall be provided, in writing, notice to proceed and shall provide contractual services for a twelve (12) month period, commencing on the date specified in the notice to proceed.

N. The Contractor agrees that the work and services set forth in this contract shall be performed during the period commencing the effective date of this contract and shall continue through the end of the twelve month period of service (CLIN 1 through 8), excluding the exercise of any option.

P. An Invoice, suitable for payment, shall contain, but not limited to, the following information:

1. Name of Contractor;
2. Date of Invoice;
3. Original Invoice Number (Consecutive numbers);
4. Contract number;
5. Task or Delivery Order number, as applicable;
6. Government Specific Accounting and Appropriation Data (Funding Cite.) (Example: 19X0113-2015-X75041-180100-5327-2332);
7. Contract Line Item Number (CLIN) of item or service provided;
8. Description of the item, or service actually provided;
9. Period of performance of service or date item is provided;

10. Block/Space reserved for COR acceptance signature and date;
11. Signature, Name and Phone number of Company representative authorized to sign invoices;
12. Remit to address
13. Name, phone number and Mailing address to whom any disputed invoices should be addressed;
14. Credits with explanation and period covered.

Failure to submit Invoices which do not identify this information shall be returned without payment to the Contractor for correction.

R. Authorized Instruction to Contractor

a. No person or agency other than the Contracting Officer (CO) is authorized to give instruction, orders or directions on behalf of the Government to the Contractor or his employees, unless such person or agency is authorized in writing by the CO to so act. The authority of such person or agency is strictly limited to the written authorization provided by the CO. The duty is upon the Contractor to determine the authority of such person or agency. Any questions regarding the authority of such person or agency should be directed to the CO in writing.

b. Contracting Officer's Representative (COR): The CO may designate and authorize a representative(s) to act on his/her behalf under this contract. Such representative(s) as may be appointed shall be designated by a letter from the CO and a copy of the letter shall be given to the Contractor. The COR shall represent the CO as specified in his/her delegation of authority letter. The COR shall not be authorized to issue change orders or adjustments. Changes in the Scope of Work/Specifications or any increase or decrease in the work called for by this contract shall be made by the CO by an executed modification to this contract.

S. Government-Furnished Equipment (GFE): **None**

T. Release of Information

1. The Contractor's organization shall clear with the Information Office listed below any public release of information on this contract. This information includes news stories, articles, sales literature, advertisements, radio-TV spots, etc.

2. The request for public release of information should be addressed to***: PAO***

3. Limited Use of Data and Information. Performance of this contract may require the Contractor to access and use data and information proprietary to the Government agency or agency personnel, or which is of such a nature that its dissemination or use, other than in performance of this contract would be adverse to the interests of the Government or others. The Contractor and Contractor personnel shall not divulge or

release data or information developed or obtained in performance of this contract, until made public by the Government, except to authorize Government personnel or upon written approval of the Contracting Officer. The Contractor will not use, disclose, or reproduce proprietary data which bears a restrictive legend, other than as required in the performance of this contract. Nothing herein shall preclude the use of any data independently acquired by the Contractor without such limitations or prohibit an agreement at no costs to the Government between the Contractor and the data owner provides for greater rights to the Contractor.

U. Circuit Downtime and Credits

Credits shall be assessed against the Contractor in those instances where the circuit during any given month or year that fail to achieve and sustain the minimum acceptance standards stated above.

1. Definitions:

Circuit Availability Acceptance Level: Yearly Circuit Availability Acceptance Level is computed by 365 calendar days times 24 (hours per day) times 99.7% acceptance level equals 8,716.20 hours annum. (365 x 24 = 8760 x 99.7% = 8,733.72). Monthly Circuit Availability is computed by the calendar days per month times 24 (hours per day) times 99.7% acceptance level (example: 31 x 24 = 744 x 99.7% = 741.76).

Downtime: That period of time when the circuit becomes non-operational or unusable for communication or transfer of data or failures to meet the minimum acceptance standards. The maximum cumulative Annual downtime that shall be acceptable for corrective or preventative maintenance is 26.28 hours (8760 x .3%). The maximum cumulative Monthly downtime that shall be acceptable for corrective or preventative maintenance shall be .3% of the total available hours for the month (example: 31 x 24 = 744 x .3% = 2.23 hours).

Period of Downtime: Downtime shall commence at the time first attempt for contact is made by the Government (or its representative) to the Contractor's Point of Contact and shall be annotated on the Remedy Ticket and shall continue until the circuit is returned into Service by the Government.

Downtime Credits: Monetary value returned to the Government for failure to meet the Circuit availability requirements. Downtime Credits shall be assessed based on cumulative downtime time with the minimum assessment being one hour. Downtime credit shall be equal to the hourly or daily rate (as applicable) as identified in the schedule in Section B. There are two (2) situations when circuit Downtime Credits can be accumulated:

1) Below Availability Level,
2) Extended Downtime.

2. Credit for Circuit Downtime by Situation

Below Availability Level: If the downtime accumulated for a circuit adds up to 26.28 (8760 x 0.3%) cumulative hours or more during any one contract year (365 calendar days) or depending on the number of hours for the month (example 744 x .3%) cumulative hours per month (example: 31 calendar day month) the Contractor shall grant a hourly credit to the Government for each hour of downtime. Each additional one hour increment or portion thereof will be assessed as an additional hour.

Extended Downtime Credit(s): Cumulative time of more than 18 hours but not greater than 24 hours for any one outage shall be assessed at a daily rate. Any increment of 24 hours beyond the initial 24 hours of any one outage shall be assessed at the standards for the hourly rate up to 12 hours, however between 12 and 24 hours the credit shall be assessed at the daily rate.

3. Exceptions to Cumulating of Downtime

Cumulating of circuit downtime shall include all unscheduled downtime deemed to be the responsibility of the Contractor, with the following exceptions:

a. When the failure to perform arises out of causes beyond the control and without the fault or negligence of the Contractor or Sub-contractor as defined in the Termination for Default clause in Section I of this contract.

b. Malfunction of equipment, frequency fading and interference, errors of commission and/or omission by the Contractor or Sub-contractor, and commercial power surges or failures are considered to be normal hazards of the industry and therefore do not qualify as causes beyond the control of the Contractor or Sub-contractor. The Contractor shall be charged with credits for all reported outages determined "no trouble found" or "came clear while testing" but which exceed minutes.

The Contracting Officer shall make final determination as to whether downtime is the responsibility of the Contractor. If requested by the Contracting Officer, the Contractor shall provide documentation to support claims of excusable downtime. For downtime determined to be the Contractor's responsibility, the Contracting Officer may elect to assess a credit for each instance of non-performance.

4. Payment Reduction for Downtime Credits

When Circuit Downtime credit(s) is owed to the Government, the total number of creditable hours shall be accumulated for the month and will be deducted from the payment due the Contractor in the month they accrued.

5. Trouble Escalation Procedure

a. The Government shall refer the problem to the carrier after performing tests as prescribed in the Trouble Analysis procedure. Obtain the name of the carrier test person and a carrier ticket number; record this information on the Government's Remedy Ticket.

b. After the trouble has been referred to the carrier for two (2) hours, recall the carrier for an update on the current trouble. Record the carrier's response, the name of the individual you talked with, and the carrier ticket number on the Remedy Ticket.

c. After the trouble has been referred to the carrier for four (4) hours, recall the carrier for an update on the current trouble. If the carrier's response is not satisfactory escalate the trouble to the carrier's management. Record the carrier's response, the name of the individual you talked with, and the carrier ticket number on the Remedy Ticket.

d. After the trouble has been referred to the Contractor for six (6) hours the COR shall escalate the trouble to the Contractor's manager; also notify IRM/IMO and the Contracting Officer and the STATE IRM/ISC Office. Record the contractor's response, the name of the individual you talked with, the Contractor ticket number, and the names of the IRM managers that were notified on the Remedy Ticket.

e. Continue to status the Contractor for the remainder of the outage or until you have received a problem resolved status.

6. Technological Refreshment

After contract award, the Government may; pursuant to FAR clause 52.212-4 - Contract Terms and Conditions –Commercial Items, paragraph (c), Changes; request changes within the scope of the contract. These changes may be required to improve performance or react to changes in technology.

The Contractor may propose for the Government's technological refreshment, substitutions or additions for any provided products or services that may become available as a result of technological improvements. The Government may, at any time during the term of this contract or any extensions thereof, modify the contract to acquire products which are similar to those under the contract and that the Contractor has, or has not, formally announced for marketing purposes. This action is considered to be within the scope of the contract. At the option of the Government, a demonstration of the substitute product may be required. The Government is under no obligation to modify the contract in response to the proposed additions or substitutions.

Such substitutions or additions may include any part of, or all of, a given product(s) provided that the following conditions are met and substantiated by documentation in the technological refreshment proposal:

a. The proposed product(s) shall meet all of the technical specifications of this document and conform to the terms and conditions cited in the contract.

b. The proposed product(s) shall have the capacity, performance, or functional characteristics equal to or greater than, the current product(s).

c. The proposal shall discuss the impact on hardware, services, and delivery schedules. The cost of the changes not specifically addressed in the proposal shall be borne entirely by the Contractor.

d. Contractor has the right to withdraw, in whole or in part, any technological refreshment proposal prior to acceptance by the Government. Contractor will use commercially reasonable efforts to ensure that prices for substitutions or additions are comparable to replaced or discontinued products. If a technological refreshment proposal is accepted and made a part of this contract, an equitable adjustment, increasing or decreasing the contract price, may be required and any other affected provisions of this contract shall be made in accordance with FAR clause 52.212-4, paragraph (c), Changes, and other applicable clauses of the contract.

7. QUALITY ASSURANCE AND SURVEILLANCE PLAN (QASP)

This plan provides an effective method to promote satisfactory contractor performance. The QASP provides a method for the Contracting Officer's Representative (COR) to monitor Contractor performance, advise the Contractor of unsatisfactory performance, and notify the Contracting Officer of continued unsatisfactory performance. The Contractor, not the Government, is responsible for management and quality control to meet the terms of the contract. The role of the Government is to monitor quality to ensure that contract standards are achieved.

Performance Objective	Scope of Work Para	Performance Threshold
Services. Performs all **Internet / circuitary** services set forth in the scope of work.	1. thru 6.	All required services are performed and no more than one (1) customer complaint is received per month.

SECTION 2 - CONTRACT CLAUSES

52.212-4 CONTRACT TERMS AND CONDITIONS – COMMERCIAL ITEMS (NOV 2023) IS INCORPORATED BY REFERENCE. (SEE SF-1449, BLOCK 27A)

52.212-5 Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services. (OCT 2025)

As prescribed in 12.301(b)(4), insert the following clause:

Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services (Oct 2025)

(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:

_x_ (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.)

_x_ (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).

_x_ (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).

_x_ (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 (Jan 2025)(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).

_x_ (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 (DEVIATION FEB 2025)) ~~(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).

_x_ (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).

_x_ (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).

_x_ (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:

__ (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)

ADD THE FOLLOWING CLAUSE IN FULL TEXT:

52.229-12 TAX ON CERTAIN FOREIGN PROCUREMENTS—NOTICE AND REPRESENTATION (FEB 2021)

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

Foreign person means any person other than a United States person.

United States person, as defined in 26 U.S.C. 7701(a)(30), means–

(1) A citizen or resident of the United States;

(2) A domestic partnership;

(3) A domestic corporation;

(4) Any estate (other than a foreign estate, within the meaning of 26 U.S.C. 7701(a)(31)); and

(5) Any trust if-

(i) A court within the United States is able to exercise primary supervision over the administration of the trust; and

(ii) One or more United States persons have the authority to control all substantial decisions of the trust.

(b) This clause applies only to foreign persons. It implements 26 U.S.C. 5000C and its implementing regulations at 26 CFR 1.5000C-1 through 1.5000C-7.

(c)

(1) If the Contractor is a foreign person and has only a partial or no exemption to the withholding, the Contractor shall include the Department of the Treasury Internal Revenue Service Form W-14, Certificate of Foreign Contracting Party Receiving Federal Procurement Payments, with each voucher or invoice submitted under this contract throughout the period in which this status is applicable. The excise tax withholding is applied at the payment level, not at the contract level. The Contractor should revise each IRS Form W-14 submission to reflect the exemption (if any) that applies to that particular invoice, such as a different exemption applying. In the absence of a completed IRS Form W-14 accompanying a payment request, the default withholding percentage is 2 percent for the section 5000C withholding for that payment request. Information about IRS Form W-14 and its separate instructions is available via the internet at www.irs.gov/w14.

(2) If the Contractor is a foreign person and has indicated in its offer in the provision 52.229-11, Tax on Certain Foreign Procurements—Notice and Representation, that it is fully exempt from the withholding, and certified the full exemption on the IRS Form W-14, and if that full exemption no longer applies due to a change in circumstances during the performance of the contract that causes the Contractor to become subject to the withholding for the 2 percent excise tax then the Contractor shall–

(i) Notify the Contracting Officer within 30 days of a change in circumstances that causes the Contractor to be subject to the excise tax withholding under 26 U.S.C. 5000C; and

(ii) Comply with paragraph (c)(1) of this clause.

(d) The Government will withhold a full 2 percent of each payment unless the Contractor claims an exemption. If the Contractor enters a ratio in Line 12 of the IRS Form W-14, the result of Line 11 divided by Line 10, the Government will withhold from each payment an amount equal to 2 percent multiplied by the contract ratio. If the Contractor marks box 9 of the IRS Form W-14 (rather than completes Lines 10 through 12), the Contractor must identify and enter the specific exempt and nonexempt amounts in Line 15 of the IRS Form W-14; the Government will then withhold 2 percent only from the nonexempt amount. See the IRS Form W-14 and its instructions.

(e) Exemptions from the withholding under this clause are described at 26 CFR 1.5000C-1(d)(5) through (7). Any exemption claimed and self-certified on the IRS Form W-14 is subject to audit by the IRS. Any disputes regarding the imposition and collection of the 26 U.S.C. 5000C tax are adjudicated by the IRS as the 26 U.S.C. 5000C tax is a tax matter, not a contract issue.

(f) Taxes imposed under 26 U.S.C. 5000C may not be—

(1) Included in the contract price; nor

(2) Reimbursed.

(g) A taxpayer may, for a fee, seek advice from the Internal Revenue Service (IRS) as to the proper tax treatment of a transaction. This is called a private letter ruling. Also, the IRS may publish a revenue ruling, which is an official interpretation by the IRS of the Internal Revenue Code, related statutes, tax treaties, and regulations. A revenue ruling is the conclusion of the IRS on how the law is applied to a specific set of facts. For questions relating to the interpretation of the IRS regulations go to https://www.irs.gov/help/tax-law-questions.

(End of clause)

Cybersecurity Supply Chain Risk Management Requirements (FEB 2023)
(a)Definitions. As used in this clause:

Covered article - The term "covered article" includes-
(1)"Information and Communications technology" which means-

(i)any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use of that equipment, or of that equipment to a significant extent in the performance of a service or the furnishing of a product.

(ii)computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; however, does not include any equipment acquired by a federal contractor incidental to a federal contract.

(2)"Telecommunications Equipment", which means equipment, other than customer premises equipment, used by a carrier to provide telecommunications services, and includes software integral to such equipment (including upgrades).

(3)"Telecommunications Service", which means the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.

(4)“Cybersecurity Supply Chain Risk”, which means the risk that a person may sabotage, maliciously introduce unwanted function, extract data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, maintenance, disposition, or retirement of covered articles to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the covered articles or information stored or transmitted on the covered articles.

(b)Contractor Cybersecurity Supply Chain Risk Management Responsibilities. The Contractor shall take all prudent actions and comply with all Government direction (as identified in paragraph (c)) to regularly identify, assess, monitor, and mitigate cybersecurity supply chain risks when providing covered articles or services affecting covered articles to the Government. The Contractor shall maintain artifacts that document its compliance with this paragraph and shall provide these artifacts to the Government within 48 hours of request.

(c) Supporting Government Cybersecurity Supply Chain Risk Assessments. The Government may perform a cybersecurity supply chain risk assessment at any time during contract administration to identity, assess, and monitor the cyber risks of the Contractor's supply chain. The Contractor agrees that the Government may, at its own discretion, perform on-site assessments to collect information for the cybersecurity supply chain risk assessment. In performing the cybersecurity supply chain risk assessment, the Government may review any information provided by the Contractor, along with any other information available to the Government from public, unclassified, classified, or any other sources. Examples of information that the Government may collect for the cybersecurity supply chain risk assessment includes the following:

1. Functionality and features of covered articles, including access to data and information system privileges.
2. The user environment where a covered article is used or installed.
3. The ability of a source to produce and deliver covered articles as expected.
4. Foreign control of, or influence over, a source or covered article (e.g., foreign ownership, personal and professional ties between a source and any foreign entity or legal regime of any foreign country in which a source is headquartered or conducts operations).
5. Implications to Government mission(s) or assets, national security, homeland security, or critical functions associated with use of a source or covered article.
6. Vulnerability of Federal systems, programs, or facilities.
7. Market alternatives to the covered source.
8. Potential impact or harm caused by the possible loss, damage, or compromise of a

product, material, or service to an organization's operations or mission.
9. Likelihood of a potential impact or harm, or the exploitability of a system.
10. Security standards of the supplier as demonstrated by cooperation with assessments.
11. Security, authenticity, and integrity of covered articles and their supply and compilation chain.
12. Capacity to mitigate risks identified.
13. Factors that could lead to inability of the supplier to provide security updates.
14. Factors that may reflect upon the reliability of other supply chain risk information.
15. Any other considerations that would factor into an analysis of the security, integrity, resilience, quality, trustworthiness, or authenticity of covered articles or sources.

(d) Non-Destructive and Destructive Testing. The Government may engage in non-destructive and/or destructive testing of any information system, equipment, and software to determine whether it will negatively affect the security or performance of a Department of State information system.

(e) Novation Agreement Notice. FAR 42.1203 require Government approval of novation agreements. For proposed novation agreements for this contract, the Contractor shall provide any information requested by the Government regarding the proposed successor's identity and information regarding its supply chain.

(f) Software Bill of Materials (SBOM) Requests. For software, within 10 business days of request by a Department of State representative, the Contractor shall submit a SBOM to a designated representative. This request may be requested on one (1) or more occasions and shall be delivered at no increase in contract price.

(g) SBOM Sharing Notice. The Contractor consents to the sharing of its SBOM data with other contractors, such as tool solution providers, for the sole purpose of mapping against known vulnerabilities.

(h) Notification procedures for cybersecurity supply chain events. When cybersecurity supply chain events occur, the Contractor must contact the Contracting Officer or his/her designee within 12 hours of the event.

(i) Subcontracts. The Contractor shall insert the substance of this clause in all subcontracts and other contractual instruments in support of this contract.

(j) Vulnerability Exploitability eXchange (VEX). The Contractor is required to notify the Department of any discovered software vulnerabilities within 12 hours. Within three (3) days, they shall provide a report using a VEX format.

(k) Attestation following Major Version Change. Critical Software, as defined by National Institute for Science and Technology (NIST) Guidance, that is provided by the Contractor or subcontractors and is modified during the contract's period of performance by a major version change (e.g., using a semantic versioning schema of Major.Minor.Patch, the software version number goes from 2.5 to 3.0) requires a new self-attestation. For indefinite delivery contract vehicles, this self-attestation must be provided for all critical software available for ordering on the contract vehicle when the software is modified during the contract vehicle's ordering period of performance by a major version change. The Contractor shall either (i) post the new attestation in a publicly available internet location within 15 days of the major version change and provide the COR, or Contracting Officer if a COR is not appointed, with the internet link or
(ii) shall contact the COR, or Contracting Officer if a COR is not appointed, and request the agency's current software self-attestation form and submit it to the Government within 15 days of the major version change. The self-attestation form will contain the following elements: (i) the software producer's name; (ii) a description of which product or products the statement refers to including the number of the major version change; and (iii) a statement attesting that the software producer follows secure development practices and tasks consistent with NIST Guidance.

(end of clause)

ADDENDUM TO CONTRACT CLAUSES
FAR AND DOSAR CLAUSES NOT PRESCRIBED IN PART 12

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. In addition, the full text of a clause may be accessed electronically at: Acquisition.gov this address is subject to change.

If the Federal Acquisition Regulation (FAR) is not available at the location indicated above, use the Department of State Acquisition website at e-CFR to see the links to the FAR. You may also use an Internet "search engine" (for example, Google, Yahoo or Excite) to obtain the latest location of the most current FAR.

THE FOLLOWING FEDERAL ACQUISITION REGULATIONS (FAR) CLAUSES ARE INCORPORATED BY REFERENCE:

CLAUSE	TITLE AND DATE
52.204-9	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (JAN 2011)
52.204-13	SYSTEM FOR AWARD MANAGEMENT MAINTENANCE (OCT 2018)
52.204-18	COMMERCIAL AND GOVERNMENT ENTITY CODE MAINTENANCE (AUG 2020)
52.204-25	PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (NOV 2021)
52.216-20	Definite Quantity (OCT 1995).
52.225-14	INCONSISTENCY BETWEEN ENGLISH VERSION AND TRANSLATION OF CONTRACT (FEB 2000)
52.225-19	CONTRACTOR PERSONNEL IN A DESIGNED OPERATIONAL AREA OR SUPPORTING A DIPLOMATIC MISSION OUTSIDE THE UNITED STATES (MAY 2020)
52.228-3	WORKERS' COMPENSATION INSURANCE (DEFENSE BASE ACT) (JUL 2014)
52.228-4	WORKER'S COMPENSATION AND WAR-HAZARD INSURANCE OVERSEAS (APRIL 1984)

52.228-5 INSURANCE - WORK ON A GOVERNMENT INSTALLATION (JAN 1997)

52.229-6 TAXES - FOREIGN FIXED PRICE CONTRACTS (FEB 2013)

52.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (JUNE 2013)

52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (MAR 2023)

52.244-6 SUBCONTRACTS FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (JAN 2025)

THE FOLLOWING FAR CLAUSES ARE PROVIDED IN FULL TEXT:

52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within the performance period of the contract.

(End of clause)

52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within the performance period of the contract or within 30 days after funds for the option year become available, whichever is later.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed ***36 months.***

(End of clause)

52.232-19 AVAILABILITY OF FUNDS FOR THE NEXT FISCAL YEAR (APR 1984)

Funds are not presently available for performance under this contract beyond September 30 of the current calendar year. The Government's obligation for performance of this contract beyond that date is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise for performance under this contract beyond September 30 of the current calendar year, until funds are made available to the Contracting Officer for performance and until the Contractor receives notice of availability, to be confirmed in writing by the Contracting Officer.

(End of clause)

THE FOLLOWING DOSAR CLAUSES ARE PROVIDED IN FULL TEXT:

652.204-70 DEPARTMENT OF STATE PERSONAL IDENTIFICATION CARD ISSUANCE (FEB 2015)

(a) The Contractor shall comply with the Department of State (DOS) Personal Identification Card Policy and Procedures for all employees performing under this contract who require frequent and continuing access to DOS facilities, or information systems. The Contractor shall insert the substance of this clause in all subcontracts when the subcontractor's employees will require frequent and continuing access to DOS facilities, or information systems.
(b) The DOS Personal Identification Card Policy and

CONTRACTOR IDENTIFICATION (JULY 2008)

Contract performance may require contractor personnel to attend meetings with government personnel and the public, work within government offices, and/or utilize government email.

Contractor personnel must take the following actions to identify themselves as non-federal employees:

1) Use an email signature block that shows name, the office being supported and company affiliation (e.g. "John Smith, Office of Human Resources, ACME Corporation Support Contractor");

2) Clearly identify themselves and their contractor affiliation in meetings;

3) Identify their contractor affiliation in Departmental e-mail and phone listings whenever contractor personnel are included in those listings; and

4) Contractor personnel may not utilize Department of State logos or indicia on business cards.

(End of clause)

652.215-70 EXAMINATION OF RECORDS

(a) With respect to matters related to this contract or a subcontract hereunder, the Department of State Office of the Inspector General, or an authorized representative, shall have upon request:
(1) Complete, prompt, and free access to all Contractor and Subcontractor files (in any format), documents, records, data, premises, and employees, except as limited by law; and

(2) The right to interview any current Contractor and Subcontractor personnel, individually and directly, with respect to such matters.

(b) This clause may not be construed to require the contractor or any subcontractor to create or maintain any record that the contractor or subcontractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(c) The Contractor shall insert a clause containing all the terms of this clause, including this paragraph (c), in all subcontracts under this contract other than acquisitions described in Federal Acquisition Regulation 15.209(b)(1).

652.225-71 SECTION 8(A) OF THE EXPORT ADMINISTRATION ACT OF 1979, AS AMENDED (AUG 1999)

(a) Section 8(a) of the U.S. Export Administration Act of 1979, as amended (50 U.S.C. 2407(a)), prohibits compliance by U.S. persons with any boycott fostered by a foreign country against a country which is friendly to the United States and which is not itself the object of any form of boycott pursuant to United States law or regulation. The Boycott of Israel by Arab League countries is such a boycott, and therefore, the following actions, if taken with intent to comply with, further, or support the Arab League Boycott of Israel, are prohibited activities under the Export Administration Act:

(1) Refusing, or requiring any U.S. person to refuse to do business with or in Israel, with any Israeli business concern, or with any national or resident of Israel, or with any other person, pursuant to an agreement of, or a request from or on behalf of a boycotting country;

(2) Refusing, or requiring any U.S. person to refuse to employ or otherwise discriminating against any person on the basis of race, religion, sex, or national origin of that person or of any owner, officer, director, or employee of such person;

(3) Furnishing information with respect to the race, religion, or national origin of any U.S. person or of any owner, officer, director, or employee of such U.S. person;

(4) Furnishing information about whether any person has, has had, or proposes to have any business relationship (including a relationship by way of sale, purchase, legal or commercial representation, shipping or other transport, insurance, investment, or supply) with or in the State of Israel, with any business concern organized under the laws of the State of Israel, with any Israeli national or resident, or with any person which is known or believed to be restricted from having any business relationship with or in Israel;

(5) Furnishing information about whether any person is a member of, has made contributions to, or is otherwise associated with or involved in the activities of any charitable or fraternal organization which supports the State of Israel; and,

(6) Paying, honoring, confirming, or otherwise implementing a letter of credit which contains any condition or requirement against doing business with the State of Israel.

(b) Under Section 8(a), the following types of activities are not forbidden ``compliance with the boycott," and are therefore exempted from Section 8(a)'s prohibitions listed in paragraphs (a)(1)-(6)

above:

(1) Complying or agreeing to comply with requirements:

(i) Prohibiting the import of goods or services from Israel or goods produced or services provided by any business concern organized under the laws of Israel or by nationals or residents of Israel; or,

(ii) Prohibiting the shipment of goods to Israel on a carrier of Israel, or by a route other than that prescribed by the boycotting country or the recipient of the shipment;

(2) Complying or agreeing to comply with import and shipping document requirements with respect to the country of origin, the name of the carrier and route of shipment, the name of the supplier of the shipment or the name of the provider of other services, except that no information knowingly furnished or conveyed in response to such requirements may be stated in negative, blacklisting, or similar exclusionary terms, other than with respect to carriers or route of shipments as may be permitted by such regulations in order to comply with precautionary requirements protecting against war risks and confiscation;

(3) Complying or agreeing to comply in the normal course of business with the unilateral and specific selection by a boycotting country, or national or resident thereof, of carriers, insurance, suppliers of services to be performed within the boycotting country or specific goods which, in the normal course of business, are identifiable by source when imported into the boycotting country;

(4) Complying or agreeing to comply with the export requirements of the boycotting country relating to shipments or transshipments of exports to Israel, to any business concern of or organized under the laws of Israel, or to any national or resident of Israel;

(5) Compliance by an individual or agreement by an individual to comply with the immigration or passport requirements of any country with respect to such individual or any member of such individual's family or with requests for information regarding requirements of employment of such individual within the boycotting country; and,

(6) Compliance by a U.S. person resident in a foreign country or agreement by such person to comply with the laws of that country with respect to his or her activities exclusively therein, and such regulations may contain exceptions for such resident complying with the laws or regulations of that foreign country governing imports into such country of trademarked, trade named, or similarly specifically identifiable products, or components of products for his or her own use, including the performance of contractual services within that country, as may be defined by such regulations.

(End of clause)

652.229-70 EXCISE TAX EXEMPTION STATEMENT FOR CONTRACTORS WITHIN THE UNITED STATES (JUL 1988)

This is to certify that the item(s) covered by this contract is/are for export solely for the use of the U.S. Foreign Service Post identified in the contract schedule.

The Contractor shall use a photocopy of this contract as evidence of intent to export. Final proof of exportation may be obtained from the agent handling the shipment. Such proof shall be accepted in lieu of payment of excise tax.

(End of clause)

652.232-70 PAYMENT SCHEDULE AND INVOICE SUBMISSION (FIXED-PRICE) (AUG 1999)

(a) General. The Government shall pay the Contractor as full compensation for all work required, performed, and accepted under this contract the firm fixed-price stated in this contract.

(b) Invoice Submission. The Contractor shall submit invoices in an original and copies to the office identified in Block 18b of the SF-1449. To constitute a proper invoice, the invoice shall include all the items required by FAR 32.905(e).

The Contractor shall show Value Added Tax (VAT) as a separate item on invoices submitted for payment.

(c) Contractor Remittance Address. The Government will make payment to the contractor's address stated on the cover page of this contract, unless a separate remittance address is shown below:

Attn: TO COR
JEDDAHDBO@STATE.GOV

(End of clause)

652.237-72 OBSERVANCE OF LEGAL HOLIDAYS AND ADMINISTRATIVE LEAVE (FEB 2015)

(a) The Department of State observes the following days as holidays:

New Year's Day
Martin Luther King's Birthday
Washington's Birthday
Memorial Day
Juneteenth
Independence Day

Labor Day
Columbus Day
Veterans Day
Thanksgiving Day
Christmas Day
Saudi Founding Day
Eid Al Fitr
Eid Al Adha
Saudi National Day

Any other day designated by Federal law, Executive Order, or Presidential Proclamation.

(b) When New Year's Day, Independence Day, Veterans Day or Christmas Day falls on a Sunday, the following Monday is observed; if it falls on Saturday the preceding Friday is observed. Observance of such days by Government personnel shall not be cause for additional period of performance or entitlement to compensation except as set forth in the contract. If the contractor's personnel work on a holiday, no form of holiday or other premium compensation will be reimbursed either as a direct or indirect cost, unless authorized pursuant to an overtime clause elsewhere in this contract.

(c) When the Department of State grants administrative leave to its Government employees, assigned contractor personnel in Government facilities shall also be dismissed. However, the contractor agrees to continue to provide sufficient personnel to perform round-the-clock requirements of critical tasks already in operation or scheduled, and shall be guided by the instructions issued by the contracting officer or his/her duly authorized representative.

(d) For fixed-price contracts, if services are not required or provided because the building is closed due to inclement weather, unanticipated holidays declared by the President, failure of Congress to appropriate funds, or similar reasons, deductions will be computed as follows:

(1) The deduction rate in dollars per day will be equal to the per month contract price divided by 21 days per month.

(2) The deduction rate in dollars per day will be multiplied by the number of days services are not required or provided.

If services are provided for portions of days, appropriate adjustment will be made by the contracting officer to ensure that the contractor is compensated for services provided.

(e) If administrative leave is granted to contractor personnel as a result of conditions stipulated in any "Excusable Delays" clause of this contract, it will be without loss to the contractor. The cost of salaries and wages to the contractor for the period of any such excused absence shall be a reimbursable item of direct cost hereunder for employees whose regular time is normally charged, and a reimbursable item of indirect cost for employees whose time is normally charged indirectly in accordance with the contractors accounting policy.

(End of clause)

652.242-70 CONTRACTING OFFICER'S REPRESENTATIVE (COR) AUG 1999)

(a) The Contracting Officer may designate in writing one or more Government employees, by name or position title, to take action for the Contracting Officer under this contract. Each designee shall be identified as a Contracting Officer's Representative (COR). Such designation(s) shall specify the scope and limitations of the authority so delegated; provided, that the designee shall not change the terms or conditions of the contract, unless the COR is a warranted Contracting Officer and this authority is delegated in the designation.

(a) The COR for this contract is **TBD**

(End of clause)

652.242-73 AUTHORIZATION AND PERFORMANCE (AUG 1999)

(a) The Contractor warrants the following:

(1) That is has obtained authorization to operate and do business in the country or countries in which this contract will be performed;

(2) That is has obtained all necessary licenses and permits required to perform this contract; and,

(3) That it shall comply fully with all laws, decrees, labor standards, and regulations of said country or countries during the performance of this contract.

(b) If the party actually performing the work will be a subcontractor or joint venture partner, then such subcontractor or joint venture partner agrees to the requirements of paragraph (a) of this clause.

652.243-70 NOTICES (AUG 1999)

Any notice or request relating to this contract given by either party to the other shall be in writing. Said notice or request shall be mailed or delivered by hand to the other party at the address provided in the schedule of the contract. All modifications to the contract must be made in writing by the Contracting Officer.

SECTION 3 - SOLICITATION PROVISIONS

52.212-1 INSTRUCTIONS TO OFFERORS -- COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (SEP 2023) IS INCORPORATED BY REFERENCE (SEE SF-1449, BLOCK 27A)

ADDENDUM TO 52.212-1

A. Summary of Instructions. Each offer must consist of the following:

A.1. A completed solicitation, in which the SF-1449 cover page (blocks 12, 17, 19-24, and 30 as appropriate), and Section 1 has been filled out.

The Offeror shall include Defense Base Act (DBA) insurance premium costs covering employees. The offeror may obtain DBA insurance directly from any Department of Labor approved providers at the DOL website at http://www.dol.gov/owcp/dlhwc/lscarrier.htm]

A.2. Information demonstrating the offeror's ability to perform, including:

(1) Name of a Project Manager (or other liaison to the Consulate who understands written and spoken English;

(2) Evidence that the offeror operates an established business with a permanent address and telephone listing***;*** in ***KSA*** or plans to establish an office within 30 days of contract award.

(3) The offeror shall provide proof of SAM registration to include the SAM UEI number.

(4) List of clients over the past Five years, demonstrating prior experience with relevant past performance information and references (provide dates of contracts, places of performance, value of contracts, contact names, telephone and fax numbers and email addresses). If the offeror has not performed comparable services in KSA then the offeror shall provide its international experience. Offerors are advised that the past performance information requested above may be discussed with the client's contact person. In addition, the client's contact person may be asked to comment on the offeror's:

- Quality of services provided under the contract;
- Compliance with contract terms and conditions;
- Effectiveness of management;
- Willingness to cooperate with and assist the customer in routine matters, and when confronted by unexpected difficulties; and
- Business integrity / business conduct.

The Government will use past performance information primarily to assess an offeror's capability to meet the solicitation performance requirements, including the relevance and successful performance of the offeror's work experience. The Government may also use this data to evaluate the credibility of the offeror's proposal. In addition, the Contracting Officer may use past performance information in making a determination of responsibility.

(5) Evidence that the offeror can provide the necessary personnel, equipment, and financial resources needed to perform the work;

(6) The offeror shall address its plan to obtain all licenses and permits required by local law (see DOSAR 652.242-73 in Section 2). If offeror already possesses the locally required licenses and permits, a copy shall be provided.

(7) The offeror's strategic plan for DIA VPN Dedicated Internet Services to include but not limited to:

(a) A work plan taking into account all work elements in Section 1, Performance Work Statement.
(b) Identify types and quantities of equipment, supplies and materials required for performance of services under this contract. Identify if the offeror already possesses the listed items and their condition for suitability and if not already possessed or inadequate for use how and when the items will be obtained;
(c) Plan of ensuring quality of services including but not limited to contract administration and oversight; and
(d) (1) If insurance is required by the solicitation, a copy of the Certificate of Insurance(s), **or** (2) a statement that the contractor will get the required insurance, and the name of the insurance provider to be used.

ADDENDUM TO SOLICITATION PROVISIONS
FAR AND DOSAR PROVISIONS NOT PRESCRIBED IN PART 12

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. In addition, the full text of a clause may be accessed electronically at Acquisition.gov this address is subject to change.

If the Federal Acquisition Regulation (FAR) is not available at the location indicated above, use the Department of State Acquisition website at e-CFR to see the links to the FAR. You may also use an Internet "search engine" (for example, Google, Yahoo or Excite) to obtain the latest location of the most current FAR.

THE FOLLOWING FEDERAL ACQUISITION REGULATION SOLICITATION PROVISIONS ARE INCORPORATED BY REFERENCE:

PROVISION TITLE AND DATE

52.204-7 SYSTEM FOR AWARD MANAGEMENT (NOV 2024)

52.204-16 COMMERCIAL AND GOVERNMENT ENTITY CODE REPORTING (AUG 2020)

52.209-7 INFORMATION REGARDING RESPONSIBILITY MATTERS (OCT 2018)

52.214-34 SUBMISSION OF OFFERS IN THE ENGLISH LANGUAGE (APR 1991)

52.222-56 CERTIFICATION REGARDING TRAFFICKING IN PERSONS (OCT 2020)

THE FOLLOWING FEDERAL ACQUISITION REGULATION SOLICITATION PROVISIONS IS/ARE PROVIDED IN FULL TEXT:

52.212-1 Instructions to Offerors—Commercial Products and Commercial Services.

As prescribed in 12.301(b)(1), insert the following provision:

Instructions to Offerors—Commercial Products and Commercial Services (Sep 2023)

(a) North American Industry Classification System (NAICS) code and small business size standard. The NAICS code(s) and small business size standard(s) for this acquisition appear elsewhere in the solicitation. However, the small business size standard for a concern that submits an offer, other than on a construction or service acquisition, but proposes to furnish an end item that it did not itself manufacture, process, or produce is 500 employees, or 150 employees for information technology value-added resellers under NAICS code 541519, if the acquisition—

(1)Is set aside for small business and has a value above the simplified acquisition threshold;

(2)Uses the HUBZone price evaluation preference regardless of dollar value, unless the offeror waives the price evaluation preference; or

(3)Is an 8(a), HUBZone, service-disabled veteran-owned, economically disadvantaged women-owned, or women-owned small business set-aside or sole-source award regardless of dollar value.

(b) Submission of offers. Submit signed and dated offers to the office specified in this solicitation at or before the exact time specified in this solicitation. Offers may be submitted on the SF 1449, letterhead stationery, or as otherwise specified in the solicitation. As a minimum, offers must show—

(1) The solicitation number;

(2) The time specified in the solicitation for receipt of offers;

(3) The name, address, and telephone number of the offeror;

(4) A technical description of the items being offered in sufficient detail to evaluate compliance with the requirements in the solicitation. This may include product literature, or other documents, if necessary;

(5) Terms of any express warranty;

(6) Price and any discount terms;

(7) "Remit to" address, if different than mailing address;

(8) A completed copy of the representations and certifications at Federal Acquisition Regulation (FAR) 52.212-3 (see FAR 52.212-3(b) for those representations and certifications that the offeror shall complete electronically);

(9) Acknowledgment of Solicitation Amendments;

(10) Past performance information, when included as an evaluation factor, to include recent and relevant contracts for the same or similar items and other references (including contract numbers, points of contact with telephone numbers and other relevant information); and

(11) If the offer is not submitted on the SF 1449, include a statement specifying the extent of agreement with all terms, conditions, and provisions included in the solicitation. Offers that fail to furnish required representations or information, or reject the terms and conditions of the solicitation may be excluded from consideration.

(c) Period for acceptance of offers. The offeror agrees to hold the prices in its offer firm for 30 calendar days from the date specified for receipt of offers, unless another time period is specified in an addendum to the solicitation.

(d) Product samples. When required by the solicitation, product samples shall be submitted at or prior to the time specified for receipt of offers. Unless otherwise specified in this solicitation, these samples shall be submitted at no expense to the Government, and returned at the sender's request and expense, unless they are destroyed during preaward testing.

(e) Multiple offers. Offerors are encouraged to submit multiple offers presenting alternative terms and conditions, including alternative line items (provided that the alternative line items are consistent with FAR subpart 4.10), or alternative commercial products or commercial services for satisfying the requirements of this solicitation. Each offer submitted will be evaluated separately.

(f) Late submissions, modifications, revisions, and withdrawals of offers. (1) Offerors are responsible for submitting offers, and any modifications, revisions, or withdrawals, so as to reach the Government office designated in the solicitation by the time specified in the solicitation. If no time is specified in the solicitation, the time for receipt is 4:30 p.m., local time, for the designated Government office on the date that offers or revisions are due.
(2) (i) Any offer, modification, revision, or withdrawal of an offer received at the Government office designated in the solicitation after the exact time specified for receipt of offers is "late" and will not be considered unless it is received before award is made, the Contracting Officer determines that accepting the late offer would not unduly delay the acquisition; and-
(A) If it was transmitted through an electronic commerce method authorized by the solicitation, it was received at the initial point of entry to the Government infrastructure not later than 5:00 p.m. one working day prior to the date specified for receipt of offers; or

(B) There is acceptable evidence to establish that it was received at the Government installation designated for receipt of offers and was under the Government's control prior to the time set for receipt of offers; or

(C) If this solicitation is a request for proposals, it was the only proposal received.

(ii) However, a late modification of an otherwise successful offer, that makes its terms more favorable to the Government, will be considered at any time it is received and may be accepted.

(3) Acceptable evidence to establish the time of receipt at the Government installation includes the time/date stamp of that installation on the offer wrapper, other documentary evidence of receipt maintained by the installation, or oral testimony or statements of Government personnel.

(4) If an emergency or unanticipated event interrupts normal Government processes so that offers cannot be received at the Government office designated for receipt of offers by the exact time specified in the solicitation, and urgent Government requirements preclude amendment of the solicitation or other notice of an extension of the closing date, the time specified for receipt of offers will be deemed to be extended to the same time of day specified in the solicitation on the first work day on which normal Government processes resume.

(5) Offers may be withdrawn by written notice received at any time before the exact time set for receipt of offers. Oral offers in response to oral solicitations may be withdrawn orally. If the solicitation authorizes facsimile offers, offers may be withdrawn via facsimile received at any time before the exact time set for receipt of offers, subject to the conditions specified in the solicitation concerning facsimile offers. An offer may be withdrawn in person by an offeror or its authorized representative if, before the exact time set for receipt of offers, the identity of the person requesting withdrawal is established and the person signs a receipt for the offer.

(g) Contract award (not applicable to Invitation for Bids). The Government intends to evaluate offers and award a contract without discussions with offerors. Therefore, the offeror's initial offer should contain the offeror's best terms from a price and technical standpoint. However, the Government reserves the right to conduct discussions if later determined by the Contracting Officer to be necessary. The Government may reject any or all offers if such action is in the public interest; accept other than the lowest offer; and waive informalities and minor irregularities in offers received.

(h) Multiple awards. The Government may accept any item or group of items of an offer, unless the offeror qualifies the offer by specific limitations. Unless otherwise provided in the Schedule, offers may not be submitted for quantities less than those specified. The Government reserves the right to make an award on any item for a quantity less than the quantity offered, at the unit prices offered, unless the offeror specifies otherwise in the offer.

(i) Availability of requirements documents cited in the solicitation.

(1) (i) The GSA Index of Federal Specifications, Standards and Commercial Item Descriptions, FPMR Part 101–29, and copies of Federal specifications, standards, and product descriptions can be downloaded from the ASSIST website at https://assist.dla.mil.
(ii) If the General Services Administration, Department of Agriculture, or Department of Veterans Affairs issued this solicitation, a copy of specifications, standards, and commercial item descriptions cited in this solicitation may be obtained from the address in paragraph (i)(1)(i) of this provision.

(2) Most unclassified Defense specifications and standards may be downloaded from the ASSIST website at https://assist.dla.mil.

(3) Defense documents not available from the ASSIST website may be requested from the Defense Standardization Program Office by—

(i) Using the ASSIST feedback module (https://assist.dla.mil/feedback); or

(ii) Contacting the Defense Standardization Program Office by telephone at 571–767–6688 or email at assisthelp@dla.mil.

(4) Nongovernment (voluntary) standards must be obtained from the organization responsible for their preparation, publication, or maintenance.

(j) Unique entity identifier.(Applies to all offers that exceed the micro-purchase threshold, and offers at or below the micro-purchase threshold if the solicitation requires the Contractor to be registered in the System for Award Management (SAM).) The Offeror shall enter, in the block with its name and address on the cover page of its offer, the annotation "Unique Entity Identifier" followed by the unique entity identifier that identifies the Offeror's name and address. The Offeror also shall enter its Electronic Funds Transfer (EFT) indicator, if applicable. The EFT indicator is a four-character suffix to the unique entity identifier. The suffix is assigned at the discretion of the Offeror to establish additional SAM records for identifying alternative EFT accounts (see FAR subpart 32.11) for the same entity. If the Offeror does not have a unique entity identifier, it should contact the entity designated at www.sam.gov for unique entity identifier establishment directly to obtain one. The Offeror should indicate that it is an offeror for a Government contract when contacting the entity designated at www.sam.gov for establishing the unique entity identifier.

(k) [Reserved]

(l) Debriefing. If a post-award debriefing is given to requesting offerors, the Government shall disclose the following information, if applicable:

(1) The agency’s evaluation of the significant weak or deficient factors in the debriefed offeror’s offer.

(2) The overall evaluated cost or price and technical rating of the successful and the debriefed offeror and past performance information on the debriefed offeror.

(3) The overall ranking of all offerors, when any ranking was developed by the agency during source selection.

(4) A summary of the rationale for award;

(5) For acquisitions of commercial products, the make and model of the product to be delivered by the successful offeror.

(6) Reasonable responses to relevant questions posed by the debriefed offeror as to whether source-selection procedures set forth in the solicitation, applicable regulations, and other applicable authorities were followed by the agency.

(End of provision)

Addendum to 52.212-1

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT C-SCRM Proposal Instructions

Cybersecurity C-SCRM Questionnaire

The offeror shall include in its offer a completed C- SCRM Questionnaire and C-SCRM Software Producer Attestation Form, which shall be completed in accordance with the instructions. Failure to follow the instructions may result in rejection of the offer.

THE FOLLOWING DOSAR PROVISION(S) IS/ARE PROVIDED IN FULL TEXT:

652.206-70 ADVOCATE FOR COMPETITION/OMBUDSMAN (FEB 2015)

(a) The Department of State's Advocate for Competition is responsible for assisting industry in removing restrictive requirements from Department of State solicitations and removing barriers to full and open competition and use of commercial items. If such a solicitation is considered competitively restrictive or does not appear properly conducive to competition and commercial practices, potential offerors are encouraged first to contact the contracting office for the solicitation. If concerns remain unresolved, contact:

(1) For solicitations issued by the Office of Acquisition Management (A/GA/AMD) or a Regional Procurement Support Office, the A/GA/AMD Advocate for Competition, at AQMCompetitionAdvocate@state.gov.

(2) For all others, the Department of State Advocate for Competition at cat@state.gov.

(b) The Department of State's Acquisition Ombudsman has been appointed to hear concerns from potential offerors and contractors during the pre-award and post-award phases of this acquisition. The role of the ombudsman is not to diminish the authority of the contracting officer, the Technical Evaluation Panel or Source Evaluation Board, or the selection official. The purpose of the ombudsman is to facilitate the communication of concerns, issues, disagreements, and recommendations of interested parties to the appropriate Government personnel, and work to resolve them. When requested and appropriate, the ombudsman will maintain strict confidentiality as to the source of the concern. The ombudsman does not participate in the evaluation of proposals, the source selection process, or the adjudication of formal contract disputes. Interested parties are invited to contact the contracting activity ombudsman, **Robert Blakeslee** , at **blakesleere@state.gov** . For an American Embassy or overseas post, refer to the numbers below for the Department Acquisition Ombudsman. Concerns, issues, disagreements, and recommendations which cannot be resolved at a contracting activity level may be referred to the Department of State Acquisition Ombudsman at (703) 516-1696 or write to: Department of State, Acquisition Ombudsman, Office of Global Acquisitions (A/GA), Suite 1060, SA-15, Washington, DC 20520.
(End of provision)

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM) SOFTWARE PRODUCER ATTESTATION FORM

This form must be completed by the software producer.

ITEM NUMBER	ITEM DESCRIPTION	VENDOR RESPONSE
1.1	Enter the name of the software producer.	
1.2	Provide a statement attesting that the software products listed in Item Number 1.3 of this form follow the secure development "practices" and "tasks" identified in NIST SP 800-218. A summary of these practices and tasks are provided below for reference from NIST SP 800-218. If you cannot attest to all practices and tasks, identify the ones that you attest to and the ones that you cannot attest to. For those practices and tasks that you cannot attest to, describe the practices that you have in place to mitigate those risks (i.e., risks for practices or tasks you cannon attest to), and provide a Plan of Action & Milestones (POA&M) detailing how your firm will reach compliance for those non-compliant practices and tasks.	
1.3	A description of which product or products the statement provided for Item Number 1.2 refers to (preferably focused at the company or product line level and inclusive of all unclassified products sold to Federal agencies).	

NIST SP 800-218, Table 1: The Secure Software Development Framework (SSDF) Version 1.1

Practices	Tasks	Notional Implementation Examples	References
Define Security Requirements for Software Development (PO.1): Ensure that security requirements for software development are known at all times so that they can be taken into account throughout the SDLC and duplication of effort can be minimized because the requirements information can be collected once and shared. This includes requirements from internal sources (e.g., the organization's policies, business objectives, and risk management strategy) and external sources (e.g., applicable laws and regulations).	**PO.1.1**: Identify and document all security requirements for the organization's software development infrastructures and processes, and maintain the requirements over time.	Example 1: Define policies for securing software development infrastructures and their components, including development endpoints, throughout the SDLC and maintaining that security.	**BSAFSS**: SM.3, DE.1, IA.1, IA.2
		Example 2: Define policies for securing software development processes throughout the SDLC and maintaining that security, including for open-source and other third-party software components utilized by software being developed.	**BSIMM**: CP1.1, CP1.3, SR1.1, SR2.2, SE1.2, SE2.6
		Example 3: Review and update security requirements at least annually, or sooner if there are new requirements from internal or external sources, or a major security incident targeting software development infrastructure has occurred.	**EO14028**: 4e(ix)
		Example 4: Educate affected individuals on impending changes to requirements.	**IEC62443**: SM-7, SM-9 **NISTCSF**: ID.GV-3 **OWASPASVS**: 1.1.1 **OWASPMASVS**: 1.10 **OWASPSAMM**: PC1-A, PC1-B, PC2-A **PCISSLC**: 2.1, 2.2 **SCFPSSD**: Planning the Implementation and Deployment of Secure Development Practices **SP80053**: SA-1, SA-8, SA-15, SR-3 **SP800160**: 3.1.2, 3.2.1, 3.2.2, 3.3.1, 3.4.2, 3.4.3 **SP800161**: SA-1, SA-8, SA-15, SR-3 **SP800181**: T0414; K0003, K0039, K0044, K0157, K0168, K0177, K0211, K0260, K0261, K0262, K0524; S0010, S0357, S0368; A0033, A0123, A0151
	PO.1.2: Identify and document all security requirements for organization-developed software to meet, and maintain the requirements over time.	Example 1: Define policies that specify risk-based software architecture and design requirements, such as making code modular to facilitate code reuse and updates; isolating security components from other components during execution; avoiding undocumented commands and settings; and providing features that will aid software acquirers with the secure deployment, operation, and maintenance of the software.	**BSAFSS**: SC.1-1, SC.2, PD.1-1, PD.1-2, PD.1-3, PD.2-2, SI, PA, CS, AA, LO, EE
		Example 2: Define policies that specify the security requirements for the organization's software, and verify compliance at key points in the SDLC (e.g., classes of software flaws verified by gates, responses to vulnerabilities discovered in released software).	**BSIMM**: SM1.1, SM1.4, SM2.2, CP1.1, CP1.2, CP1.3, CP2.1, CP2.3, AM1.2, SFD1.1, SFD2.1, SFD3.2, SR1.1, SR1.3, SR2.2, SR3.3, SR3.4
		Example 3: Analyze the risk of applicable technology stacks (e.g., languages, environments, deployment models), and recommend or require the use of stacks that will reduce risk compared to others.	**EO14028**: 4e(ix)
		Example 4: Define policies that specify what needs to be archived for each software release (e.g., code, package files, third-party libraries, documentation, data inventory) and how long it needs to be retained based on the SDLC model, software end-of-life, and other factors.	**IEC62443**: SR-3, SR-4, SR-5, SD-4
		Example 5: Ensure that policies cover the entire software life cycle, including notifying users of the impending end of software support and the date of software end-of-life.	**ISO27034**: 7.3.2

		Example 6: Review all security requirements at least annually, or sooner if there are new requirements from internal or external sources, a major vulnerability is discovered in released software, or a major security incident targeting organization-developed software has occurred.	**MSSDL**: 2, 5
		Example 7: Establish and follow processes for handling requirement exception requests, including periodic reviews of all approved exceptions.	**NISTCSF**: ID.GV-3 **OWASPMASVS**: 1.12 **OWASPSAMM**: PC1-A, PC1-B, PC2-A, PC3-A, SR1-A, SR1-B, SR2-B, SA1-B, IR1-A **PCISSLC**: 2.1, 2.2, 2.3, 3.3 **SCFPSSD**: Establish Coding Standards and Conventions **SP80053**: SA-8, SA-8(3), SA-15, SR-3 **SP800160**: 3.1.2, 3.2.1, 3.3.1 **SP800161**: SA-8, SA-15, SR-3 **SP800181**: T0414; K0003, K0039, K0044, K0157, K0168, K0177, K0211, K0260, K0261, K0262, K0524; S0010, S0357, S0368; A0033, A0123, A0151
	PO.1.3: Communicate requirements to all third parties who will provide commercial software components to the organization for reuse by the organization's own software. [Formerly PW.3.1]	Example 1: Define a core set of security requirements for software components, and include it in acquisition documents, software contracts, and other agreements with third parties.	**BSAFSS**: SM.1, SM.2, SM.2-1, SM.2-4
		Example 2: Define security-related criteria for selecting software; the criteria can include the third party's vulnerability disclosure program and product security incident response capabilities or the third party's adherence to organization-defined practices.	**BSIMM**: CP2.4, CP3.2, SR2.5, SR3.2
		Example 3: Require third parties to attest that their software complies with the organization's security requirements.	**EO14028**: 4e(vi), 4e(ix)
		Example 4: Require third parties to provide provenance data and integrity verification mechanisms for all components of their software.	**IDASOAR**: 19, 21
		Example 5: Establish and follow processes to address risk when there are security requirements that third-party software components to be acquired do not meet; this should include periodic reviews of all approved exceptions to requirements.	**IEC62443**: SM-9, SM-10 **MSSDL**: 7 **NISTCSF**: ID.SC-3 **OWASPSAMM**: SR3-A **SCAGILE**: Tasks Requiring the Help of Security Experts 8 **SCFPSSD**: Manage Security Risk Inherent in the Use of Third-Party Components **SCSIC**: Vendor Sourcing Integrity Controls **SP80053**: SA-4, SA-9, SA-10, SA-10(1), SA-15, SR-3, SR-4, SR-5 **SP800160**: 3.1.1, 3.1.2 **SP800161**: SA-4, SA-9, SA-9(1), SA-9(3), SA-10, SA-10(1), SA-15, SR-3, SR-4, SR-5 **SP800181**: T0203, T0415; K0039; S0374; A0056, A0161
Implement Roles and Responsibilities (PO.2): Ensure that everyone inside and outside of the organization involved in the SDLC is prepared to perform their SDLC-related roles and responsibilities throughout the SDLC.	**PO.2.1**: Create new roles and alter responsibilities for existing roles as needed to encompass all parts of the SDLC. Periodically review and maintain the defined roles and responsibilities, updating them as needed.	Example 1: Define SDLC-related roles and responsibilities for all members of the software development team.	**BSAFSS**: PD.2-1, PD.2-2
		Example 2: Integrate the security roles into the software development team.	**BSIMM**: SM1.1, SM2.3, SM2.7, CR1.7

		Example 3: Define roles and responsibilities for cybersecurity staff, security champions, project managers and leads, senior management, software developers, software testers, software assurance leads and staff, product owners, operations and platform engineers, and others involved in the SDLC.	**EO14028**: 4e(ix)
		Example 4: Conduct an annual review of all roles and responsibilities.	**IEC62443**: SM-2, SM-13
		Example 5: Educate affected individuals on impending changes to roles and responsibilities, and confirm that the individuals understand the changes and agree to follow them.	**NISTCSF**: ID.AM-6, ID.GV-2
		Example 6: Implement and use tools and processes to promote communication and engagement among individuals with SDLC-related roles and responsibilities, such as creating messaging channels for team discussions.	**PCISSLC**: 1.2
		Example 7: Designate a group of individuals or a team as the code owner for each project.	**SCSIC**: Vendor Software Development Integrity Controls **SP80053**: SA-3 **SP800160**: 3.2.1, 3.2.4, 3.3.1 **SP800161**: SA-3 **SP800181**: K0233
	PO.2.2: Provide role-based training for all personnel with responsibilities that contribute to secure development. Periodically review personnel proficiency and role-based training, and update the training as needed.	Example 1: Document the desired outcomes of training for each role.	**BSAFSS**: PD.2-2
		Example 2: Define the type of training or curriculum required to achieve the desired outcome for each role.	**BSIMM**: T1.1, T1.7, T1.8, T2.5, T2.8, T2.9, T3.1, T3.2, T3.4
		Example 3: Create a training plan for each role.	**EO14028**: 4e(ix)
		Example 4: Acquire or create training for each role; acquired training may need to be customized for the organization.	**IEC62443**: SM-4
		Example 5: Measure outcome performance to identify areas where changes to training may be beneficial.	**MSSDL**: 1 **NISTCSF**: PR.AT **OWASPSAMM**: EG1-A, EG2-A **PCISSLC**: 1.3 **SCAGILE**: Operational Security Tasks 14, 15; Tasks Requiring the Help of Security Experts 1 **SCFPSSD**: Planning the Implementation and Deployment of Secure Development Practices **SCSIC**: Vendor Software Development Integrity Controls **SP80053**: SA-8 **SP800160**: 3.2.4, 3.2.6 **SP800161**: SA-8 **SP800181**: OV-TEA-001, OV-TEA-002; T0030, T0073, T0320; K0204, K0208, K0220, K0226, K0243, K0245, K0252; S0100, S0101; A0004, A0057
	PO.2.3: Obtain upper management or authorizing official commitment to secure development, and convey that commitment to all with development-related roles and responsibilities.	Example 1: Appoint a single leader or leadership team to be responsible for the entire secure software development process, including being accountable for releasing software to production and delegating responsibilities as appropriate.	**BSIMM**: SM1.3, SM2.7, CP2.5
		Example 2: Increase authorizing officials' awareness of the risks of developing software without integrating security throughout the development life cycle and the risk mitigation provided by secure development practices.	**EO14028**: 4e(ix)
		Example 3: Assist upper management in incorporating secure development support into their communications with personnel with development-related roles and responsibilities.	**NISTCSF**: ID.RM-1, ID.SC-1

		Example 4: Educate all personnel with development-related roles and responsibilities on upper management's commitment to secure development and the importance of secure development to the organization.	**OWASPSAMM**: SM1.A **PCISSLC**: 1.1 **SP800181**: T0001, T0004
Implement Supporting Toolchains (PO.3): Use automation to reduce human effort and improve the accuracy, reproducibility, usability, and comprehensiveness of security practices throughout the SDLC, as well as provide a way to document and demonstrate the use of these practices. Toolchains and tools may be used at different levels of the organization, such as organization-wide or project-specific, and may address a particular part of the SDLC, like a build pipeline.	**PO.3.1**: Specify which tools or tool types must or should be included in each toolchain to mitigate identified risks, as well as how the toolchain components are to be integrated with each other.	Example 1: Define categories of toolchains, and specify the mandatory tools or tool types to be used for each category. Example 2: Identify security tools to integrate into the developer toolchain. Example 3: Define what information is to be passed between tools and what data formats are to be used. Example 4: Evaluate tools' signing capabilities to create immutable records/logs for auditability within the toolchain. Example 5: Use automated technology for toolchain management and orchestration.	**BSIMM**: CR1.4, ST1.4, ST2.5, SE2.7 **CNCFSSCP**: Securing Materials—Verification; Securing Build Pipelines—Verification, Automation, Secure Authentication/Access; Securing Artefacts—Verification; Securing Deployments—Verification **EO14028**: 4e(iii), 4e(ix) **MSSDL**: 8 **OWASPSAMM**: IR2-B, ST2-B **SCAGILE**: Tasks Requiring the Help of Security Experts 9 **SCSIC**: Vendor Software Delivery Integrity Controls **SP80053**: SA-15 **SP800161**: SA-15 **SP800181**: K0013, K0178
	PO.3.2: Follow recommended security practices to deploy, operate, and maintain tools and toolchains.	Example 1: Evaluate, select, and acquire tools, and assess the security of each tool. Example 2: Integrate tools with other tools and existing software development processes and workflows. Example 3: Use code-based configuration for toolchains (e.g., pipelines-as-code, toolchains-as-code). Example 4: Implement the technologies and processes needed for reproducible builds. Example 5: Update, upgrade, or replace tools as needed to address tool vulnerabilities or add new tool capabilities. Example 6: Continuously monitor tools and tool logs for potential operational and security issues, including policy violations and anomalous behavior. Example 7: Regularly verify the integrity and check the provenance of each tool to identify potential problems. Example 8: See PW.6 regarding compiler, interpreter, and build tools. Example 9: See PO.5 regarding implementing and maintaining secure environments.	**BSAFSS**: DE.2 **BSIMM**: SR1.1, SR1.3, SR3.4 **CNCFSSCP**: Securing Build Pipelines—Verification, Automation, Controlled Environments, Secure Authentication/Access; Securing Artefacts—Verification, Automation, Controlled Environments, Encryption; Securing Deployments—Verification, Automation **EO14028**: 4e(i)(F), 4e(ii), 4e(iii), 4e(v), 4e(vi), 4e(ix) **IEC62443**: SM-7 **IR8397**: 2.2 **OWASPASVS**: 1.14.3, 1.14.4, 14.1, 14.2 **OWASPMASVS**: 7.9 **OWASPSCVS**: 3, 5 **SCAGILE**: Tasks Requiring the Help of Security Experts 9 **SCFPSSD**: Use Current Compiler and Toolchain Versions and Secure Compiler Options **SCSIC**: Vendor Software Delivery Integrity Controls **SP80053**: SA-15 **SP800161**: SA-15

			SP800181: K0013, K0178
	PO.3.3: Configure tools to generate artifacts of their support of secure software development practices as defined by the organization.	Example 1: Use existing tooling (e.g., workflow tracking, issue tracking, value stream mapping) to create an audit trail of the secure development-related actions that are performed for continuous improvement purposes. Example 2: Determine how often the collected information should be audited, and implement the necessary processes. Example 3: Establish and enforce security and retention policies for artifact data. Example 4: Assign responsibility for creating any needed artifacts that tools cannot generate.	**BSAFSS**: PD.1-5 **BSIMM**: SM1.4, SM3.4, SR1.3 **CNCFSSCP**: Securing Build Pipelines—Verification, Automation, Controlled Environments; Securing Artefacts—Verification **EO14028**: 4e(i)(F), 4e(ii), 4e(v), 4e(ix) **IEC62443**: SM-12, SI-2 **MSSDL**: 8 **OWASPSAMM**: PC3-B **OWASPSCVS**: 3.13, 3.14 **PCISSLC**: 2.5 **SCAGILE**: Tasks Requiring the Help of Security Experts 9 **SCSIC**: Vendor Software Delivery Integrity Controls **SP80053**: SA-15 **SP800161**: SA-15 **SP800181**: K0013; T0024
Define and Use Criteria for Software Security Checks (PO.4): Help ensure that the software resulting from the SDLC meets the organization's expectations by defining and using criteria for checking the software's security during development.	**PO.4.1**: Define criteria for software security checks and track throughout the SDLC.	Example 1: Ensure that the criteria adequately indicate how effectively security risk is being managed. Example 2: Define key performance indicators (KPIs), key risk indicators (KRIs), vulnerability severity scores, and other measures for software security. Example 3: Add software security criteria to existing checks (e.g., the Definition of Done in agile SDLC methodologies). Example 4: Review the artifacts generated as part of the software development workflow system to determine if they meet the criteria. Example 5: Record security check approvals, rejections, and exception requests as part of the workflow and tracking system. Example 6: Analyze collected data in the context of the security successes and failures of each development project, and use the results to improve the SDLC.	**BSAFSS**: TV.2-1, TV.5-1 **BSIMM**: SM1.4, SM2.1, SM2.2, SM2.6, SM3.3, CP2.2 **EO14028**: 4e(iv), 4e(v), 4e(ix) **IEC62443**: SI-1, SI-2, SVV-3 **ISO27034**: 7.3.5 **MSSDL**: 3 **OWASPSAMM**: PC3-A, DR3-B, IR3-B, ST3-B **PCISSLC**: 3.3 **SP80053**: SA-15, SA-15(1) **SP800160**: 3.2.1, 3.2.5, 3.3.1 **SP800161**: SA-15, SA-15(1) **SP800181**: K0153, K0165
	PO.4.2: Implement processes, mechanisms, etc. to gather and safeguard the necessary information in support of the criteria.	Example 1: Use the toolchain to automatically gather information that informs security decision-making. Example 2: Deploy additional tools if needed to support the generation and collection of information supporting the criteria. Example 3: Automate decision-making processes utilizing the criteria, and periodically review these processes. Example 4: Only allow authorized personnel to access the gathered information, and prevent any alteration or deletion of the information.	**BSAFSS**: PD.1-4, PD.1-5 **BSIMM**: SM1.4, SM2.1, SM2.2, SM3.4 **EO14028**: 4e(iv), 4e(v), 4e(ix) **IEC62443**: SI-1, SVV-1, SVV-2, SVV-3, SVV-4 **OWASPSAMM**: PC3-B **PCISSLC**: 2.5

			SCSIC: Vendor Software Delivery Integrity Controls **SP80053**: SA-15, SA-15(1), SA-15(11) **SP800160**: 3.2.5, 3.3.7 **SP800161**: SA-15, SA-15(1), SA-15(11) **SP800181**: T0349; K0153
Implement and Maintain Secure Environments for Software Development (PO.5): Ensure that all components of the environments for software development are strongly protected from internal and external threats to prevent compromises of the environments or the software being developed or maintained within them. Examples of environments for software development include development, build, test, and distribution environments.	**PO.5.1**: Separate and protect each environment involved in software development.	Example 1: Use multi-factor, risk-based authentication and conditional access for each environment. Example 2: Use network segmentation and access controls to separate the environments from each other and from production environments, and to separate components from each other within each non-production environment, in order to reduce attack surfaces and attackers' lateral movement and privilege/access escalation. Example 3: Enforce authentication and tightly restrict connections entering and exiting each software development environment, including minimizing access to the internet to only what is necessary. Example 4: Minimize direct human access to toolchain systems, such as build services. Continuously monitor and audit all access attempts and all use of privileged access. Example 5: Minimize the use of production-environment software and services from non-production environments. Example 6: Regularly log, monitor, and audit trust relationships for authorization and access between the environments and between the components within each environment. Example 7: Continuously log and monitor operations and alerts across all components of the development environment to detect, respond, and recover from attempted and actual cyber incidents. Example 8: Configure security controls and other tools involved in separating and protecting the environments to generate artifacts for their activities. Example 9: Continuously monitor all software deployed in each environment for new vulnerabilities, and respond to vulnerabilities appropriately following a risk-based approach. Example 10: Configure and implement measures to secure the environments' hosting infrastructures following a zero trust architecture.	**BSAFSS**: DE.1, IA.1, IA.2 **CNCFSSCP**: Securing Build Pipelines—Controlled Environments **EO14028**: 4e(i)(A), 4e(i)(B), 4e(i)(C), 4e(i)(D), 4e(i)(F), 4e(ii), 4e(iii), 4e(v), 4e(vi), 4e(ix) **IEC62443**: SM-7 **NISTCSF**: PR.AC-5, PR.DS-7 **SCAGILE**: Tasks Requiring the Help of Security Experts 11 **SCSIC**: Vendor Software Delivery Integrity Controls **SP80053**: SA-3(1), SA-8, SA-15 **SP800161**: SA-3, SA-8, SA-15 **SP800181**: OM-NET-001, SP-SYS-001; T0019, T0023, T0144, T0160, T0262, T0438, T0484, T0485, T0553; K0001, K0005, K0007, K0033, K0049, K0056, K0061, K0071, K0104, K0112, K0179, K0326, K0487; S0007, S0084, S0121; A0048

	PO.5.2: Secure and harden development endpoints (i.e., endpoints for software designers, developers, testers, builders, etc.) to perform development-related tasks using a risk-based approach.	Example 1: Configure each development endpoint based on approved hardening guides, checklists, etc.; for example, enable FIPS-compliant encryption of all sensitive data at rest and in transit. Example 2: Configure each development endpoint and the development resources to provide the least functionality needed by users and services and to enforce the principle of least privilege. Example 3: Continuously monitor the security posture of all development endpoints, including monitoring and auditing all use of privileged access. Example 4: Configure security controls and other tools involved in securing and hardening development endpoints to generate artifacts for their activities. Example 5: Require multi-factor authentication for all access to development endpoints and development resources. Example 6: Provide dedicated development endpoints on non-production networks for performing all development-related tasks. Provide separate endpoints on production networks for all other tasks. Example 7: Configure each development endpoint following a zero trust architecture.	**BSAFSS**: DE.1-1, IA.1, IA.2 **EO14028**: 4e(i)(C), 4e(i)(E), 4e(i)(F), 4e(ii), 4e(iii), 4e(v), 4e(vi), 4e(ix) **IEC62443**: SM-7 **NISTCSF**: PR.AC-4, PR.AC-7, PR.IP-1, PR.IP-3, PR.IP-12, PR.PT-1, PR.PT-3, DE.CM **SCAGILE**: Tasks Requiring the Help of Security Experts 11 **SCSIC**: Vendor Software Delivery Integrity Controls **SP80053**: SA-15 **SP800161**: SA-15 **SP800181**: OM-ADM-001, SP-SYS-001; T0484, T0485, T0489, T0553; K0005, K0007, K0077, K0088, K0130, K0167, K0205, K0275; S0076, S0097, S0121, S0158; A0155
Protect All Forms of Code from Unauthorized Access and Tampering (PS.1): Help prevent unauthorized changes to code, both inadvertent and intentional, which could circumvent or negate the intended security characteristics of the software. For code that is not intended to be publicly accessible, this helps prevent theft of the software and may make it more difficult or time-consuming for attackers to find vulnerabilities in the software.	**PS.1.1**: Store all forms of code – including source code, executable code, and configuration-as-code – based on the principle of least privilege so that only authorized personnel, tools, services, etc. have access.	Example 1: Store all source code and configuration-as-code in a code repository, and restrict access to it based on the nature of the code. For example, open-source code intended for public access may need its integrity and availability protected; other code may also need its confidentiality protected. Example 2: Use version control features of the repository to track all changes made to the code with accountability to the individual account. Example 3: Use commit signing for code repositories. Example 4: Have the code owner review and approve all changes made to the code by others. Example 5: Use code signing to help protect the integrity of executables. Example 6: Use cryptography (e.g., cryptographic hashes) to help protect file integrity.	**BSAFSS**: IA.1, IA.2, SM.4-1, DE.1-2 **BSIMM**: SE2.4 **CNCFSSCP**: Securing the Source Code—Verification, Automation, Controlled Environments, Secure Authentication; Securing Materials—Automation **EO14028**: 4e(iii), 4e(iv), 4e(ix) **IDASOAR**: Fact Sheet 25 **IEC62443**: SM-6, SM-7, SM-8 **NISTCSF**: PR.AC-4, PR.DS-6, PR.IP-3 **OWASPASVS**: 1.10, 10.3.2 **OWASPMASVS**: 7.1 **OWASPSAMM**: OE3-B **PCISSLC**: 5.1, 6.1 **SCSIC**: Vendor Software Delivery Integrity Controls, Vendor Software Development Integrity Controls **SP80053**: SA-10 **SP800161**: SA-8, SA-10

Provide a Mechanism for Verifying Software Release Integrity (PS.2): Help software acquirers ensure that the software they acquire is legitimate and has not been tampered with.	**PS.2.1**: Make software integrity verification information available to software acquirers.	Example 1: Post cryptographic hashes for release files on a well-secured website. Example 2: Use an established certificate authority for code signing so that consumers' operating systems or other tools and services can confirm the validity of signatures before use. Example 3: Periodically review the code signing processes, including certificate renewal, rotation, revocation, and protection.	**BSAFSS**: SM.4, SM.5, SM.6 **BSIMM**: SE2.4 **CNCFSSCP**: Securing Deployments—Verification **EO14028**: 4e(iii), 4e(ix), 4e(x) **IEC62443**: SM-6, SM-8, SUM-4 **NISTCSF**: PR.DS-6 **NISTLABEL**: 2.2.2.4 **OWASPSAMM**: OE3-B **OWASPSCVS**: 4 **PCISSLC**: 6.1, 6.2 **SCSIC**: Vendor Software Delivery Integrity Controls **SP80053**: SA-8 **SP800161**: SA-8 **SP800181**: K0178
Archive and Protect Each Software Release (PS.3): Preserve software releases in order to help identify, analyze, and eliminate vulnerabilities discovered in the software after release.	**PS.3.1**: Securely archive the necessary files and supporting data (e.g., integrity verification information, provenance data) to be retained for each software release.	Example 1: Store the release files, associated images, etc. in repositories following the organization's established policy. Allow read-only access to them by necessary personnel and no access by anyone else. Example 2: Store and protect release integrity verification information and provenance data, such as by keeping it in a separate location from the release files or by signing the data.	**BSAFSS**: PD.1-5, DE.1-2, IA.2 **CNCFSSCP**: Securing Artefacts—Automation, Controlled Environments, Encryption; Securing Deployments—Verification **EO14028**: 4e(iii), 4e(vi), 4e(ix), 4e(x) **IDASOAR**: 25 **IEC62443**: SM-6, SM-7 **NISTCSF**: PR.IP-4 **OWASPSCVS**: 1, 3.18, 3.19, 6.3 **PCISSLC**: 5.2, 6.1, 6.2 **SCSIC**: Vendor Software Delivery Integrity Controls **SP80053**: SA-10, SA-15, SA-15(11), SR-4 **SP800161**: SA-8, SA-10, SA-15(11), SR-4
	PS.3.2: Collect, safeguard, maintain, and share provenance data for all components of each software release (e.g., in a software bill of materials [SBOM]).	Example 1: Make the provenance data available to software acquirers in accordance with the organization's policies, preferably using standards-based formats. Example 2: Make the provenance data available to the organization's operations and response teams to aid them in mitigating software vulnerabilities. Example 3: Protect the integrity of provenance data, and provide a way for recipients to verify provenance data integrity. Example 4: Update the provenance data every time any of the software's components are updated.	**BSAFSS**: SM.2 **BSIMM**: SE3.6 **CNCFSSCP**: Securing Materials—Verification, Automation **EO14028**: 4e(vi), 4e(vii), 4e(ix), 4e(x) **NTIASBOM**: All **OWASPSCVS**: 1.4, 2 **SCSIC**: Vendor Software Delivery Integrity Controls **SCTPC**: MAINTAIN3 **SP80053**: SA-8, SR-3, SR-4 **SP800161**: SA-8, SR-3, SR-4

Design Software to Meet Security Requirements and Mitigate Security Risks (PW.1): Identify and evaluate the security requirements for the software; determine what security risks the software is likely to face during operation and how the software's design and architecture should mitigate those risks; and justify any cases where risk-based analysis indicates that security requirements should be relaxed or waived. Addressing security requirements and risks during software design (secure by design) is key for improving software security and also helps improve development efficiency.	**PW.1.1**: Use forms of risk modeling – such as threat modeling, attack modeling, or attack surface mapping – to help assess the security risk for the software.	Example 1: Train the development team (security champions, in particular) or collaborate with a risk modeling expert to create models and analyze how to use a risk-based approach to communicate the risks and determine how to address them, including implementing mitigations. Example 2: Perform more rigorous assessments for high-risk areas, such as protecting sensitive data and safeguarding identification, authentication, and access control, including credential management. Example 3: Review vulnerability reports and statistics for previous software to inform the security risk assessment. Example 4: Use data classification methods to identify and characterize each type of data that the software will interact with.	**BSAFSS**: SC.1 **BSIMM**: AM1.2, AM1.3, AM1.5, AM2.1, AM2.2, AM2.5, AM2.6, AM2.7, SFD2.2, AA1.1, AA1.2, AA1.3, AA2.1 **EO14028**: 4e(ix) **IDASOAR**: 1 **IEC62443**: SM-4, SR-1, SR-2, SD-1 **IR8397**: 2.1 **ISO27034**: 7.3.3 **MSSDL**: 4 **NISTCSF**: ID.RA **OWASPASVS**: 1.1.2, 1.2, 1.4, 1.6, 1.8, 1.9, 1.11, 2, 3, 4, 6, 8, 9, 11, 12, 13 **OWASPMASVS**: 1.6, 1.8, 2, 3, 4, 5, 6 **OWASPSAMM**: TA1-A, TA1-B, TA3-B, DR1-A **PCISSLC**: 3.2, 3.3 **SCAGILE**: Tasks Requiring the Help of Security Experts 3 **SCFPSSD**: Threat Modeling **SCTTM**: Entire guide **SP80053**: SA-8, SA-11(2), SA-11(6), SA-15(5) **SP800160**: 3.3.4, 3.4.5 **SP800161**: SA-8, SA-11(2), SA-11(6), SA-15(5) **SP800181**: T0038, T0062; K0005, K0009, K0038, K0039, K0070, K0080, K0119, K0147, K0149, K0151, K0152, K0160, K0161, K0162, K0165, K0297, K0310, K0344, K0362, K0487, K0624; S0006, S0009, S0022, S0078, S0171, S0229, S0248; A0092, A0093, A0107
	PW.1.2: Track and maintain the software's security requirements, risks, and design decisions.	Example 1: Record the response to each risk, including how mitigations are to be achieved and what the rationales are for any approved exceptions to the security requirements. Add any mitigations to the software's security requirements. Example 2: Maintain records of design decisions, risk responses, and approved exceptions that can be used for auditing and maintenance purposes throughout the rest of the software life cycle. Example 3: Periodically re-evaluate all approved exceptions to the security requirements, and implement changes as needed.	**BSAFSS**: SC.1-1, PD.1-1 **BSIMM**: SFD3.1, SFD3.3, AA2.2, AA3.2 **EO14028**: 4e(v), 4e(ix) **IEC62443**: SD-1 **ISO27034**: 7.3.3 **MSSDL**: 4 **NISTLABEL**: 2.2.2.2 **OWASPASVS**: 1.1.3, 1.1.4 **OWASPMASVS**: 1.3, 1.6 **OWASPSAMM**: DR1-B **PCISSLC**: 3.2, 3.3

			SP80053: SA-8, SA-10, SA-17 **SP800161**: SA-8, SA-17 **SP800181**: T0256; K0005, K0038, K0039, K0147, K0149, K0160, K0161, K0162, K0165, K0344, K0362, K0487; S0006, S0009, S0078, S0171, S0229, S0248; A0092, A0107
	PW.1.3: Where appropriate, build in support for using standardized security features and services (e.g., enabling software to integrate with existing log management, identity management, access control, and vulnerability management systems) instead of creating proprietary implementations of security features and services. [Formerly PW.4.3]	Example 1: Maintain one or more software repositories of modules for supporting standardized security features and services. Example 2: Determine secure configurations for modules for supporting standardized security features and services, and make these configurations available (e.g., as configuration-as-code) so developers can readily use them. Example 3: Define criteria for which security features and services must be supported by software to be developed.	**BSAFSS**: SI.2-1, SI.2-2, LO.1 **BSIMM**: SFD1.1, SFD2.1, SFD3.2, SR1.1, SR3.4 **EO14028**: 4e(ix) **IEC62443**: SD-1, SD-4 **MSSDL**: 5 **OWASPASVS**: 1.1.6 **OWASPSAMM**: SA2-A **SCFPSSD**: Standardize Identity and Access Management; Establish Log Requirements and Audit Practices
Review the Software Design to Verify Compliance with Security Requirements and Risk Information (PW.2): Help ensure that the software will meet the security requirements and satisfactorily address the identified risk information.	**PW.2.1**: Have 1) a qualified person (or people) who were not involved with the design and/or 2) automated processes instantiated in the toolchain review the software design to confirm and enforce that it meets all of the security requirements and satisfactorily addresses the identified risk information.	Example 1: Review the software design to confirm that it addresses applicable security requirements. Example 2: Review the risk models created during software design to determine if they appear to adequately identify the risks. Example 3: Review the software design to confirm that it satisfactorily addresses the risks identified by the risk models. Example 4: Have the software's designer correct failures to meet the requirements. Example 5: Change the design and/or the risk response strategy if the security requirements cannot be met. Example 6: Record the findings of design reviews to serve as artifacts (e.g., in the software specification, in the issue tracking system, in the threat model).	**BSAFSS**: TV.3 **BSIMM**: AA1.1, AA1.2, AA1.3, AA2.1, AA3.1 **EO14028**: 4e(iv), 4e(v), 4e(ix) **IEC62443**: SM-2, SR-2, SR-5, SD-3, SD-4, SI-2 **ISO27034**: 7.3.3 **OWASPASVS**: 1.1.5 **OWASPSAMM**: DR1-A, DR1-B **PCISSLC**: 3.2 **SP800181**: T0328; K0038, K0039, K0070, K0080, K0119, K0152, K0153, K0161, K0165, K0172, K0297; S0006, S0009, S0022, S0036, S0141, S0171
Reuse Existing, Well-Secured Software When Feasible Instead of Duplicating Functionality (PW.4): Lower the costs of software development, expedite software development, and decrease the likelihood of introducing additional security vulnerabilities into the software by reusing software modules and services that have already had their security posture checked. This is particularly important for software that implements security functionality, such as cryptographic modules and protocols.	**PW.4.1**: Acquire and maintain well-secured software components (e.g., software libraries, modules, middleware, frameworks) from commercial, open-source, and other third-party developers for use by the organization's software.	Example 1: Review and evaluate third-party software components in the context of their expected use. If a component is to be used in a substantially different way in the future, perform the review and evaluation again with that new context in mind. Example 2: Determine secure configurations for software components, and make these available (e.g., as configuration-as-code) so developers can readily use the configurations. Example 3: Obtain provenance information (e.g., SBOM, source composition analysis, binary software composition analysis) for each software component, and analyze that information to better assess the risk that the component may introduce. Example 4: Establish one or more software repositories to host sanctioned and vetted open-source components. Example 5: Maintain a list of organization-approved commercial software components and component versions along with their provenance data.	**BSAFSS**: SM.2 **BSIMM**: SFD2.1, SFD3.2, SR2.4, SR3.1, SE3.6 **CNCFSSCP**: Securing Materials—Verification **EO14028**: 4e(iii), 4e(vi), 4e(ix), 4e(x) **IDASOAR**: 19

		Example 6: Designate which components must be included in software to be developed. Example 7: Implement processes to update deployed software components to newer versions, and retain older versions of software components until all transitions from those versions have been completed successfully. Example 8: If the integrity or provenance of acquired binaries cannot be confirmed, build binaries from source code after verifying the source code's integrity and provenance.	**IEC62443**: SM-9, SM-10 **MSSDL**: 6 **NISTCSF**: ID.SC-2 **OWASPASVS**: 1.1.6 **OWASPSAMM**: SA1-A **OWASPSCVS**: 4 **SCSIC**: Vendor Sourcing Integrity Controls **SCTPC**: MAINTAIN **SP80053**: SA-4, SA-5, SA-8(3), SA-10(6), SR-3, SR-4 **SP800161**: SA-4, SA-5, SA-8(3), SA-10(6), SR-3, SR-4 **SP800181**: K0039
	PW.4.2: Create and maintain well-secured software components in-house following SDLC processes to meet common internal software development needs that cannot be better met by third-party software components.	Example 1: Follow organization-established security practices for secure software development when creating and maintaining the components. Example 2: Determine secure configurations for software components, and make these available (e.g., as configuration-as-code) so developers can readily use the configurations. Example 3: Maintain one or more software repositories for these components. Example 4: Designate which components must be included in software to be developed. Example 5: Implement processes to update deployed software components to newer versions, and maintain older versions of software components until all transitions from those versions have been completed successfully.	**BSIMM**: SFD1.1, SFD2.1, SFD3.2, SR1.1 **EO14028**: 4e(ix) **IDASOAR**: 19 **OWASPASVS**: 1.1.6 **SCTPC**: MAINTAIN **SP80053**: SA-8(3) **SP800161**: SA-8(3) **SP800181**: SP-DEV-001
	PW.4.4: Verify that acquired commercial, open-source, and all other third-party software components comply with the requirements, as defined by the organization, throughout their life cycles.	Example 1: Regularly check whether there are publicly known vulnerabilities in the software modules and services that vendors have not yet fixed. Example 2: Build into the toolchain automatic detection of known vulnerabilities in software components. Example 3: Use existing results from commercial services for vetting the software modules and services. Example 4: Ensure that each software component is still actively maintained and has not reached end of life; this should include new vulnerabilities found in the software being remediated. Example 5: Determine a plan of action for each software component that is no longer being maintained or will not be available in the near future. Example 6: Confirm the integrity of software components through digital signatures or other mechanisms. Example 7: Review, analyze, and/or test code. See PW.7 and PW.8.	**BSAFSS**: SC.3-1, SM.2-1, SM.2-2, SM.2-3, TV.2, TV.3 **BSIMM**: CP3.2, SR2.4, SR3.1, SR3.2, SE2.4, SE3.6 **CNCFSSCP**: Securing Materials—Verification, Automation **EO14028**: 4e(iii), 4e(iv), 4e(vi), 4e(ix), 4e(x) **IDASOAR**: 21 **IEC62443**: SI-1, SM-9, SM-10, DM-1 **IR8397**: 2.11 **MSSDL**: 7 **NISTCSF**: ID.SC-4, PR.DS-6 **NISTLABEL**: 2.2.2.2

			OWASPASVS: 10, 14.2 **OWASPMASVS**: 7.5 **OWASPSAMM**: TA3-A, SR3-B **OWASPSCVS**: 4, 5, 6 **PCISSLC**: 3.2, 3.4, 4.1 **SCAGILE**: Tasks Requiring the Help of Security Experts 8 **SCFPSSD**: Manage Security Risk Inherent in the Use of Third-Party Components **SCSIC**: Vendor Sourcing Integrity Controls, Peer Reviews and Security Testing **SCTPC**: MAINTAIN, ASSESS **SP80053**: SA-9, SR-3, SR-4, SR-4(3), SR-4(4) **SP800160**: 3.1.2, 3.3.8 **SP800161**: SA-4, SA-8, SA-9, SA-9(3), SR-3, SR-4, SR-4(3), SR-4(4) **SP800181**: SP-DEV-002; K0153, K0266; S0298
Create Source Code by Adhering to Secure Coding Practices (PW.5): Decrease the number of security vulnerabilities in the software, and reduce costs by minimizing vulnerabilities introduced during source code creation that meet or exceed organization-defined vulnerability severity criteria.	**PW.5.1**: Follow all secure coding practices that are appropriate to the development languages and environment to meet the organization's requirements.	Example 1: Validate all inputs, and validate and properly encode all outputs. Example 2: Avoid using unsafe functions and calls. Example 3: Detect errors, and handle them gracefully. Example 4: Provide logging and tracing capabilities. Example 5: Use development environments with automated features that encourage or require the use of secure coding practices with just-in-time training-in-place. Example 6: Follow procedures for manually ensuring compliance with secure coding practices when automated methods are insufficient or unavailable. Example 7: Use tools (e.g., linters, formatters) to standardize the style and formatting of the source code. Example 8: Check for other vulnerabilities that are common to the development languages and environment. Example 9: Have the developer review their own human-readable code to complement (not replace) code review performed by other people or tools. See PW.7.	**BSAFSS**: SC.2, SC.3, LO.1, EE.1 **BSIMM**: SR3.3, CR1.4, CR3.5 **EO14028**: 4e(iv), 4e(ix) **IDASOAR**: 2 **IEC62443**: SI-1, SI-2 **ISO27034**: 7.3.5 **MSSDL**: 9 **OWASPASVS**: 1.1.7, 1.5, 1.7, 5, 7 **OWASPMASVS**: 7.6 **SCFPSSD**: Establish Log Requirements and Audit Practices, Use Code Analysis Tools to Find Security Issues Early, Handle Data Safely, Handle Errors, Use Safe Functions Only **SP800181**: SP-DEV-001; T0013, T0077, T0176; K0009, K0016, K0039, K0070, K0140, K0624; S0019, S0060, S0149, S0172, S0266; A0036, A0047
Configure the Compilation, Interpreter, and Build Processes to Improve Executable Security (PW.6): Decrease the number of security vulnerabilities in the software and reduce costs by eliminating vulnerabilities before testing occurs.	**PW.6.1**: Use compiler, interpreter, and build tools that offer features to improve executable security.	Example 1: Use up-to-date versions of compiler, interpreter, and build tools. Example 2: Follow change management processes when deploying or updating compiler, interpreter, and build tools, and audit all unexpected changes to tools. Example 3: Regularly validate the authenticity and integrity of compiler, interpreter, and build tools. See PO.3.	**BSAFSS**: DE.2-1 **BSIMM**: SE2.4 **CNCFSSCP**: Securing Build Pipelines—Verification, Automation **EO14028**: 4e(iv), 4e(ix) **IEC62443**: SI-2 **MSSDL**: 8 **SCAGILE**: Operational Security Task 3 **SCFPSSD**: Use Current Compiler and Toolchain Versions and Secure Compiler Options

			SCSIC: Vendor Software Development Integrity Controls **SP80053**: SA-15 **SP800161**: SA-15
	PW.6.2: Determine which compiler, interpreter, and build tool features should be used and how each should be configured, then implement and use the approved configurations.	Example 1: Enable compiler features that produce warnings for poorly secured code during the compilation process. Example 2: Implement the "clean build" concept, where all compiler warnings are treated as errors and eliminated except those determined to be false positives or irrelevant. Example 3: Perform all builds in a dedicated, highly controlled build environment. Example 4: Enable compiler features that randomize or obfuscate execution characteristics, such as memory location usage, that would otherwise be predictable and thus potentially exploitable. Example 5: Test to ensure that the features are working as expected and are not inadvertently causing any operational issues or other problems. Example 6: Continuously verify that the approved configurations are being used. Example 7: Make the approved tool configurations available as configuration-as-code so developers can readily use them.	**BSAFSS**: DE.2-3, DE.2-4, DE.2-5 **BSIMM**: SE2.4, SE3.2 **CNCFSSCP**: Securing Build Pipelines—Verification, Automation **EO14028**: 4e(iv), 4e(ix) **IEC62443**: SI-2 **IR8397**: 2.5 **MSSDL**: 8 **OWASPASVS**: 14.1, 14.2.1 **OWASPMASVS**: 7.2 **PCISSLC**: 3.2 **SCAGILE**: Operational Security Task 8 **SCFPSSD**: Use Current Compiler and Toolchain Versions and Secure Compiler Options **SCSIC**: Vendor Software Development Integrity Controls **SP80053**: SA-15, SR-9 **SP800161**: SA-15, SR-9 **SP800181**: K0039, K0070
Review and/or Analyze Human-Readable Code to Identify Vulnerabilities and Verify Compliance with Security Requirements (PW.7): Help identify vulnerabilities so that they can be corrected before the software is released to prevent exploitation. Using automated methods lowers the effort and resources needed to detect vulnerabilities. Human-readable code includes source code, scripts, and any other form of code that an organization deems human-readable.	**PW.7.1**: Determine whether code review (a person looks directly at the code to find issues) and/or code analysis (tools are used to find issues in code, either in a fully automated way or in conjunction with a person) should be used, as defined by the organization.	Example 1: Follow the organization's policies or guidelines for when code review should be performed and how it should be conducted. This may include third-party code and reusable code modules written in-house. Example 2: Follow the organization's policies or guidelines for when code analysis should be performed and how it should be conducted. Example 3: Choose code review and/or analysis methods based on the stage of the software.	**BSIMM**: CR1.5 **EO14028**: 4e(iv), 4e(ix) **IEC62443**: SM-5, SI-1, SVV-1 **NISTLABEL**: 2.2.2.2 **SCSIC**: Peer Reviews and Security Testing **SP80053**: SA-11 **SP800161**: SA-11 **SP800181**: SP-DEV-002; K0013, K0039, K0070, K0153, K0165; S0174
	PW.7.2: Perform the code review and/or code analysis based on the organization's secure coding standards, and record and triage all discovered issues and recommended remediations in the development team's workflow or issue tracking system.	Example 1: Perform peer review of code, and review any existing code review, analysis, or testing results as part of the peer review. Example 2: Use expert reviewers to check code for backdoors and other malicious content. Example 3: Use peer reviewing tools that facilitate the peer review process, and document all discussions and other feedback.	**BSAFSS**: TV.2, PD.1-4 **BSIMM**: CR1.2, CR1.4, CR1.6, CR2.6, CR2.7, CR3.4, CR3.5 **EO14028**: 4e(iv), 4e(v), 4e(ix)

		Example 4: Use a static analysis tool to automatically check code for vulnerabilities and compliance with the organization's secure coding standards with a human reviewing the issues reported by the tool and remediating them as necessary. Example 5: Use review checklists to verify that the code complies with the requirements. Example 6: Use automated tools to identify and remediate documented and verified unsafe software practices on a continuous basis as human-readable code is checked into the code repository. Example 7: Identify and document the root causes of discovered issues. Example 8: Document lessons learned from code review and analysis in a wiki that developers can access and search.	**IDASOAR**: 3, 4, 5, 14, 15, 48 **IEC62443**: SI-1, SVV-1, SVV-2 **IR8397**: 2.3, 2.4 **ISO27034**: 7.3.6 **MSSDL**: 9, 10 **NISTLABEL**: 2.2.2.2 **OWASPASVS**: 1.1.7, 10 **OWASPMASVS**: 7.5 **OWASPSAMM**: IR1-B, IR2-A, IR2-B, IR3-A **PCISSLC**: 3.2, 4.1 **SCAGILE**: Operational Security Tasks 4, 7; Tasks Requiring the Help of Security Experts 10 **SCFPSSD**: Use Code Analysis Tools to Find Security Issues Early, Use Static Analysis Security Testing Tools, Perform Manual Verification of Security Features/Mitigations **SCSIC**: Peer Reviews and Security Testing **SP80053**: SA-11, SA-11(1), SA-11(4), SA-15(7) **SP800161**: SA-11, SA-11(1), SA-11(4), SA-15(7) **SP800181**: SP-DEV-001, SP-DEV-002; T0013, T0111, T0176, T0267, T0516; K0009, K0039, K0070, K0140, K0624; S0019, S0060, S0078, S0137, S0149, S0167, S0174, S0242, S0266; A0007, A0015, A0036, A0044, A0047
Test Executable Code to Identify Vulnerabilities and Verify Compliance with Security Requirements (PW.8): Help identify vulnerabilities so that they can be corrected before the software is released in order to prevent exploitation. Using automated methods lowers the effort and resources needed to detect vulnerabilities and improves traceability and repeatability. Executable code includes binaries, directly executed bytecode and source code, and any other form of code that an organization deems executable.	**PW.8.1**: Determine whether executable code testing should be performed to find vulnerabilities not identified by previous reviews, analysis, or testing and, if so, which types of testing should be used.	Example 1: Follow the organization's policies or guidelines for when code testing should be performed and how it should be conducted (e.g., within a sandboxed environment). This may include third-party executable code and reusable executable code modules written in-house. Example 2: Choose testing methods based on the stage of the software.	**BSAFSS**: TV.3 **BSIMM**: PT2.3 **EO14028**: 4e(ix) **IEC62443**: SVV-1, SVV-2, SVV-3, SVV-4, SVV-5 **NISTLABEL**: 2.2.2.2 **SCSIC**: Peer Reviews and Security Testing **SP80053**: SA-11 **SP800161**: SA-11 **SP800181**: SP-DEV-001, SP-DEV-002; T0456; K0013, K0039, K0070, K0153, K0165, K0342, K0367, K0536, K0624; S0001, S0015, S0026, S0061, S0083, S0112, S0135

	PW.8.2: Scope the testing, design the tests, perform the testing, and document the results, including recording and triaging all discovered issues and recommended remediations in the development team's workflow or issue tracking system.	Example 1: Perform robust functional testing of security features. Example 2: Integrate dynamic vulnerability testing into the project's automated test suite. Example 3: Incorporate tests for previously reported vulnerabilities into the project's test suite to ensure that errors are not reintroduced. Example 4: Take into consideration the infrastructures and technology stacks that the software will be used with in production when developing test plans. Example 5: Use fuzz testing tools to find issues with input handling. Example 6: If resources are available, use penetration testing to simulate how an attacker might attempt to compromise the software in high-risk scenarios. Example 7: Identify and record the root causes of discovered issues. Example 8: Document lessons learned from code testing in a wiki that developers can access and search. Example 9: Use source code, design records, and other resources when developing test plans.	**BSAFSS**: TV.3, TV.5, PD.1-4 **BSIMM**: ST1.1, ST1.3, ST1.4, ST2.4, ST2.5, ST2.6, ST3.3, ST3.4, ST3.5, ST3.6, PT1.1, PT1.2, PT1.3, PT3.1 **EO14028**: 4e(iv), 4e(v), 4e(ix) **IDASOAR**: 7, 8, 10, 11, 38, 39, 43, 44, 48, 55, 56, 57 **IEC62443**: SM-5, SM-13, SI-1, SVV-1, SVV-2, SVV-3, SVV-4, SVV-5 **IR8397**: 2.6, 2.7, 2.8, 2.9, 2.10, 2.11 **ISO27034**: 7.3.6 **MSSDL**: 10, 11 **NISTLABEL**: 2.2.2.2 **OWASPMASVS**: 7.5 **OWASPSAMM**: ST1-A, ST1-B, ST2-A, ST2-B, ST3-A **PCISSLC**: 4.1 **SCAGILE**: Operational Security Tasks 10, 11; Tasks Requiring the Help of Security Experts 4, 5, 6, 7 **SCFPSSD**: Perform Dynamic Analysis Security Testing, Fuzz Parsers, Network Vulnerability Scanning, Perform Automated Functional Testing of Security Features/Mitigations, Perform Penetration Testing **SCSIC**: Peer Reviews and Security Testing **SP80053**: SA-11, SA-11(5), SA-11(8), SA-15(7) **SP800161**: SA-11, SA-11(5), SA-11(8), SA-15(7) **SP800181**: SP-DEV-001, SP-DEV-002; T0013, T0028, T0169, T0176, T0253, T0266, T0456, T0516; K0009, K0039, K0070, K0272, K0339, K0342, K0362, K0536, K0624; S0001, S0015, S0046, S0051, S0078, S0081, S0083, S0135, S0137, S0167, S0242; A0015
Configure Software to Have Secure Settings by Default (PW.9): Help improve the security of the software at the time of installation to reduce the likelihood of the software being deployed with weak security settings, putting it at greater risk of compromise.	**PW.9.1**: Define a secure baseline by determining how to configure each setting that has an effect on security or a security-related setting so that the default settings are secure and do not weaken the security functions provided by the platform, network infrastructure, or services.	Example 1: Conduct testing to ensure that the settings, including the default settings, are working as expected and are not inadvertently causing any security weaknesses, operational issues, or other problems.	**BSAFSS**: CF.1 **BSIMM**: SE2.2 **EO14028**: 4e(iv), 4e(ix) **IDASOAR**: 23 **IEC62443**: SD-4, SVV-1, SG-1 **ISO27034**: 7.3.5 **SCAGILE**: Tasks Requiring the Help of Security Experts 12 **SCSIC**: Vendor Software Delivery Integrity Controls, Vendor Software Development Integrity Controls **SP800181**: SP-DEV-002; K0009, K0039, K0073, K0153, K0165, K0275, K0531; S0167

	PW.9.2: Implement the default settings (or groups of default settings, if applicable), and document each setting for software administrators.	Example 1: Verify that the approved configuration is in place for the software. Example 2: Document each setting's purpose, options, default value, security relevance, potential operational impact, and relationships with other settings. Example 3: Use authoritative programmatic technical mechanisms to record how each setting can be implemented and assessed by software administrators. Example 4: Store the default configuration in a usable format and follow change control practices for modifying it (e.g., configuration-as-code).	**BSAFSS**: CF.1 **BSIMM**: SE2.2 **EO14028**: 4e(iv), 4e(ix) **IDASOAR**: 23 **IEC62443**: SG-3 **OWASPSAMM**: OE1-A **PCISSLC**: 8.1, 8.2 **SCAGILE**: Tasks Requiring the Help of Security Experts 12 **SCFPSSD**: Verify Secure Configurations and Use of Platform Mitigation **SCSIC**: Vendor Software Delivery Integrity Controls, Vendor Software Development Integrity Controls **SP80053**: SA-5, SA-8(23) **SP800161**: SA-5, SA-8(23) **SP800181**: SP-DEV-001; K0009, K0039, K0073, K0153, K0165, K0275, K0531
Identify and Confirm Vulnerabilities on an Ongoing Basis (RV.1): Help ensure that vulnerabilities are identified more quickly so that they can be remediated more quickly in accordance with risk, reducing the window of opportunity for attackers.	**RV.1.1**: Gather information from software acquirers, users, and public sources on potential vulnerabilities in the software and third-party components that the software uses, and investigate all credible reports.	Example 1: Monitor vulnerability databases , security mailing lists, and other sources of vulnerability reports through manual or automated means. Example 2: Use threat intelligence sources to better understand how vulnerabilities in general are being exploited. Example 3: Automatically review provenance and software composition data for all software components to identify any new vulnerabilities they have.	**BSAFSS**: VM.1-3, VM.3 **BSIMM**: AM1.5, CMVM1.2, CMVM2.1, CMVM3.4, CMVM3.7 **CNCFSSCP**: Securing Materials—Verification **EO14028**: 4e(iv), 4e(vi), 4e(viii), 4e(ix) **IEC62443**: DM-1, DM-2, DM-3 **ISO29147**: 6.2.1, 6.2.2, 6.2.4, 6.3, 6.5 **ISO30111**: 7.1.3 **OWASPSAMM**: IM1-A, IM2-B, EH1-B **OWASPSCVS**: 4 **PCISSLC**: 3.4, 4.1, 9.1 **SCAGILE**: Operational Security Task 5 **SCFPSSD**: Vulnerability Response and Disclosure **SCTPC**: MONITOR1 **SP80053**: SA-10, SR-3, SR-4 **SP800161**: SA-10, SR-3, SR-4 **SP800181**: K0009, K0038, K0040, K0070, K0161, K0362; S0078

	RV.1.2: Review, analyze, and/or test the software's code to identify or confirm the presence of previously undetected vulnerabilities.	Example 1: Configure the toolchain to perform automated code analysis and testing on a regular or continuous basis for all supported releases. Example 2: See PW.7 and PW.8.	**BSAFSS**: VM.1-2, VM.2-1 **BSIMM**: CMVM3.1 **EO14028**: 4e(iv), 4e(vi), 4e(viii), 4e(ix) **IEC62443**: SI-1, SVV-2, SVV-3, SVV-4, DM-1, DM-2 **ISO27034**: 7.3.6 **ISO29147**: 6.4 **ISO30111**: 7.1.4 **PCISSLC**: 3.4, 4.1 **SCAGILE**: Operational Security Tasks 10, 11 **SP80053**: SA-11 **SP800161**: SA-11 **SP800181**: SP-DEV-002; K0009, K0039, K0153
	RV.1.3: Have a policy that addresses vulnerability disclosure and remediation, and implement the roles, responsibilities, and processes needed to support that policy.	Example 1: Establish a vulnerability disclosure program, and make it easy for security researchers to learn about your program and report possible vulnerabilities. Example 2: Have a Product Security Incident Response Team (PSIRT) and processes in place to handle the responses to vulnerability reports and incidents, including communications plans for all stakeholders. Example 3: Have a security response playbook to handle a generic reported vulnerability, a report of zero-days, a vulnerability being exploited in the wild, and a major ongoing incident involving multiple parties and open-source software components. Example 4: Periodically conduct exercises of the product security incident response processes.	**BSAFSS**: VM.1-1, VM.2 **BSIMM**: CMVM1.1, CMVM2.1, CMVM3.3, CMVM3.7 **EO14028**: 4e(viii), 4e(ix) **IEC62443**: DM-1, DM-2, DM-3, DM-4, DM-5 **ISO29147**: All **ISO30111**: All **MSSDL**: 12 **NISTLABEL**: 2.2.2.3 **OWASPMASVS**: 1.11 **OWASPSAMM**: IM1-A, IM1-B, IM2-A, IM2-B **PCISSLC**: 9.2, 9.3 **SCFPSSD**: Vulnerability Response and Disclosure **SP80053**: SA-15(10) **SP800160**: 3.3.8 **SP800161**: SA-15(10) **SP800181**: K0041, K0042, K0151, K0292, K0317; S0054; A0025 **SP800216**: All

Assess, Prioritize, and Remediate Vulnerabilities (RV.2): Help ensure that vulnerabilities are remediated in accordance with risk to reduce the window of opportunity for attackers.	**RV.2.1**: Analyze each vulnerability to gather sufficient information about risk to plan its remediation or other risk response.	Example 1: Use existing issue tracking software to record each vulnerability. Example 2: Perform risk calculations for each vulnerability based on estimates of its exploitability, the potential impact if exploited, and any other relevant characteristics.	**BSAFSS**: VM.2 **BSIMM**: CMVM1.2, CMVM2.2 **EO14028**: 4e(iv), 4e(viii), 4e(ix) **IEC62443**: DM-2, DM-3 **ISO30111**: 7.1.4 **NISTLABEL**: 2.2.2.2 **PCISSLC**: 3.4, 4.2 **SCAGILE**: Operational Security Task 1, Tasks Requiring the Help of Security Experts 10 **SP80053**: SA-10, SA-15(7) **SP800160**: 3.3.8 **SP800161**: SA-15(7) **SP800181**: K0009, K0039, K0070, K0161, K0165; S0078
	RV.2.2: Plan and implement risk responses for vulnerabilities.	Example 1: Make a risk-based decision as to whether each vulnerability will be remediated or if the risk will be addressed through other means (e.g., risk acceptance, risk transference), and prioritize any actions to be taken. Example 2: If a permanent mitigation for a vulnerability is not yet available, determine how the vulnerability can be temporarily mitigated until the permanent solution is available, and add that temporary remediation to the plan. Example 3: Develop and release security advisories that provide the necessary information to software acquirers, including descriptions of what the vulnerabilities are, how to find instances of the vulnerable software, and how to address them (e.g., where to get patches and what the patches change in the software; what configuration settings may need to be changed; how temporary workarounds could be implemented). Example 4: Deliver remediations to acquirers via an automated and trusted delivery mechanism. A single remediation could address multiple vulnerabilities. Example 5: Update records of design decisions, risk responses, and approved exceptions as needed. See PW.1.2.	**BSAFSS**: VM.1-1, VM-2 **BSIMM**: CMVM2.1 **EO14028**: 4e(iv), 4e(vi), 4e(viii), 4e(ix) **IEC62443**: DM-4 **ISO30111**: 7.1.4, 7.1.5 **NISTLABEL**: 2.2.2.2 **PCISSLC**: 4.1, 4.2, 10.1 **SCAGILE**: Operational Security Task 2 **SCFPSSD**: Fix the Vulnerability, Identify Mitigating Factors or Workarounds **SCTPC**: MITIGATE **SP80053**: SA-5, SA-10, SA-11, SA-15(7) **SP800160**: 3.3.8 **SP800161**: SA-5, SA-8, SA-10, SA-11, SA-15(7) **SP800181**: T0163, T0229, T0264; K0009, K0070

Analyze Vulnerabilities to Identify Their Root Causes (RV.3): Help reduce the frequency of vulnerabilities in the future.	**RV.3.1**: Analyze identified vulnerabilities to determine their root causes.	Example 1: Record the root cause of discovered issues. Example 2: Record lessons learned through root cause analysis in a wiki that developers can access and search.	**BSAFSS**: VM.2-1 **BSIMM**: CMVM3.1, CMVM3.2 **EO14028**: 4e(ix) **IEC62443**: DM-3 **ISO30111**: 7.1.4 **OWASPSAMM**: IM3-A **PCISSLC**: 4.2 **SCFPSSD**: Secure Development Lifecycle Feedback **SP800181**: T0047, K0009, K0039, K0070, K0343
	RV.3.2: Analyze the root causes over time to identify patterns, such as a particular secure coding practice not being followed consistently.	Example 1: Record lessons learned through root cause analysis in a wiki that developers can access and search. Example 2: Add mechanisms to the toolchain to automatically detect future instances of the root cause. Example 3: Update manual processes to detect future instances of the root cause.	**BSAFSS**: VM.2-1, PD.1-3 **BSIMM**: CP3.3, CMVM3.2 **EO14028**: 4e(ix) **IEC62443**: DM-4 **ISO30111**: 7.1.7 **OWASPSAMM**: IM3-B **PCISSLC**: 2.6, 4.2 **SCFPSSD**: Secure Development Lifecycle Feedback **SP800160**: 3.3.8 **SP800181**: T0111, K0009, K0039, K0070, K0343
	RV.3.3: Review the software for similar vulnerabilities to eradicate a class of vulnerabilities, and proactively fix them rather than waiting for external reports.	Example 1: See PW.7 and PW.8.	**BSAFSS**: VM.2 **BSIMM**: CR3.3, CMVM3.1 **EO14028**: 4e(iv), 4e(viii), 4e(ix) **IEC62443**: SI-1, DM-3, DM-4 **ISO30111**: 7.1.4 **PCISSLC**: 4.2 **SP80053**: SA-11 **SP800161**: SA-11 **SP800181**: SP-DEV-001, SP-DEV-002; K0009, K0039, K0070
	RV.3.4: Review the SDLC process, and update it if appropriate to prevent (or reduce the likelihood of) the root cause recurring in updates to the software or in new software that is created.	Example 1: Record lessons learned through root cause analysis in a wiki that developers can access and search. Example 2: Plan and implement changes to the appropriate SDLC practices.	**BSAFSS**: PD.1-3 **BSIMM**: CP3.3, CMVM3.2 **EO14028**: 4e(ix) **IEC62443**: DM-6 **ISO30111**: 7.1.7 **MSSDL**: 2 **PCISSLC**: 2.6, 4.2 **SCFPSSD**: Secure Development Lifecycle Feedback **SP80053**: SA-15 **SP800161**: SA-15 **SP800181**: K0009, K0039, K0070

SECTION 4 - EVALUATION FACTORS

The Government intends to establish a single indefinite quantity contract that includes a one-year base year plus two 12-month optional periods of performance, at the discretion of the Government, resulting from this solicitation to the best qualified responsible offeror whose proposal conforms to the solicitation and represents the best value to the Government, price and other factors considered utilizing FAR 12 Comparative Evaluation.

This selection process will utilize FAR 12 procedures.

After preliminary consideration of all offers, the Department will no longer consider offers that do not meet basic standards to be eligible for award. The offers that remain will be subject to a comparative evaluation.

The preliminary evaluation process shall include the following:

COMPLIANCE REVIEW. The Government will perform an initial review of proposals/quotations received to determine completeness and compliance with the terms of the solicitation to include **CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM) Go/No-Go Evaluation Factor**. The Government may reject as unacceptable proposals/quotations that do not conform to the solicitation.

C-SCRM Go/No-Go Evaluation Factor
This factor is evaluated on a go/no-go basis. The Government will evaluate whether the submitted C-SCRM Questionnaire and State Department Secure Software Development Attestation Form meet the definition for the "Go" or "No-Go" ratings for this factor. The "Go" and "No-Go" ratings and their definitions are as follows:

RATING	RATING DEFINITION
GO	The proposal **meets** the criteria in the following two (2) paragraphs.

The C-SCRM Questionnaire contains both of the following: (1) C-SCRM Questionnaire instructions are completed; and (2) contains "Yes" answers for all questions in Sections 2 and 3 of the questionnaire; or the vendor has submitted a third party authorizing official conducted assessment such as, ISO 27001, ISO 9000, SOC II, or FEDRAMP authorization.

For suppliers offering any software, the State Department Secure Software Development Attestation Form (or another federal agency's equivalent form) is signed and submitted in accordance with the form's instructions. In lieu of submitting the State Department Secure Software Development Attestation Form, the offeror provides the information required by section "Additional Information" of the form and the Government finds that this information satisfactory mitigates associated risks.

NO-GO The proposal **does not meet** one (1) or more of the criteria in the following two (2) paragraphs.

The C-SCRM Questionnaire contains both of the following: (1) C-SCRM Questionnaire instructions are completed; and (2) contains Yes answers for all questions in Sections 2 and 3 of the questionnaire; or the vendor has submitted a third party authorizing official conducted assessment such as, ISO 27001, ISO 9000, SOC II, or FEDRAMP authorization.

For suppliers offering any software, the State Department Secure Software Development Attestation Form (or another federal agency's equivalent form) is signed and submitted in accordance with the form's instructions. In lieu of submitting the State Department Secure Software Development Attestation Form, the offeror provides the information required by section "Additional Information" of the form and the Government finds that this information satisfactory mitigates associated risks.

Evaluation Criteria
Technical. Technical will be evaluated on the basis of a direct comparison to other offers to discern if there is any kind of technical quality superiority that would support an award to a higher priced offer.

Past Performance. Past performance will be evaluated based on direct comparison to other offers to discern if there is any significant past performance superiority that would support an award to a higher priced offer. Past performance as a discriminator may be appropriate whereas based on the offeror's performance record, the Government has a high expectation that the offeror will successfully perform the required effort.

Price will be evaluated to ensure the proposed price is fair and reasonable. The price will be determined by multiplying the offered prices times the estimated quantities in "Prices - Continuation of SF-1449, block 23", and arriving at a grand total, including all options. The Government reserves the right to reject proposals that are unreasonably low or high in price.

RESPONSIBILITY DETERMINATION. The Government will determine contractor responsibility by analyzing whether the apparent successful offeror complies with the requirements of FAR 9.1, including:

• Adequate financial resources or the ability to obtain them;
• Ability to comply with the required performance period, taking into consideration all existing commercial and governmental business commitments;
• Satisfactory record of integrity and business ethics;
• Necessary organization, experience, and skills or the ability to obtain them;
• Necessary equipment and facilities or the ability to obtain them; and
Otherwise, qualified and eligible to receive an award under applicable laws and regulations.

ADDENDUM TO EVALUATION FACTORS
FAR AND DOSAR PROVISION(S) NOT PRESCRIBED IN PART 12

THE FOLLOWING FAR PROVISION(S) IS/ARE PROVIDED IN FULL TEXT:

52.217-5 EVALUATION OF OPTIONS (JUL 1990)

The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. Evaluation of options will not obligate the Government to exercise the option(s).

52.225-17 EVALUATION OF FOREIGN CURRENCY OFFERS (FEB 2000)

If the Government receives offers in more than one currency, the Government will evaluate offers by converting the foreign currency to United States currency using the exchange rate used by the Embassy in effect as follows:

(a) For acquisitions conducted using sealed bidding procedures, on the date of bid opening.

(b) For acquisitions conducted using negotiation procedures—

(1) On the date specified for receipt of offers, if award is based on initial offers; otherwise

(2) On the date specified for receipt of proposal revisions.

SECTION 5 - REPRESENTATIONS AND CERTIFICATIONS

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

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

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

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

(b) *Prohibition*.

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

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

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

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an entity that uses any equipment,

system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or
(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

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

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

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

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

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

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

(i) For covered equipment—

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

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

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

(ii) For covered services—

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

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.
(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded "does" in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

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

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

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

(ii) For covered services—

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

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

(End of provision)

52.204-26 COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICES REPRESENTATION (OCT 2020)

(a) *Definitions.* As used in this provision, "covered telecommunications equipment or services" and "reasonable inquiry" have the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

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

(c) *Representations.* (1) The Offeror represents that it [ ] does, [ ] does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(2) After conducting a reasonable inquiry for purposes of this representation, the Offeror represents that it [ ] does, [ ] does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

(End of provision)

52.212-3 Offeror Representations and Certifications—Commercial Products and Commercial Services. As prescribed in 12.301(b)(2), insert the following provision:

Offeror Representations and Certifications—Commercial Products and Commercial Services (Oct 2025) (DEVIATION FEB 2025)

The Offeror shall complete only paragraph (b) of this provision if the Offeror has completed the annual representations and certification electronically in the System for Award Management (SAM) accessed through https://www.sam.gov. If the Offeror has not completed the annual representations and certifications electronically, the Offeror shall complete only paragraphs (c) through (v) of this provision.

(a) Definitions. As used in this provision—

Covered telecommunications equipment or services has the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

Economically disadvantaged women-owned small business (EDWOSB) concern means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management

and daily business operations of which are controlled by, one or more women who are citizens of the United States and who are economically disadvantaged in accordance with 13 CFR part 127, and the concern is certified by SBA or an approved third-party certifier in accordance with 13 CFR 127.300. It automatically qualifies as a women-owned small business eligible under the WOSB Program.

Forced or indentured child labor means all work or service—

(1) Exacted from any person under the age of 18 under the menace of any penalty for its nonperformance and for which the worker does not offer himself voluntarily; or

(2) Performed by any person under the age of 18 pursuant to a contract the enforcement of which can be accomplished by process or penalties.

Highest-level owner means the entity that owns or controls an immediate owner of the offeror, or that owns or controls one or more entities that control an immediate owner of the offeror. No entity owns or exercises control of the highest level owner.

Immediate owner means an entity, other than the offeror, that has direct control of the offeror. Indicators of control include, but are not limited to, one or more of the following: ownership or interlocking management, identity of interests among family members, shared facilities and equipment, and the common use of employees.

Inverted domestic corporation, means a foreign incorporated entity that meets the definition of an inverted domestic corporation under 6 U.S.C. 395(b), applied in accordance with the rules and definitions of 6 U.S.C. 395(c).

Manufactured end product means any end product in product and service codes (PSCs) 1000-9999, except—

(1) PSC 5510, Lumber and Related Basic Wood Materials;

(2) Product or Service Group (PSG) 87, Agricultural Supplies;

(3) PSG 88, Live Animals;

(4) PSG 89, Subsistence;

(5) PSC 9410, Crude Grades of Plant Materials;

(6) PSC 9430, Miscellaneous Crude Animal Products, Inedible;

(7) PSC 9440, Miscellaneous Crude Agricultural and Forestry Products;

(8) PSC 9610, Ores;

(9) PSC 9620, Minerals, Natural and Synthetic; and

(10) PSC 9630, Additive Metal Materials.

Place of manufacture means the place where an end product is assembled out of components, or otherwise made or processed from raw materials into the finished product that is to be provided to the Government. If a product is disassembled and reassembled, the place of reassembly is not the place of manufacture.

Predecessor means an entity that is replaced by a successor and includes any predecessors of the predecessor.

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

Restricted business operations means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person (as that term is defined in Section 2 of the Sudan Accountability and Divestment Act of 2007) conducting the business can demonstrate—

(1) Are conducted under contract directly and exclusively with the regional government of southern Sudan;

(2) Are conducted pursuant to specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization;

(3) Consist of providing goods or services to marginalized populations of Sudan;

(4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;

(5) Consist of providing goods or services that are used only to promote health or education; or

(6) Have been voluntarily suspended."Sensitive technology"—

Sensitive technology—

(1) Means hardware, software, telecommunications equipment, or any other technology that is to be used specifically—

(i) To restrict the free flow of unbiased information in Iran; or

(ii) To disrupt, monitor, or otherwise restrict speech of the people of Iran; and

(2) Does not include information or informational materials the export of which the President does not have the authority to regulate or prohibit pursuant to section 203(b)(3)of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)(3)).

Service-disabled veteran-owned small business (SDVOSB) concern means a small business concern—

(1) (i) Not less than 51 percent of which is owned and controlled by one or more service-disabled veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veterans; and
(ii) The management and daily business operations of which are controlled by one or more service-disabled veterans or, in the case of a service-disabled veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran; or

(2) A small business concern eligible under the SDVOSB Program in accordance with 13 CFR part 128 (see subpart 19.14).

(3) Service-disabled veteran, as used in this definition, means a veteran as defined in 38 U.S.C. 101(2), with a disability that is service connected, as defined in 38 U.S.C. 101(16), and who is registered in the Beneficiary Identification and Records Locator Subsystem, or successor system that is maintained by the Department of Veterans Affairs' Veterans Benefits Administration, as a service-disabled veteran.

Service-disabled veteran-owned small business (SDVOSB) concern eligible under the SDVOSB Program means an SDVOSB concern that—

(1) Effective January 1, 2024, is designated in the System for Award Management (SAM) as certified by the Small Business Administration (SBA) in accordance with 13 CFR 128.300; or

(2) Has represented that it is an SDVOSB concern in SAM and submitted a complete application for certification to SBA on or before December 31, 2023.

Service-disabled veteran-owned small business (SDVOSB) Program means a program that authorizes contracting officers to limit competition, including award on a sole-source basis, to SDVOSB concerns eligible under the SDVOSB Program.

Small business concern—

(1) Means a concern, including its affiliates, that is independently owned and operated, not dominant in its field of operation, and qualified as a small business under the criteria in 13 CFR part 121 and size standards in this solicitation.

(2) Affiliates, as used in this definition, means business concerns, one of whom directly or indirectly controls or has the power to control the others, or a third party or parties control or have the power to control the others. In determining whether affiliation exists, consideration is given to all appropriate factors including common ownership, common management, and contractual relationships. SBA determines affiliation based on the factors set forth at 13 CFR 121.103.

Small disadvantaged business concern, consistent with 13 CFR 124.1001, means a small business concern under the size standard applicable to the acquisition, that—

(1) Is at least 51 percent unconditionally and directly owned (as defined at 13 CFR 124.105) by—

(i) One or more socially disadvantaged (as defined at13 CFR 124.103) and economically disadvantaged (as defined at 13 CFR 124.104) individuals who are citizens of the United States; and

(ii) Each individual claiming economic disadvantage has a net worth not exceeding the threshold at 13 CFR 124.104(c)(2) after taking into account the applicable exclusions set forth at 13 CFR124.104(c)(2); and

(2) The management and daily business operations of which are controlled (as defined at 13.CFR 124.106) by individuals, who meet the criteria in paragraphs (1)(i) and (ii) of this definition.

Subsidiary means an entity in which more than 50 percent of the entity is owned—

(1) Directly by a parent corporation; or

(2) Through another subsidiary of a parent corporation

Successor means an entity that has replaced a predecessor by acquiring the assets and carrying out the affairs of the predecessor under a new name (often through acquisition or merger). The term "successor" does not include new offices/divisions of the same company or a company that only changes its name. The extent of the responsibility of the successor for the liabilities of the predecessor may vary, depending on State law and specific circumstances.

Veteran-owned small business concern means a small business concern—

(1) Not less than 51 percent of which is owned and controlled by one or more veterans (as defined at 38 U.S.C. 101(2)) or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and

(2) The management and daily business operations of which are controlled by one or more veterans.

Women-owned business concern means a concern which is at least 51 percent owned by one or more women; or in the case of any publicly owned business, at least 51 percent of its stock is owned by one

or more women; and whose management and daily business operations are controlled by one or more women

Women-owned small business concern means a small business concern—

(1) That is at least 51 percent owned by one or more women; or, in the case of any publicly owned business, at least51 percent of the stock of which is owned by one or more women; and

(2) Whose management and daily business operations are controlled by one or more women.

Women-owned small business (WOSB) concern eligible under the WOSB Program (in accordance with 13 CFR part 127), means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States, and the concern is certified by SBA or an approved third-party certifier in accordance with 13 CFR 127.300.

(b) (1) Annual Representations and Certifications. Any changes provided by the Offeror in paragraph (b)(2) of this provision do not automatically change the representations and certifications in SAM.
(2) The offeror has completed the annual representations and certifications electronically in SAM accessed through http://www.sam.gov. After reviewing SAM information, the Offeror verifies by submission of this offer that the representations and certifications currently posted electronically at FAR 52.212-3, Offeror Representations and Certifications-Commercial Products and Commercial Services, have been entered or updated in the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard(s) applicable to the NAICS code(s) referenced for this solicitation), at the time this offer is submitted and are incorporated in this offer by reference (see FAR 4.1201), except for paragraphs __.

[Offeror to identify the applicable paragraphs at (c) through (v) of this provision that the offeror has completed for the purposes of this solicitation only, if any.

These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer.

Any changes provided by the offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications posted electronically on SAM.]

(c) Offerors must complete the following representations when the resulting contract is for supplies to be delivered or services to be performed in the United States or its outlying areas, or when the contracting officer has applied part 19 in accordance with 19.000(b)(1)(ii). Check all that apply.

(1) Small business concern. The offeror represents as part of its offer that—

(i) It □ is, □ is not a small business concern; or

(ii) It □ is, □ is not a small business joint venture that complies with the requirements of 13 CFR 121.103(h) and 13 CFR 125.8(a) and (b). [The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.]

(2) Veteran-owned small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents as part of its offer that it □ is, □ is not a veteran-owned small business concern.

(3) SDVOSB concern. [Complete only if the offeror represented itself as a veteran-owned small business concern in paragraph (c)(2) of this provision.] The offeror represents that it □ is, □ is not an SDVOSB concern.

(4) SDVOSB concern joint venture eligible under the SDVOSB Program. The offeror represents that it □ is, □ is not an SDVOSB joint venture eligible under the SDVOSB Program that complies with the requirements of 13 CFR 128.402. [Complete only if the offeror represented itself as an SDVOSB concern in paragraph (c)(3) of this provision.] [The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.]

(5) Small disadvantaged business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents that it □ is, □ is not a small disadvantaged business concern as defined in 13 CFR 124.1001.

(6) Women-owned small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents that it □ is, □ is not a women-owned small business concern.

(7) WOSB joint venture eligible under the WOSB Program. The offeror represents that it □ is, □ is not a joint venture that complies with the requirements of 13 CFR 127.506(a) through (c). [The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.]

(8) Economically disadvantaged women-owned small business (EDWOSB) joint venture. The offeror represents that it □ is, □ is not a joint venture that complies with the requirements of 13 CFR 127.506(a) through (c). [The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.]

Note to paragraphs (c)(9) and (10): Complete paragraphs (c)(9) and (10) only if this solicitation is expected to exceed the simplified acquisition threshold.

(9) Women-owned business concern (other than small business concern). [Complete only if the offeror is a women-owned business concern and did not represent itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents that it □ is a women-owned business concern.

(10) Tie bid priority for labor surplus area concerns. If this is an invitation for bid, small business offerors may identify the labor surplus areas in which costs to be incurred on account of manufacturing

or production (by offeror or first-tier subcontractors) amount to more than 50 percent of the contract price:_____

(11) HUBZone small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents, as part of its offer, that–

(i) It □ is, □ is not a HUBZone small business concern listed, on the date of this representation, as having been certified by SBA as a HUBZone small business concern in the Dynamic Small Business Search and SAM, and will attempt to maintain an employment rate of HUBZone residents of 35 percent of its employees during performance of a HUBZone contract (see 13 CFR 126.200(e)(1)); and

(ii) It □ is, □ is not a HUBZone joint venture that complies with the requirements of 13 CFR 126.616(a) through (c). [The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.] Each HUBZone small business concern participating in the HUBZone joint venture shall provide representation of its HUBZone status.

(d) Representations required to implement provisions of Executive Order 11246- (1) Previous contracts and compliance. The offeror represents that-
(i) It □ has, □ has not participated in a previous contract or subcontract subject to the Equal Opportunity clause of this solicitation; and

(ii) It □ has, □ has not filed all required compliance reports.

(2) Affirmative Action Compliance. The offeror represents that-

(i) It □ has developed and has on file, □ has not developed and does not have on file, at each establishment, affirmative action programs required by rules and regulations of the Secretary of Labor (41 CFR parts 60-1 and 60-2), or

(ii) It □ has not previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor.

(e) Certification Regarding Payments to Influence Federal Transactions (31 http://uscode.house.gov/ U.S.C. 1352). (Applies only if the contract is expected to exceed $200,000.) By submission of its offer, the offeror certifies to the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress or an employee of a Member of Congress on his or her behalf in connection with the award of any resultant contract. If any registrants under the Lobbying Disclosure Act of 1995 have made a lobbying contact on behalf of the offeror with respect to this contract, the offeror shall complete and submit, with its offer, OMB Standard Form LLL, Disclosure of Lobbying Activities, to provide the name of the registrants. The offeror need not report regularly employed officers or employees of the offeror to whom payments of reasonable compensation were made.

(f) Buy American Certificate. (Applies only if the clause at Federal Acquisition Regulation (FAR) 52.225-1, Buy American-Supplies, is included in this solicitation.)

(1) (i) The Offeror certifies that each end product, except those listed in paragraph (f)(2) of this provision, is a domestic end product and that each domestic end product listed in paragraph (f)(3) of this provision contains a critical component.
(ii) The Offeror shall list as foreign end products those end products manufactured in the United States that do not qualify as domestic end products. For those foreign end products that do not consist wholly or predominantly of iron or steel or a combination of both, the Offeror shall also indicate whether these foreign end products exceed 55 percent domestic content, except for those that are COTS items. If the percentage of the domestic content is unknown, select “no”.

(iii) The Offeror shall separately list the line item numbers of domestic end products that contain a critical component (see FAR 25.105).

(iv) The terms “commercially available off-the-shelf (COTS) item,” “critical component,” “domestic end product,” "end product," "foreign end product," and "United States" are defined in the clause of this solicitation entitled "Buy American-Supplies."

(2) Foreign End Products:

Line Item No. Country of Origin Exceeds 55% domestic content (yes/no)

_____

_____

_____

_____

_____

_____

_____

_____

_____

[List as necessary]

(3) Domestic end products containing a critical component:

Line Item No. ___

[List as necessary]

(4) The Government will evaluate offers in accordance with the policies and procedures of FAR part 25.

(g) (1) Buy American-Free Trade Agreements-Israeli Trade Act Certificate. (Applies only if the clause at FAR 52.225-3, Buy American-Free Trade Agreements-Israeli Trade Act, is included in this solicitation.)
(i) (A) The Offeror certifies that each end product, except those listed in paragraph (g)(1)(ii) or (iii) of this provision, is a domestic end product and that each domestic end product listed in paragraph (g)(1)(iv) of this provision contains a critical component.
(B) The terms "Bahraini, Moroccan, Omani, Panamanian, or Peruvian end product," "commercially available off-the-shelf (COTS) item," "critical component," "domestic end product," "end product," "foreign end product," "Free Trade Agreement country," "Free Trade Agreement country end product," "Israeli end product," and "United States" are defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements-Israeli Trade Act."

(ii) The Offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahraini, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements-Israeli Trade Act."

Free Trade Agreement Country End Products (Other than Bahraini, Moroccan, Omani, Panamanian, or Peruvian End Products) or Israeli End Products:

Line Item No. Country of Origin
_____

_____

_____

_____

_____

_____

[List as necessary]

(iii) The Offeror shall list those supplies that are foreign end products (other than those listed in paragraph (g)(1)(ii) of this provision) as defined in the clause of this solicitation entitled "Buy

American-Free Trade Agreements-Israeli Trade Act." The Offeror shall list as other foreign end products those end products manufactured in the United States that do not qualify as domestic end products. For those foreign end products that do not consist wholly or predominantly of iron or steel or a combination of both, the Offeror shall also indicate whether these foreign end products exceed 55 percent domestic content, except for those that are COTS items. If the percentage of the domestic content is unknown, select “no”.

Other Foreign End Products:

Line Item No. Country of Origin Exceeds 55% domestic content (yes/no)

_____

_____

_____

_____

_____

_____

_____

_____

_____

[List as necessary]

(iv) The Offeror shall list the line item numbers of domestic end products that contain a critical component (see FAR 25.105).

Line Item No. ___

[List as necessary]

(v) The Government will evaluate offers in accordance with the policies and procedures of FAR part 25.

(2) Buy American-Free Trade Agreements-Israeli Trade Act Certificate, Alternate II. If Alternate II to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Israeli end products as defined in the clause of this solicitation entitled “Buy American—Free Trade Agreements—Israeli Trade Act”:

Israeli End Products:

Line Item No.

_____

_____

_____

[List as necessary]

(3) Buy American-Free Trade Agreements-Israeli Trade Act Certificate, Alternate III. If Alternate III to the clause at 52.225-3 is included in this solicitation, substitute the following paragraphs (g)(1)(i)(B) and (g)(1)(ii) for paragraphs (g)(1)(i)(B) and (g)(1)(ii) of the basic provision:

(g)(1)(i)(B) The terms “Korean end product”, “commercially available off-the-shelf (COTS) item,” “critical component,” “domestic end product,” “end product,” “foreign end product,” “Free Trade Agreement country,” “Free Trade Agreement country end product,” “Israeli end product,” and “United States” are defined in the clause of this solicitation entitled “Buy American—Free Trade Agreements—Israeli Trade Act.”

(g)(1)(ii) The Offeror certifies that the following supplies are Korean end products or Israeli end products as defined in the clause of this solicitation entitled “Buy American—Free Trade Agreements—Israeli Trade Act”:

Korean End Products or Israeli End Products:

Line Item No. Country of Origin

_____

_____

_____

_____

_____

_____

[List as necessary]

(4) Trade Agreements Certificate. (Applies only if the clause at FAR 52.225-5, Trade Agreements, is included in this solicitation.)

(i) The offeror certifies that each end product, except those listed in paragraph (g)(4)(ii) of this provision, is a U.S.-made or designated country end product, as defined in the clause of this solicitation entitled "Trade Agreements."

(ii) The offeror shall list as other end products those end products that are not U.S.-made or designated country end products.

Other End Products:

Line Item No. Country of Origin

_____

_____

_____

_____

_____

_____

[List as necessary]

(iii) The Government will evaluate offers in accordance with the policies and procedures of FAR part 25. For line items covered by the WTO GPA, the Government will evaluate offers of U.S.-made or designated country end products without regard to the restrictions of the Buy American statute. The Government will consider for award only offers of U.S.-made or designated country end products unless the Contracting Officer determines that there are no offers for such products or that the offers for such products are insufficient to fulfill the requirements of the solicitation.

(h) Certification Regarding Responsibility Matters (Executive Order 12689). (Applies only if the contract value is expected to exceed the simplified acquisition threshold.) The offeror certifies, to the best of its knowledge and belief, that the offeror and/or any of its principals–

(1) □ Are, □ are not presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;

(2) □ Have, □ have not, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with

obtaining, attempting to obtain, or performing a Federal, state or local government contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating Federal criminal tax laws, or receiving stolen property;

(3) □ Are, □ are not presently indicted for, or otherwise criminally or civilly charged by a Government entity with, commission of any of these offenses enumerated in paragraph (h)(2) of this clause; and

(4) □ Have, □ have not, within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds the threshold at 9.104-5(a)(2) for which the liability remains unsatisfied.

(i) Taxes are considered delinquent if both of the following criteria apply:

(A) The tax liability is finally determined. The liability is finally determined if it has been assessed. A liability is not finally determined if there is a pending administrative or judicial challenge. In the case of a judicial challenge to the liability, the liability is not finally determined until all judicial appeal rights have been exhausted.

(B) The taxpayer is delinquent in making payment. A taxpayer is delinquent if the taxpayer has failed to pay the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where enforced collection action is precluded.

(ii) Examples. (A) The taxpayer has received a statutory notice of deficiency, under I.R.C. §6212, which entitles the taxpayer to seek Tax Court review of a proposed tax deficiency. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek Tax Court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.
(B) The IRS has filed a notice of Federal tax lien with respect to an assessed tax liability, and the taxpayer has been issued a notice under I.R.C. §6320 entitling the taxpayer to request a hearing with the IRS Office of Appeals contesting the lien filing, and to further appeal to the Tax Court if the IRS determines to sustain the lien filing. In the course of the hearing, the taxpayer is entitled to contest the underlying tax liability because the taxpayer has had no prior opportunity to contest the liability. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek tax court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(C) The taxpayer has entered into an installment agreement pursuant to I.R.C. §6159. The taxpayer is making timely payments and is in full compliance with the agreement terms. The taxpayer is not delinquent because the taxpayer is not currently required to make full payment.

(D) The taxpayer has filed for bankruptcy protection. The taxpayer is not delinquent because enforced collection action is stayed under 11 U.S.C. §362 (the Bankruptcy Code).

(i) Certification Regarding Knowledge of Child Labor for Listed End Products (Executive Order 13126). [The Contracting Officer must list in paragraph (i)(1) any end products being acquired under

this solicitation that are included in the List of Products Requiring Contractor Certification as to Forced or Indentured Child Labor, unless excluded at 22.1503(b).]

(1) Listed end products.

Listed End Product Listed Countries of Origin

_____

_____

_____

_____

(2) Certification. [If the Contracting Officer has identified end products and countries of origin in paragraph (i)(1) of this provision, then the offeror must certify to either (i)(2)(i) or (i)(2)(ii) by checking the appropriate block.]

☐ (i) The offeror will not supply any end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product.
☐ (ii) The offeror may supply an end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product. The offeror certifies that it has made a good faith effort to determine whether forced or indentured child labor was used to mine, produce, or manufacture any such end product furnished under this contract. On the basis of those efforts, the offeror certifies that it is not aware of any such use of child labor.
(j) Place of manufacture. (Does not apply unless the solicitation is predominantly for the acquisition of manufactured end products.) For statistical purposes only, the offeror shall indicate whether the place of manufacture of the end products it expects to provide in response to this solicitation is predominantly-

(1) □ In the United States (Check this box if the total anticipated price of offered end products manufactured in the United States exceeds the total anticipated price of offered end products manufactured outside the United States); or

(2) □ Outside the United States.

(k) Certificates regarding exemptions from the application of the Service Contract Labor Standards (Certification by the offeror as to its compliance with respect to the contract also constitutes its certification as to compliance by its subcontractor if it subcontracts out the exempt services.) [The contracting officer is to check a box to indicate if paragraph (k)(1) or (k)(2) applies.]

☐ (1) Maintenance, calibration, or repair of certain equipment as described in FAR 22.1003-4(c)(1). The offeror □ does □ does not certify that–

(i) The items of equipment to be serviced under this contract are used regularly for other than Governmental purposes and are sold or traded by the offeror (or subcontractor in the case of an exempt subcontract) in substantial quantities to the general public in the course of normal business operations;

(ii) The services will be furnished at prices which are, or are based on, established catalog or market prices (see FAR 22.1003-4(c)(2)(ii)) for the maintenance, calibration, or repair of such equipment; and

(iii) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract will be the same as that used for these employees and equivalent employees servicing the same equipment of commercial customers.

☐ (2) Certain services as described in FAR 22.1003-4(d)(1). The offeror □ does □ does not certify that-
(i) The services under the contract are offered and sold regularly to non-Governmental customers, and are provided by the offeror (or subcontractor in the case of an exempt subcontract) to the general public in substantial quantities in the course of normal business operations;

(ii) The contract services will be furnished at prices that are, or are based on, established catalog or market prices (see FAR 22.1003-4(d)(2)(iii));

(iii) Each service employee who will perform the services under the contract will spend only a small portion of his or her time (a monthly average of less than 20 percent of the available hours on an annualized basis, or less than 20 percent of available hours during the contract period if the contract period is less than a month) servicing the Government contract; and

(iv) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract is the same as that used for these employees and equivalent employees servicing commercial customers.

(3) If paragraph (k)(1) or (k)(2) of this clause applies–

(i) If the offeror does not certify to the conditions in paragraph (k)(1) or (k)(2) and the Contracting Officer did not attach a Service Contract Labor Standards wage determination to the solicitation, the offeror shall notify the Contracting Officer as soon as possible; and

(ii) The Contracting Officer may not make an award to the offeror if the offeror fails to execute the certification in paragraph (k)(1) or (k)(2) of this clause or to contact the Contracting Officer as required in paragraph (k)(3)(i) of this clause.

(l) Taxpayer Identification Number (TIN) (26 U.S.C. 6109, 31 U.S.C. 7701). (Not applicable if the offeror is required to provide this information to the SAM to be eligible for award.)

(1) All offerors must submit the information required in paragraphs (l)(3) through (l)(5) of this provision to comply with debt collection requirements of 31 U.S.C. 7701(c) and 3325(d), reporting

requirements of 26 U.S.C. 6041, 6041A, and 6050M, and implementing regulations issued by the Internal Revenue Service (IRS).

(2) The TIN may be used by the Government to collect and report on any delinquent amounts arising out of the offeror's relationship with the Government (31 U.S.C. 7701(c)(3)). If the resulting contract is subject to the payment reporting requirements described in FAR 4.904, the TIN provided hereunder may be matched with IRS records to verify the accuracy of the offeror's TIN.

(3) Taxpayer Identification Number (TIN).

☐TIN: _____.

☐TIN has been applied for.

☐TIN is not required because:

☐Offeror is a nonresident alien, foreign corporation, or foreign partnership that does not have income effectively connected with the conduct of a trade or business in the United States and does not have an office or place of business or a fiscal paying agent in the United States;

☐Offeror is an agency or instrumentality of a foreign government;

☐Offeror is an agency or instrumentality of the Federal Government.

(4) Type of organization.

☐Sole proprietorship;

☐Partnership;

☐Corporate entity (not tax-exempt);

☐Corporate entity (tax-exempt);

☐Government entity (Federal, State, or local);

☐Foreign government;

☐International organization per 26 CFR1.6049-4;

☐Other _____.

(5) Common parent.

☐Offeror is not owned or controlled by a common parent;

☐Name and TIN of common parent:

Name _____.

TIN _____.

(m) Restricted business operations in Sudan. By submission of its offer, the offeror certifies that the offeror does not conduct any restricted business operations in Sudan.

(n) Prohibition on Contracting with Inverted Domestic Corporations. (1) Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with either an inverted

domestic corporation, or a subsidiary of an inverted domestic corporation, unless the exception at 9.108-2(b) applies or the requirement is waived in accordance with the procedures at 9.108-4.
(2) Representation. The Offeror represents that–

(i) It □ is, □ is not an inverted domestic corporation; and

(ii) It □ is, □ is not a subsidiary of an inverted domestic corporation.

(o) Prohibition on contracting with entities engaging in certain activities or transactions relating to Iran.
(1) The offeror shall e-mail questions concerning sensitive technology to the Department of State at CISADA106@state.gov.
(2) Representation and Certifications. Unless a waiver is granted or an exception applies as provided in paragraph (o)(3) of this provision, by submission of its offer, the offeror-

(i) Represents, to the best of its knowledge and belief, that the offeror does not export any sensitive technology to the government of Iran or any entities or individuals owned or controlled by, or acting on behalf or at the direction of, the government of Iran;

(ii) Certifies that the offeror, or any person owned or controlled by the offeror, does not engage in any activities for which sanctions may be imposed under section 5 of the Iran Sanctions Act; and

(iii) Certifies that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any transaction that exceeds the threshold at FAR 25.703-2(a)(2) with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (et seq.) (see OFAC's Specially Designated Nationals and Blocked Persons List at https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx).

(3) The representation and certification requirements of paragraph (o)(2) of this provision do not apply if-

(i) This solicitation includes a trade agreements certification (e.g., 52.212-3(g) or a comparable agency provision); and

(ii) The offeror has certified that all the offered products to be supplied are designated country end products.

(p) Ownership or Control of Offeror. (Applies in all solicitations when there is a requirement to be registered in SAM or a requirement to have a unique entity identifier in the solicitation).

(1) The Offeror represents that it □ has or □ does not have an immediate owner. If the Offeror has more than one immediate owner (such as a joint venture), then the Offeror shall respond to paragraph (2) and if applicable, paragraph (3) of this provision for each participant in the joint venture.

(2) If the Offeror indicates "has" in paragraph (p)(1) of this provision, enter the following information:

Immediate owner CAGE code: _____.

Immediate owner legal name: _____.

(Do not use a "doing business as" name)

Is the immediate owner owned or controlled by another entity: □ Yes or □ No.

(3) If the Offeror indicates "yes" in paragraph (p)(2) of this provision, indicating that the immediate owner is owned or controlled by another entity, then enter the following information:

Highest-level owner CAGE code: _____.

Highest-level owner legal name: _____.

(Do not use a "doing business as" name)

(q) Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law.

(1) As required by sections 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), and similar provisions, if contained in subsequent appropriations acts, The Government will not enter into a contract with any corporation that–

(i) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or

(ii) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(2) The Offeror represents that–

(i) It is □ is not □ a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and

(ii) It is □ is not □ a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(r) Predecessor of Offeror. (Applies in all solicitations that include the provision at 52.204-16, Commercial and Government Entity Code Reporting.)

(1) The Offeror represents that it □ is or □ is not a successor to a predecessor that held a Federal contract or grant within the last three years.

(2) If the Offeror has indicated "is" in paragraph (r)(1) of this provision, enter the following information for all predecessors that held a Federal contract or grant within the last three years (if more than one predecessor, list in reverse chronological order):

Predecessor CAGE code: (or mark "Unknown").

Predecessor legal name: ____.

(Do not use a "doing business as" name).

(s) [Reserved].

(t) Public Disclosure of Greenhouse Gas Emissions and Reduction Goals. Applies in all solicitations that require offerors to register in SAM (12.301(d)(1)).

(1) This representation shall be completed if the Offeror received $7.5 million or more in contract awards in the prior Federal fiscal year. The representation is optional if the Offeror received less than $7.5 million in Federal contract awards in the prior Federal fiscal year.

(2) Representation. [Offeror to check applicable block(s) in paragraph (t)(2)(i) and (ii)]. (i) The Offeror (itself or through its immediate owner or highest-level owner) □ does, □ does not publicly disclose greenhouse gas emissions, i.e., makes available on a publicly accessible website the results of a greenhouse gas inventory, performed in accordance with an accounting standard with publicly available and consistently applied criteria, such as the Greenhouse Gas Protocol Corporate Standard.
(ii) The Offeror (itself or through its immediate owner or highest-level owner) □ does, □ does not publicly disclose a quantitative greenhouse gas emissions reduction goal, i.e., make available on a publicly accessible website a target to reduce absolute emissions or emissions intensity by a specific quantity or percentage.

(iii) A publicly accessible website includes the Offeror's own website or a recognized, third-party greenhouse gas emissions reporting program.

(3) If the Offeror checked "does" in paragraphs (t)(2)(i) or (t)(2)(ii) of this provision, respectively, the Offeror shall provide the publicly accessible website(s) where greenhouse gas emissions and/or reduction goals are reported:_____.

(u) (1) In accordance with 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), Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with an entity that requires employees or subcontractors of such entity seeking to report waste, fraud, or abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting such waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information. (2) The prohibition in paragraph (u)(1) of this provision does not contravene requirements applicable to Standard Form 312 (Classified Information Nondisclosure Agreement), Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement), or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(3) Representation. By submission of its offer, the Offeror represents that it will not require its employees or subcontractors to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the performance of a Government contract to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (e.g., agency Office of the Inspector General).

(v) Covered Telecommunications Equipment or Services-Representation. Section 889(a)(1)(A) and section 889 (a)(1)(B) of Public Law 115-232.

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

(2) The Offeror represents that–

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

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

(End of Provision)

Alternate I (Feb 2024). As prescribed in 12.301 (b)(2), add the following paragraph (c)(12) to the basic provision:

(12) (Complete if the offeror has represented itself as disadvantaged in paragraph (c)(5) of this provision.)

□ Black American.

□ Hispanic American.

□ Native American (American Indians, Eskimos, Aleuts, or Native Hawaiians).

□ Asian-Pacific American (persons with origins from Burma, Thailand, Malaysia, Indonesia, Singapore, Brunei, Japan, China, Taiwan, Laos, Cambodia (Kampuchea), Vietnam, Korea, The Philippines, Republic of Palau, Republic of the Marshall Islands, Federated States of Micronesia, the Commonwealth of the Northern Mariana Islands, Guam, Samoa, Macao, Hong Kong, Fiji, Tonga, Kiribati, Tuvalu, or Nauru).

□ Subcontinent Asian (Asian-Indian) American (persons with origins from India, Pakistan, Bangladesh, Sri Lanka, Bhutan, the Maldives Islands, or Nepal).

□ Individual/concern, other than one of the preceding.

52.225-4 BUY AMERICAN-FREE TRADE AGREEMENTS-ISRAELI TRADE ACT CERTIFICATE (NOV 2023)

(a) (1) The Offeror certifies that each end product, except those listed in paragraph (b) or (c)(1) of this provision, is a domestic end product and that each domestic end product listed in paragraph (c)(2) of this provision contains a critical component.
(2) The terms "Bahraini, Moroccan, Omani, Panamanian, or Peruvian end product," "commercially available off-the-shelf (COTS) item," "critical component," "domestic end product," "end product," "foreign end product," "Free Trade Agreement country," "Free Trade Agreement country end product," "Israeli end product," and "United States" are defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements-Israeli Trade Act."
(b) The Offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahrainian, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements-Israeli Trade Act":
Free Trade Agreement Country End Products (Other than Bahraini, Moroccan, Omani, Panamanian, or Peruvian End Products) or Israeli End Products:
Line Item No.

Country of Origin

_____

_____

_____

_____

_____

_____
[List as necessary]
(c)
(1) The Offeror shall list those supplies that are foreign end products (other than those listed in paragraph (b) of this provision) as defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements-Israeli Trade Act." The Offeror shall list as other foreign end products those end products manufactured in the United States that do not qualify as domestic end products. For those foreign end products that do not consist wholly or predominantly of iron or steel or a combination of both, the Offeror shall also indicate whether these foreign end products exceed 55 percent domestic content, except for those that are COTS items. If the percentage of the domestic content is unknown, select “no”.
Other Foreign End Products:
Line Item No.

Country of Origin

Exceeds 55% domestic content (yes/no)

_____

_____

_____

_____

_____

_____

_____

[List as necessary]

(2) The Offeror shall list the line item numbers of domestic end products that contain a critical component (see FAR 25.105).
Line Item No. ___
[List as necessary]
(d) The Government will evaluate offers in accordance with the policies and procedures of part 25 of the Federal Acquisition Regulation.
(End of provision)
Alternate I [Reserved]
Alternate II (Dec 2022). As prescribed in 25.1101 (b)(2)(ii), substitute the following paragraph (b) for paragraph (b) of the basic provision:
(b) The offeror certifies that the following supplies are Israeli end products as defined in the clause of this solicitation entitled “Buy American—Free Trade Agreements—Israeli Trade Act—Balance of Payments Program”:
ISRAELI END PRODUCTS:
Line Item No.

_____

_____

_____
[List as necessary]
Alternate III(Nov 2023) . As prescribed in 25.1101 (b)(2)(iii), substitute the following paragraph (b) for paragraph (b) of the basic provision:
(b) The Offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahraini, Korean, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements-Israeli Trade Act":

FREE TRADE AGREEMENT COUNTRY END PRODUCTS (OTHER THAN BAHRAINI, KOREAN, MOROCCAN, OMANI, PANAMANIAN, OR PERUVIAN END PRODUCTS) OR ISRAELI END PRODUCTS:
Line Item No.

Country of Origin

_____

_____

_____

_____

_____

_____
[List as necessary]

52.229-11 TAX ON CERTAIN FOREIGN PROCUREMENTS – NOTICE AND REPRESENTATION (JUN 2020)

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

Foreign person means any person other than a United States person.

Specified Federal procurement payment means any payment made pursuant to a contract with a foreign contracting party that is for goods, manufactured or produced, or services provided in a foreign country that is not a party to an international procurement agreement with the United States. For purposes of the prior sentence, a foreign country does not include an outlying area.

United States person as defined in 26 U.S.C. 7701(a)(30) means—

(1) A citizen or resident of the United States;

(2) A domestic partnership;

(3) A domestic corporation;

(4) Any estate (other than a foreign estate, within the meaning of 26 U.S.C. 701(a)(31)); and

(5) Any trust if—

(i) A court within the United States is able to exercise primary supervision over the administration of the trust; and

(ii) One or more United States persons have the authority to control all substantial decisions of the trust.

(b) Unless exempted, there is a 2 percent tax of the amount of a specified Federal procurement payment on any foreign person receiving such payment. See 26 U.S.C. 5000C and its implementing regulations at 26 CFR 1.5000C-1 through 1.5000C-7.

(c) Exemptions from withholding under this provision are described at 26 CFR 1.5000C-1(d)(5) through (7). The Offeror would claim an exemption from the withholding by using the Department of

the Treasury Internal Revenue Service Form W-14, Certificate of Foreign Contracting Party Receiving Federal Procurement Payments, available via the internet at www.irs.gov/w14 . Any exemption claimed and self-certified on the IRS Form W-14 is subject to audit by the IRS. Any disputes regarding the imposition and collection of the 26 U.S.C. 5000C tax are adjudicated by the IRS as the 26 U.S.C. 5000C tax is a tax matter, not a contract issue. The IRS Form W-14 is provided to the acquiring agency rather than to the IRS.

(d) For purposes of withholding under 26 U.S.C. 5000C, the Offeror represents that—

(1) It [__]is [__]is not a foreign person; and

(2) If the Offeror indicates "is" in paragraph (d)(1) of this provision, then the Offeror represents that—I am claiming on the IRS Form W-14 [____] a full exemption, or [____] partial or no exemption [*Offeror shall select one*] from the excise tax.

(e) If the Offeror represents it is a foreign person in paragraph (d)(1) of this provision, then—

(1) The clause at FAR 52.229-12, Tax on Certain Foreign Procurements, will be included in any resulting contract; and

(2) The Offeror shall submit with its offer the IRS Form W-14. If the IRS Form W-14 is not submitted with the offer, exemptions will not be applied to any resulting contract and the Government will withhold a full 2 percent of each payment.

(f) If the Offeror selects "is" in paragraph (d)(1) and "partial or no exemption" in paragraph (d)(2) of this provision, the Offeror will be subject to withholding in accordance with the clause at FAR 52.229-12, Tax on Certain Foreign Procurements, in any resulting contract.

(g) A taxpayer may, for a fee, seek advice from the Internal Revenue Service (IRS) as to the proper tax treatment of a transaction. This is called a private letter ruling. Also, the IRS may publish a revenue ruling, which is an official interpretation by the IRS of the Internal Revenue Code, related statutes, tax treaties, and regulations. A revenue ruling is the conclusion of the IRS on how the law is applied to a specific set of facts. **For questions relating to the interpretation of the IRS regulations go to** https://www.irs.gov/help/tax-law-questions **.**

(End of provision)

THE FOLLOWING DOSAR PROVISION IS PROVIDED IN FULL TEXT:

652.225-70 ARAB LEAGUE BOYCOTT OF ISRAEL (AUG 1999)

(a) Definitions. As used in this provision:
Foreign person means any person other than a United States person as defined below.

United States person means any United States resident or national (other than an individual resident outside the United States and employed by other than a United States person), any domestic concern (including any permanent domestic establishment of any foreign concern), and any foreign subsidiary or affiliate (including any permanent foreign establishment) of any domestic concern which is controlled in fact by such domestic concern, as provided under the Export Administration Act of 1979, as amended.

(b) Certification. By submitting this offer, the offeror certifies that it is not:

(1) Taking or knowingly agreeing to take any action, with respect to the boycott of Israel by Arab League countries, which Section 8(a) of the Export Administration Act of 1979, as amended (50 U.S.C. 2407(a)) prohibits a United States person from taking; or,

(2) Discriminating in the award of subcontracts on the basis of religion.

(End of Provision)

ADDENDUM TO SOLICITATION PROVISIONS
FAR AND DOSAR PROVISIONS NOT PRESCRIBED IN PART 12

THE FOLLOWING FEDERAL ACQUISITION REGULATION SOLICITATION PROVISIONS ARE INCORPORATED BY REFERENCE:

52.225-25 PROHIBITION ON CONTRACTING WITH ENTITIES ENGAGING IN CERTAIN ACTIVITIES OR TRANSACTIONS RELATING TO IRAN—REPRESENTATION AND CERTIFICATIONS (JUN 2020)