REQUEST FOR QUOTATION
(THIS IS NOT AN ORDER)

THIS RFQ [X] IS [ ] IS NOT A SMALL BUSINESS SET-ASIDE

1. REQUEST NUMBER	2. DATE ISSUED	3. REQUISITION/PURCHASE REQUEST NUMBER	4. CERT. FOR NAT. DEF. UNDER BDSA REG. 2 AND/OR DMS REG. 1	RATING
140F1S26Q0085	07/29/2026	0044053319		

5a. ISSUED BY
FWS IT Services
FWS, IT Services
5275 Leesburg Pike
Falls Church VA 22041

6. DELIVER BY *(Date)*
180 Days After Receipt of Order

7. DELIVERY
[X] FOB DESTINATION [ ] OTHER *(See Schedule)*

5b. FOR INFORMATION CALL *(NO COLLECT CALLS)*

NAME	TELEPHONE NUMBER	
	AREA CODE	NUMBER
Melissa Niemi	612	713-5216

8. TO:

a. NAME

b. COMPANY

c. STREET ADDRESS

d. CITY

e. STATE

f. ZIP CODE

9. DESTINATION

a. NAME OF CONSIGNEE
FWS GREAT PLAINS NATURE CENTER

b. STREET ADDRESS
6232 EAST 29TH STREET NORTH

c. CITY
WICHITA

d. STATE
KS

e. ZIP CODE
67220-2200

10. PLEASE FURNISH QUOTATIONS TO THE ISSUING OFFICE IN BLOCK 5a ON OR BEFORE CLOSE OF BUSINESS *(Date)*
08/12/2026 1700 ED

IMPORTANT: This is a request for information and quotations furnished are not offers. If you are unable to quote, please so indicate on this form and return it to the address in Block 5a. This request does not commit the Government to pay any costs incurred in the preparation of the submission of this quotation or to contract for supplies or service. Supplies are of domestic origin unless otherwise indicated by quoter. Any representations and/or certifications attached to this Request for Quotation must be completed by the quoter.

11. SCHEDULE *(Include applicable Federal, State and local taxes)*

ITEM NUMBER (a)	SUPPLIES/SERVICES (b)	QUANTITY (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)
	The U.S. Fish and Wildlife Service (USFWS) Great Plains Nature Center, in Wichita, KS, has a need for the purchase of equipment and install of an Underwriters Laboratory (UL) listed Intrusion Detection System (IDS). The system hardware (panel) shall be of a model listed in the Statement of Work (SOW) (unless equivalent is approved) and shall have the capability of expansion with expansion modules, panel tamper notification, remote monitoring, and remote annunciation using standard internet protocol-based communications, under RFQ# 140F1S26Q0085. Continued...				

12. DISCOUNT FOR PROMPT PAYMENT	a. 10 CALENDAR DAYS (%)	b. 20 CALENDAR DAYS (%)	c. 30 CALENDAR DAYS (%)	d. CALENDAR DAYS NUMBER	PERCENTAGE

NOTE: Additional provisions and representations [ ] are [ ] are not attached.

13. NAME AND ADDRESS OF QUOTER

a. NAME OF QUOTER

b. STREET ADDRESS

c. COUNTY

d. CITY

e. STATE

f. ZIP CODE

14. SIGNATURE OF PERSON AUTHORIZED TO SIGN QUOTATION

15. DATE OF QUOTATION

16. SIGNER

a. NAME *(Type or print)*

b. TELEPHONE
AREA CODE
NUMBER

c. TITLE *(Type or print)*

NAME OF OFFEROR OR CONTRACTOR

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Please see the attached Instructions to Offerors and Statement of Work (SOW) for additional details.				
00010	Intrusion Detection System Delivery: 180 Days After Receipt of Order				

CLAUSES

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

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

For FAR Clauses: http://acquisition.gov/far/index.html

Clauses Incorporated by Reference

52.203-13 Contractor Code of Business Ethics and Conduct (Nov 2021)

52.203-17 Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights. (Nov 2023)

52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017)

52.204-13 System for Award Management - Maintenance (Mar 2026)

52.204-14 Service Contract Reporting Requirements (Mar 2026)

52.204-19 Incorporation by Reference of Representations and Certifications. (Dec 2014)

52.209-6 Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, Proposed for Debarment, or Voluntarily Excluded (May 2026)

52.209-10 Prohibition on Contracting with Inverted Domestic Corporations (May 2026)

52.212-4 Terms and Conditions-Commercial Products and Commercial Services. (Mar 2026)

52.222-3 Convict Labor (May 2026)

52.222-35 Equal Opportunity for Veterans (May 2026)

52.222-36 Equal Opportunity for Workers with Disabilities (May 2026)

52.222-37 Employment Reports on Veterans (May 2026)

52.222-50 Combating Trafficking in Persons (May 2026)

52.222-90 Addressing DEI Discrimination by Federal Contractors (May 2026)

52.222-62 Paid Sick Leave Under Executive Order 13706 (DEVIATION DATE)

52.226-8 Encouraging Contractor Policies to Ban Tec Messaging While Driving (May 2024)

52.227-14 Rights in Data-General (May 2014)

52.232-33 Payment by Electronic Funds Transfer-System for Award Management (Oct 2018)

52.233-3 Protest after Award (DEVIATION DATE)

52.233-4 Applicable Law for Breach of Contract Claim (DEVIATION DATE)

52.240-91 Security Prohibitions and Exclusions (DEVIATION DATE)

52.240-93 Basic Safeguarding of Covered Contractor Information Systems (DEVIATION DATE)

52.242-15 Stop-Work Order (Aug 1989)

Full Text Clauses

52.217-8 Option to Extend Services.

As prescribed in 17.208(f), insert a clause substantially the same as the following:

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. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. 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 *30 days.*

(End of clause)

DEPARTMENT OF THE INTERIOR ACQUISITION REGULATION (DIAR) CLAUSES INCORPORATED BY FULL TEXT

1452.201-70 Authorities and Delegations (Sep 2011)

(a) The Contracting Officer is the only individual authorized to enter into or terminate this contract, modify any term or condition of this contract, waive any requirement of this contract, or accept nonconforming work.

(b) The Contracting Officer will designate a Contracting Officer's Representative (COR) at time of award. The COR will be responsible for technical monitoring of the contractor's performance and deliveries. The COR will be appointed in writing, and a copy of the appointment will be furnished to the Contractor. Changes to this delegation will be made by written changes to the existing appointment or by issuance of a new appointment.

(c) The COR is not authorized to perform, formally or informally, any of the following actions:

(1) Promise, award, agree to award, or execute any contract, contract modification, or notice of intent that changes or may change this contract;

(2) Waive or agree to modification of the delivery schedule;

(3) Make any final decision on any contract matter subject to the Disputes Clause;

(4) Terminate, for any reason, the Contractor's right to proceed;

(5) Obligate in any way, the payment of money by the Government.

(d) The Contractor shall comply with the written or oral direction of the Contracting Officer or authorized representative(s) acting within the scope and authority of the appointment memorandum. The Contractor need not proceed with direction that it considers to have been issued without proper authority. The Contractor shall notify the Contracting Officer in writing, with as much detail as possible, when the COR has taken an action or has issued direction (written or oral) that the Contractor considers to exceed the COR's appointment, within 3 days of the occurrence. Unless otherwise provided in this contract, the Contractor assumes all costs, risks, liabilities, and consequences of performing any work it is directed to perform that falls within any of the categories defined in paragraph (c) prior to receipt of the Contracting Officer's response issued under paragraph (e) of this clause.

(e) The Contracting Officer shall respond in writing within 30 days to any notice made under paragraph (d) of this clause. A failure of the parties to agree upon the nature of a direction, or upon the contract action to be taken with respect thereto, shall be subject to the provisions of the Disputes clause of this contract.

(f) The Contractor shall provide copies of all correspondence to the Contracting Officer and the COR.

(g) Any action(s) taken by the Contractor, in response to any direction given by any person acting on behalf of the Government or any Government official other than the Contracting Officer or the COR acting within his or her appointment, shall be at the Contractor's risk.

(End of clause)

Electronic Invoicing and Payment Requirements - Invoice Processing Platform (IPP)

(February 2021)

Payment requests must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP).

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in the applicable Prompt Payment clause included in the contract, or the clause 52.212-4 Contract Terms and Conditions - Commercial Items included in commercial item contracts. The IPP website address is: https://www.ipp.gov.

Under this contract, the following documents are required to be submitted as an attachment to the IPP invoice [Contracting Officer to edit and include the documentation required under this contract]:

The Contractor must use the IPP website to register access and use IPP for submitting requests for payment. The Contractor Government Business Point of Contact (as listed in SAM) will receive enrollment instructions via email from the Federal Reserve Bank of St. Louis (FRBSTL) within 3 - 5 business days of the contract award date. Contractor assistance with enrollment can be obtained by contacting the IPP Production Helpdesk via email IPPCustomerSupport@fiscal.treasury.gov or phone (866) 973-3131.

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

(End of Local Clause)

INTERNET PROTOCOL version 6 (June 2012)

1.Any system hardware, software, firmware and/or networked component (voice, video or data) developed, procured, or acquired in support and/or performance of this contract shall be capable of transmitting, receiving, processing, forwarding and storing digital information across system boundariesutilizing system packets that are formatted in accordance with commercial standards of Internet Protocol(IP) version 6 (IPv6) as set forth in the USGv6 Profile (NIST Special Publication 500267) and corresponding declarations of conformance defined in the USGv6 Test Program. In addition, this systemshall maintain interoperability with IPv4 systems and provide at least the same level of performance andreliability capabilities of IPv4 products.
2. Specifically, any new IP product or system developed, acquired, or produced must:
 a. Interoperate with both IPv6 and IPv4 systems and products, and
 b. Have available contractor/vendor IPv6 technical support for development and implementation

andfielded product management.
3. As IPv6 evolves, the Contractor commits to upgrading or providing an appropriate migration path foreach item developed, delivered or utilized at no additional cost to 'the Government. The Contractor shallretrofit all nonIPv6 capable equipment, as defined above, that is fielded under this contract with IPv6 capable equipment, at no additional cost to the Government.
4. The contractor shall provide technical support for both IPv4 and IPv6.
5. Any system or software must be able to operate on networks supporting IPv4, IPv6 or one that supportsboth.
6. Any product whose noncompliance is discovered and made known to the Contractor within one year after acceptance shall be upgraded, modified, or replaced to bring it into compliance at no additional cost tothe Government.

(End of clause)

52.252-1 Solicitation Provisions Incorporated by Reference (Feb 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this address: www.acquisition.gov.

Solicitation Provisions Incorporated by Reference

52.204-7 System for Award Management – Registration (Mar 2026)

52.209-2 Prohibition on Contracting with Inverted Domestic Corporations-Representation (May 2029)

52.240-90 Security Prohibitions and Exclusions Representations and Certification (Mar 2026)

Full Text Provisions

1452.233-2 -- Service of Protest Department of the Interior (Jul 1996) (Deviation)
(a) Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from U.S. Fish & Wildlife, 4301 Fairfax Drive, Arlington, VA 22203.

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.
(c) A copy of the protest served on the Contracting Officer shall be simultaneously furnished by the protester to the Department of the Interior Assistant Solicitor, Acquisitions and Intellectual Property, 1849 C Street, NW, Room 6511, Washington, DC 20240.

(End of Provision)

The U.S. Fish and Wildlife Service (USFWS) Great Plains Nature Center, in Wichita, KS, has a need for the purchase of equipment and install of an Underwriters Laboratory (UL) listed Intrusion Detection System (IDS). The system hardware (panel) shall be of a model listed in the Statement of Work (SOW) (unless equivalent is approved) and shall have the capability of expansion with expansion modules, panel tamper notification, remote monitoring, and remote annunciation using standard internet protocol-based communications, under RFQ# 140F1S26Q0085.

Please see the attached Statement of Work (SOW) for additional details.

I. Type of Contract

The Government contemplates award of a firm-fixed price contract resulting from this solicitation.

II. Proposal Instructions

1. **Submission of questions**
    a. Interested vendors must submit any questions concerning the solicitation by Wednesday, August 5, 2026, at 12:00 PM EST. Questions may be submitted via email to melissa_niemi@ios.doi.gov.
2. **Submission of quotes**
    a. Quotes are to be submitted via email to Melissa Niemi at melissa_niemi@ios.doi.gov by Wednesday, August 12, 2026, at 5:00 PM EST.
3. **Period for acceptance of quote**
    a. The vendor agrees quotes will be valid for at least 60 days from the date specified for receipt of quotations.
4. **Late submissions, modifications, revisions, and withdrawals of quotes**
    a. Vendors are responsible for submitting quotes, and any modifications, revisions, or withdrawals, so as to reach the Government office designated in the solicitation by the time specified in the solicitation. Any quote, modification, revision, or withdrawal of a quote received at the Government office designated in the solicitation after the exact time specified for receipt of quotes is "late" and will not be considered unless it is received before award is made, the Contracting Officer determines that accepting the late quote would not unduly delay the acquisition. However, a late modification of an otherwise successful quote, that makes its terms more favorable to the Government, will be considered at any time it is received and may be accepted.
5. **Technical proposals**
    a. Technical quotes shall be in two (2) separate volumes and shall be no more than (15) fifteen pages not including cover page, appendix, or separate pricing volume.
        i. Volume I - Technical (factor 1 & 2)
        ii. Volume II - Price (factor 3)
    b. Volume I – Factor 1- Technical
        i. This volume should address all non-price factors. Volume I shall include the cover page, descriptive literature that explains the vendors proposed product/service with enough detail to ascertain whether the quoted product/service will meet the criteria specified in the SOW.
    c. Volume I – Factor 2 Past Performance
        i. The Vendor should be able to demonstrate successful past performance and experience in the installation and configuration management of an intrusion detection system to the USFWS or other government agencies.

ii. The vendor shall demonstrate their prior experience as it relates to similar use cases of similar size, scope, and complexity to this requirement within the past three (3) years. Minimum of three (3) examples.

iii. The examples must include the following information:

1. Project Description
2. Dollar amount of project
3. Period of performance
4. Point of contact, telephone number, and email address.

d. Volume II – Price

i. Price volume shall include the cost of requested services listed in the SOW. Pricing shall include the equipment and installation for the intrusion detection system.

ii. Vendors are encouraged to offer discounted prices. The Government intends to evaluate quotes and award a contract without discussions with vendors. Therefore, the vendor's initial quote should contain its 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 or in the Government's best interest.

III. Evaluation Factors

The technical features of each quote shall be evaluated against the Request for Quote (RFQ) requirements, assessing the strengths and weaknesses of each quote in light of evaluation criteria described below. The Contracting Officer will screen quotes to identify and eliminate any quotes that are so incomplete as to preclude consideration of award. The remaining quotes will be evaluated based upon the following factors:

1. **FACTOR 1 – Technical approach and demonstrate your understanding of the SOW**
   a. The vendor's demonstration of its technical approach and understanding of the requirements as set forth herein, including how it described meeting the specific details in the SOW.
2. **Factor 2 – Past Performance**
   a. The vendor shall clearly demonstrate satisfactory or better performance with projects of similar size, scope, and complexity of this requirement.
3. **FACTOR 2 – Price**
   a. Pricing shall be evaluated to determine completeness and reasonableness per the criteria specified in the SOW. The Government will evaluate the quoted price for reasonableness.

IV. Basis of Award

Award shall be made to the responsible vendor whose quote is determined to be the most advantageous to the Government, with appropriate consideration given to the evaluation factors. Award shall be made to the vendor whose quote, conforming to this RFQ, provides the best value to the Government. Non-pricing features of a vendor's quote shall be evaluated in such a manner as to assess the value of those features as compared to the quoted prices or costs to the Government. Implicit in this process is the Government's willingness to accept other than the lowest priced quote or highest rated quote. Overall, the non-price factors are more important than the price factor. The Government may reject any or all quotes if such action is in the public interest; accept other than the lowest quote; and waive informalities and minor irregularities in quotes received.

INTRUSION DETECTION SYSTEM (IDS)

This Intrusion Detection System (IDS) is specified for the U.S. Fish & Wildlife Service (FWS) Great Plains Nature Center, located at 6232 East 29th Street North Wichita, Kansas. The site has an existing IDS panel and equipment that needs replaced. The contractor shall remove and dispose of all existing IDS equipment.

The contractor shall install, and make fully functional, an Underwriters Laboratory (UL) listed Intrusion Detection System (IDS). The system hardware (panel) shall be of a model listed below (unless equivalent is approved) and shall have the capability of expansion with expansion modules, panel tamper notification, remote monitoring, and remote annunciation using standard internet protocol-based communications. Contract bidders shall provide an authorized dealer letter from the manufacturer prior to contract award.

MONITORING SOLUTIONS:

The Government will provide additional connection/monitoring information to the vendor once the vendor has offered an approved panel.

- The Government may choose to contract with the U.S. Department of Homeland Security (DHS) - Federal Protective Service (FPS) for monitoring services. All systems monitored by DHS will require the completion of the DHS MegaCenter Alarm Requirements 2023 (MAR) package (Instructions are associated with the MAR package). If connected to DHS, the system will require a static Internet Protocol (IP) address that the government will furnish.
- If the vendor is to provide monitoring services, the station will provide FWS-OEMPS an alarm zone data sheet obtained from the commercial monitoring company prior to acceptance of the system. Commercial monitoring may not be connected via ethernet to the FWS network and will therefore require a separate internet connection or a POTS line.

The Government may request the system be programmed to auto-arm daily (TBD).

The IDS control panel and associated power distribution hardware will be located within the Janitor's Closet (Nature Center) in a locked enclosure that shall be mounted to a ¾" plywood backer board affixed to the room wall**.** This location must be properly ventilated to ensure appropriate cooling of electronics. Vendor should have prior experience and knowledge of connecting IDS systems to FPS MegaCenter via internet.

Offeror must provide a letter from the system manufacturer showing they are an authorized dealer and certified installer for the proposed system.

A battery backup shall be incorporated into the IDS panel using a 7 AMP hour battery that will allow for a minimum of 4 hours of backup power, from initial commercial power failure.

System Panels Authorized

A. Bosch model numbers 9512G series
B. DMP model XR150
Note: Proprietary panels will not be accepted due to the inability to provide adequate support.

The doors/areas as listed in table below**,** shall be alarmed using appropriate methods for the

types of doors and areas. All doors are to be fitted with either recessed or frame mounted magnetic contacts. Ceiling or wall mounted passive infrared (PIR) motion detectors should be positioned to ensure no gaps in coverage in areas to monitored.

Each sensor (door, PIR, glass break, etc.) must be configured as a separate zone. The IDS panel box must have a panel tamper switch.

Areas – site may elect to have multiple areas configured within the system, allowing individual areas (or all areas at once) to be armed or disarmed by authorized users.

Wireless panic buttons shall be installed at locations identified below. Buttons shall be positioned discretely to allow for emergency access, but also in a location that would prevent accidental activation.

Contractor shall position and install wireless repeaters as necessary to ensure wireless device communication throughout the areas.

All components provided under this contract must be new. Used, repurposed, or refurbished equipment is not authorized for use and will not be accepted.

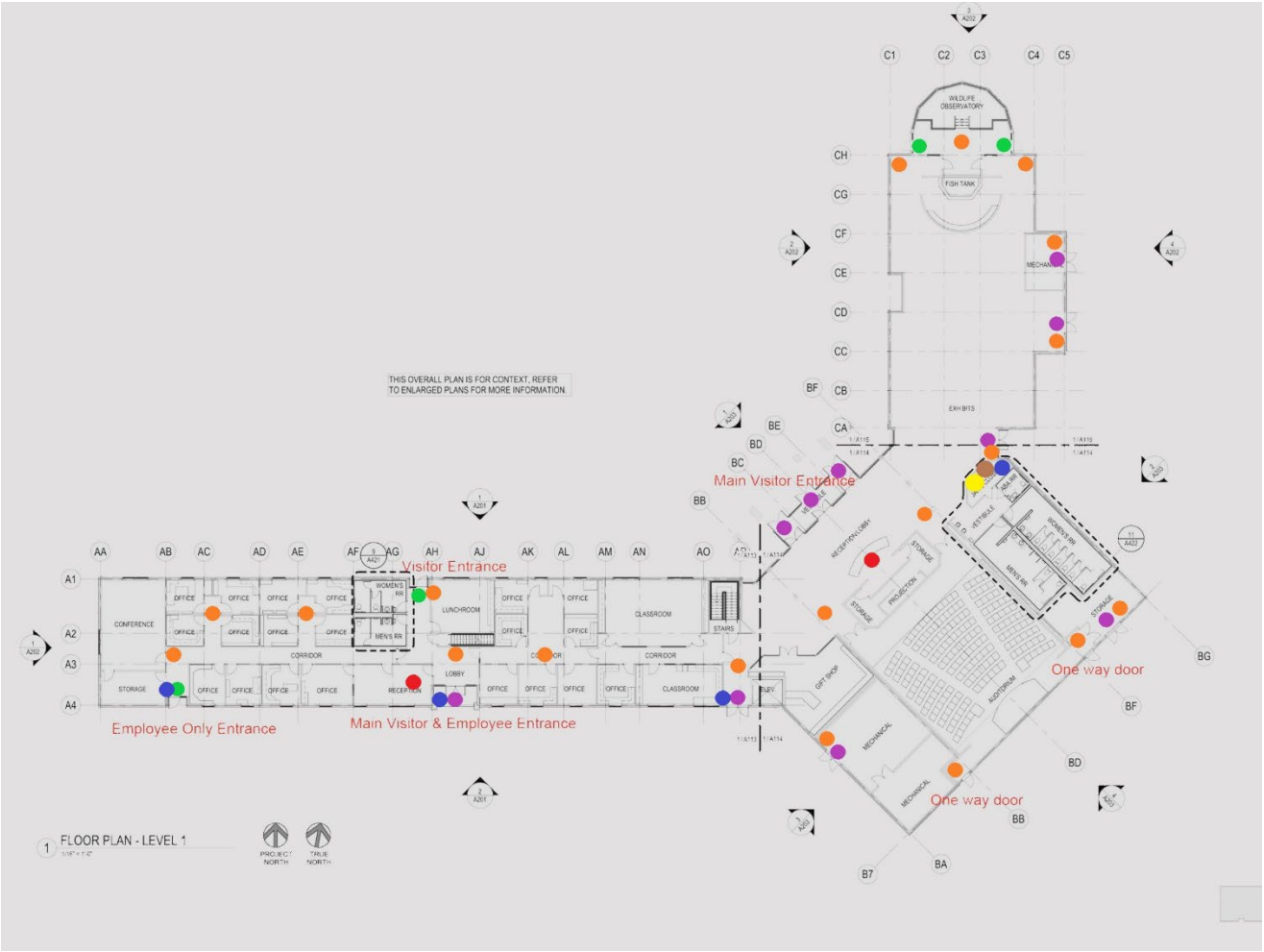
Offeror must provide cut sheets (specifications) for proposed system components.

The contractor must provide a minimum of 2 hours of end-user training to facility staff prior to facility acceptance.

Warranty: Manufacturer's standard form in which manufacturer and Installer agree to repair or replace components of intrusion detection devices and equipment that fail in materials or workmanship within one year from date of Substantial Completion.

See Equipment Tables and Drawings below:

Great Plains Nature Center – Wichita, KS



FWS Great Plains Nature Center Intrusion Detection Layout

1 – Panel (Yellow)
1 – Receiver (Brown)
4– Keypad (Blue)
4 – Door Contact (Green)
10 – Double Door Contact (Purple)
19 – Motion Sensor (Orange)
2 – Panic Button (Red)

NATURE CENTER

DEVICE LOCATION	DEVICE TYPE
Janitor's Closet	PANEL - in enclosure that shall be mounted to a ¾" plywood backer board affixed to the room wall, and connected to the internet for transmission to the Central Monitoring Station.
Panel – Janitor's Closet	WIRELESS RECEIVER
Panel – Janitor's Closet; SW entrance, south	(4) KEYPAD - Touch Screen Keypad

DEVICE LOCATION	DEVICE TYPE
entrances (x2)	
SW entrance; NW entrance; NE entrances (x2)	(4) DOOR MAGNETIC CONTACTS
South entrances (x3); west entrances (x3); SE entrance; east entrances (x3)	(10) DOUBLE DOOR MAGNETIC CONTACTS
SW office areas (x7); SE office areas (x7); NE office areas (x5)	(19) WIRELESS MOTION SENSORS
South reception desk; SE reception desk	(2) WIRELESS PANIC BUTTONS

Information Technology Baseline Compliance Contract Guidelines

July 2022

Table of Contents

Introduction 3

Section 1.0 – Information Technology and Cybersecurity Requirements 3

A. Applicability 3
B. Requirements 3
C. Information Systems 3
D. Cloud 4
E. Internet Protocol Version 6 (IPv6) 4
F. Continuous Monitoring 5
G. Security Training and Reviews 5
H. Contractor Reporting Requirements 6

Section 2.0 – Cybersecurity Incident Response 6

A. Applicability 6
B. Definitions 6
C. Requirements 7

Section 3.0 – Privacy Requirements 8

A. Applicability. 8
B. Definitions 8
C. Privacy Act Requirements 8
D. Privacy Controls 8
E. Privacy Breach Reporting Requirements 9
F. Privacy Training Requirements 10

Section 4.0 – Accessibility Requirements (Section 508) 11

A. Applicability 11
B. Requirements 11

Section 5.0 – Records Management Requirements 13

A. Applicability 13
B. Definitions 13
C. Requirements 13

Section 6.0 – Contractor Personnel Security Requirements 15

Section 7.0 – Controlled Unclassified Information Requirements 16

A. Applicability 16
B. Definitions 16
C. Authorities 16
D. Requirements 16
E. Training 17

Section 8.0 – Paperwork Reduction Act of 1995 17

Section 9.0 – Reference Documents 17

Section 10.0 – Glossary 17

Introduction

This document provides guidance regarding requirements that must be reviewed and considered for incorporation, where applicable, in all Department of the Interior (DOI, Department) contract actions that involve information technology (IT) products or services. Contracting Officer Representatives (CORs) and/or the requirement owners should work closely with their Bureau or Office Associate Chief Information Officer and Contracting Officer (CO) to ensure the below requirements are properly addressed in IT contracts within the appropriate sections. Any referenced regulation or policy should be provided to the Contractor via hypertext link or other means.

Section 1.0 – Information Technology and Cybersecurity Requirements

A. Applicability

This term applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall use these terms in all subcontracts.

B. Requirements

Information systems and system services provided to the Department by the Contractor must comply with DOI IT Cybersecurity and Privacy Control Standards, privacy policies, and other related guidance. Contracts that involve Industrial Control System (ICS) products and services should be evaluated on an individual basis and contain language specific to ICS. Please contact the Bureau of Reclamation (BOR) at ICSsecurity@usbr.gov for ICS issues and guidance.

The Contractor and the contractor-managed systems shall comply with all federal regulations and guidance, including but not limited to:

1. Federal Information Security Modernization Act of 2014 (FISMA) accessible at https://www.cisa.gov/federal-information-security-modernization-act
2. Federal Risk and Authorization Management Program (FedRAMP) for cloud hosted systems accessible at https://www.fedramp.gov
3. Section 208 of the E-Government Act of 2002 accessible at https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf
4. Privacy Act of 1974 accessible at https://www.justice.gov/opcl/privacy-act-1974
5. Federal Information Processing Standards (FIPS) and the National Institute of Standards and Technology (NIST) 800-Series Special Publications (SP) accessible at https://www.nist.gov
6. Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, accessible at https://www.cio.gov/policies-and-priorities/circular-a-130/

C. Information Systems

The Contractor shall manage information in accordance with applicable laws, regulations, executive orders, and policies regarding the marking, safeguarding, and dissemination of

Controlled Unclassified Information (CUI). Personally Identifiable Information (PII) is a subset of information designated as CUI, and Sensitive PII is a subset of PII that requires additional controls and safeguards. (See section 3, Privacy Requirements)

The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

Contractor Information Systems shall comply with FISMA. The Contractor shall provide an Assessment and Authorization (A&A) documentation package for each system that complies with Federal Information Processing Standard (FIPS) 199, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, NIST SP 800-37, NIST SP 800-53, NIST SP 800-60, et al.

The Contractor cryptographic modules used to protect DOI information shall comply with the current NIST FIPS 140 version and be validated by the Cryptographic Module Validation Program.

Access to all government data stored outside the confines of a DOI-managed data center shall comply with Trusted Internet Connections (TIC) requirements.

All Contractor personnel requiring access to DOI information data and/or systems shall be cleared at appropriate levels as set forth:

1. Low Risk position will require a National Agency Check with Written Inquiries (NACI) or equivalent investigation.
2. Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI).
3. High Risk position will require a Background Investigation (BI).

Vulnerability Scanning - All IT systems providing services to or on behalf of the Department or storing, processing, or routing DOI CUI information must be scanned monthly with a vulnerability analysis tool using authenticated scans that are acceptable to DOI. Vulnerabilities and weaknesses shall be remediated in accordance with (IAW) Department-mandated time frames commensurate with the level of risk.

D. Cloud

All Contractor cloud-hosted Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) or other “as a Service” offerings shall comply with applicable language within the DOI cloud hosting program guidelines.

E. Internet Protocol Version 6 (IPv6)

The applicability of IPv6 to DOI-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the Department Acquisition, Arts, and Asset Policy DOI-AAAP-0055, *Procuring Internet Protocol Version 6 (IPv6),* (per OMB Memorandum M-05-22, August 2, 2005) and with subsequent federal requirements (OMB Memorandum M 21-07 *Transition to IPv6*, September 28, 2010) regardless of whether the

acquisition is for modification, upgrade, or replacement. All Enterprise Architecture related component acquisitions shall be IPv6-compliant as defined in the U.S. Government Version 6 (USGv6) Profile (NIST SP 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program. In cloud service procurements, IPv6 compliance should be pursued where practicable.

F. Continuous Monitoring

All Contractor-operated systems that input, store, process, output, and/or transmit DOI CUI shall meet or exceed the continuous monitoring requirements identified in the DOI Continuous Monitoring Plan or the Bureau or Office Continuous Monitoring Plan, whichever best fits mission, security, and risk management needs.

Contractor-managed systems are required to have an assigned Information System Security Officer (ISSO) and System Owner (SO) to support the processes described in the contract. While the procuring organization designates government personnel to serve in these roles, the contractor must provide functionally equivalent personnel to enable effective day-to-day operation, management, and monitoring of the system. The Contractor ISSO and SO resources are required to comply with DOI- or other-approved annual and Role Based Security Training (RBST) requirements.

Contractors managing systems on behalf of the Department are required to submit Continuous Monitoring Reports per the Continuous Monitoring Plan to the federal point of contact designated in the contract per the timelines prescribed in the Continuous Monitoring Plan. The Contractor-managed systems may be required to submit to a penetration test (at the discretion of the awarding program) in coordination with DOI cybersecurity personnel or approved contract officials.

When required by the contract, the Contractor must provide the following in alignment with DOI's continuous monitoring strategy:

1. account management
2. vulnerability management
3. patch management
4. antivirus
5. malware detection
6. event management
7. configuration management
8. license management
9. incident management

G. Security Training and Reviews

All users of federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing federal information systems under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and

be completed on an annual basis thereafter. New Contractor employees assigned to the contract shall complete the training before accessing federal information systems under the contract. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification each year. The e-mail notification shall state that all Contractor and subcontractor employees have completed the required training.

The government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced, particularly when contractors build and operate or maintain systems on behalf of the Department. In such cases, the Contractor shall afford DOI, the Office of the Inspector General, and other government organizations access to the Contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. The Contractor shall provide access, to the extent necessary as determined by the government, for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of government data or the function of computer systems used in performance of the contract and to preserve evidence of computer crime. Cloud Service Providers should not be expected to grant physical access to government inspectors.

H. Contractor Reporting Requirements

The Contractors operating information systems on behalf of the Department shall comply with FISMA reporting requirements. Department system owners shall coordinate annual and quarterly data collection. Contractors must provide DOI with the requested information based on the timeframes provided with each request. The Contractor systems shall comply with near real time feeds in accordance with Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) requirements as coordinated by DOI. Reporting requirements are determined by OMB and may change each reporting period.

The Contractor-managed systems shall adhere to NIST 800-53 and submit to an annual assessment performed in coordination with DOI cybersecurity personnel or approved contract officials. All results of the annual assessment become the property of the Department.

The Contractor shall comply with DHS or other government oversight bodies regarding cybersecurity-related mandates and directives (Binding Operational Directives [BOD], etc.) or any additional ad-hoc reporting requirements.

Section 2.0 – Cybersecurity Incident Response

A. Applicability

This term applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall use these terms in all subcontracts.

B. Definitions.

As used in this term-

"Incident" means an occurrence that

1. actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
2. constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

C. Requirements

All Contractor employees and information system service providers shall be responsible for recognizing and reporting security incidents. Information system service providers shall receive the current version of the DOI Incident Response Plan, Policy, and Handbook at the time of award, in addition to bureau- or office-specific guidance for appropriate reporting and response at all levels. All suspected or confirmed information security incidents shall be reported in accordance with the requirements listed below, even if it is believed the incident may be limited, small, or insignificant. For hosting environments, including cloud systems and services, this includes incidents occurring on the service provider's underlying infrastructure supporting containers utilized by the Department. In such cases, the vendor's primary security operations and/or incident response unity shall engage directly with the DOI Cyber Security Operations (CSO) Section and provide DOI CSO with security and event logs covering the period of the incident and up to six months prior. The DOI CSO and Bureau or Office Incident Response Teams will determine when an incident requires additional focus and attention.

All Contractor employees and information system service providers shall report all information security incidents to the appropriate Bureau or Office Incident Response Team and to the DOI Computer Incident Response Center (DOI CIRC) immediately, no later than 1 hour after "becoming aware of the incident," at DOICIRC@ios.doi.gov, (703) 648-5655, regardless of day or time. Any contractor action to investigate, identify, respond to, contain, remediate, or recover from a security event (which includes "suspected" incidents) constitutes "becoming aware of the incident."

When notifying the DOI CIRC and the appropriate Bureau or Office Incident Response Team, the Contractor shall include the CO and COR on the correspondence email to DOICIRC@ios.doi.gov and the appropriate Bureau or Office Incident Response Team. If the Contractor reported the incident by phone, then immediately following the reporting, the Contractor shall notify the CO and COR via e-mail. The Contractor is responsible for verifying that all notification was received and acknowledged by the CO or COR. If the Contractor has any questions regarding these procedures, they shall contact the CO or the COR.

The Contractor shall not include any controlled information in the subject or body of any e-mail. Contractor shall transmit controlled information using validated encryption methods compliant with the current NIST FIPS 140 version to protect controlled information in e-mail attachments. Passwords must not be communicated in the same email as the attachment. Contractor shall contact the CO or COR if encryption software is needed for guidance on appropriate, federally approved encryption methods.

Section 3.0 – Privacy Requirements

A. Applicability.

This term applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall use these terms in all subcontracts.

B. Definitions.

As used in this term-

Breach: the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other-than-authorized purpose.

1. PII - information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

2. Sensitive PII (SPII) is a subset of PII that, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. SPII is CUI and requires additional controls and safeguards to protect the privacy of individuals. Sensitivity of PII may depend on specific PII elements, groupings of PII, context or use of PII, or requirements under applicable federal laws, regulations, and policy such as the Privacy Act of 1974 and the CUI Rule. SPII includes but is not limited to full or truncated Social Security Number (SSN), driver's license or state identification number; financial account number; date of birth; citizenship; ethnic or religious affiliation; biometric identifiers such as fingerprint, voiceprint, or iris scan; medical information; criminal history; and system authentication information such as passwords, personal identification numbers or mother's maiden name.

C. Privacy Act Requirements

The Contractor shall comply with the requirements of the Privacy Act of 1974 and shall not remove PII or Privacy Act material from government facilities or systems, or facilities or systems operated or maintained on the government's behalf, without the express written permission of the Head of the Contracting Activity. When Privacy Act records, information, data, documentary material, and equipment is no longer required, the Contractor shall return it to the Department's control or hold it until otherwise directed. Items returned to the government shall be hand carried, mailed, emailed, or securely electronically transmitted to the CO.

D. Privacy Controls

The Contractor shall meet the privacy requirements of the E-Government Act, FISMA, applicable federal privacy laws, NIST, OMB, and DOI (including but not limited to those listed in the contract table of authorities) for the collection, handling, processing, and sharing of PII, and ensure compliance with the privacy controls requirements of NIST SP 800- 53, FIPS 199,

FIPS 200, and DOI Privacy Control standards as appropriate for the sensitivity of the system. The Contractor shall monitor the information system and update controls for continued privacy compliance on an ongoing basis and shall provide status reports to the Department upon request.

The Contractor shall be required to provide all necessary support to assist the Department in meeting the requirements of the Privacy Act and related laws and shall provide supporting documentation and access to information upon request by authorized agency officials. Support in this context includes timely responding to requests for information from the Department about the access, creation, collection, use, storage, maintenance, transmission, sharing, or disposition of PII on the Contractor's system or processes, and providing timely review of relevant compliance documents for factual accuracy.

E. Privacy Breach Reporting Requirements

The Contractor shall provide notice to DOI CIRC or the appropriate Bureau or Office Incident Response Team of any known or suspected breach of PII and meet breach reporting and mitigation requirements in accordance with the DOI Privacy Breach Response Plan or bureau or office applicable response plan. The report of a breach of PII shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information or has otherwise failed to meet the requirements of the contract.

The Contractor shall report all known or suspected breaches in electronic or physical form to the CO, COR, and the DOI CIRC or bureau or office point of contact no later than one hour following discovery via email at DOICIRC@ios.doi.gov or (703) 648-5655, regardless of day or time and as specified within the DOI Privacy Breach Response Plan and the applicable bureau or office response plan.

The Contractor shall not include any controlled information in the subject or body of any e-mail and shall not include any SPII. Where necessary, SPII shall be transmitted using encryption methods to protect CUI in attachments in accordance with cryptographic requirements prescribed by the current NIST FIPS 140 version. Passwords shall be securely communicated separately.

The Contractor shall not contact individuals impacted by a breach involving PII until directed by the government. Department officials will make all determinations related to response activities, appropriate notifications to individuals and federal agencies and other organizations, and any remedial actions.

The Contractor shall take immediate action to contain and mitigate the impact of the breach and cooperate with DOI officials to investigate the breach and determine remedial measures as follows:

- The Contractor shall provide full access and cooperation for all activities—determined by the Department to be required—to ensure an effective breach response, including providing all requested images, log files, and event information to facilitate rapid resolution of breaches.
- Breach response activities—determined to be required by the Department—may include but are not limited to inspections, investigations, forensic reviews, data analyses and

processing, and final determinations of responsibility for the breach and/or liability for any additional response activities.

- The Department, at its sole discretion, may obtain the assistance of federal agencies and/or third-party firms to aid in breach response activities, as needed.

The Contractor shall provide a detailed written analysis with the following data elements available at the time of the breach, and a follow up report with any additional information or updates within 24 hours of the initial breach report, that shall address all relevant information concerning the compromise:

- Government programs, platforms, or systems involved
- Location(s) of the breach
- Date and time the breach was discovered
- Nature of the event (loss, theft, or unauthorized access)
- Description or summary of events
- Description of PII involved, such as name, Social Security number, date of birth, etc.
- Number of potentially impacted individuals
- Estimated number of records exposed or compromised

The Contractor shall collaborate with DOI officials on breach remedial activities to include notifications, credit monitoring, establishing a call center, or other relief to affected individuals as appropriate under the circumstances of the breach as prescribed in the contract. The Contractor shall have the capability to notify individuals whose PII resided in the Contractor system at the time of the breach not later than five business days after being directed by DOI officials to notify affected individuals. The Contractor shall not proceed with notifications unless the CO has directed in writing that notification is appropriate, subject to prior approval by DOI Privacy Officials, in accordance with the DOI Privacy Breach Response Plan. Notification may require the Contractor's use of address verification and/or address location services. All determinations, including response activities, notifications to affected individuals and/or federal agencies, and related services will be made by authorized DOI officials at DOI's discretion.

If an SPII or PII breach occurs because of the violation of a term of the contract by the Contractor or its employees, or the Contractor's covered persons, the Contractor shall, as directed by the CO and at no cost to the government, without delay correct or mitigate the violation. If the Department incurs a cost for individual notifications and remediation services procured as the result of a breach of SPII or PII, the COR will contact the CO to coordinate appropriate remedies per contract terms and conditions.

F. Privacy Training Requirements

All Contractor and subcontractor employees are required to take privacy awareness training prior to accessing DOI information or information systems. All Contractor and subcontractor employees must also complete role-based privacy training prior to accessing PII or Privacy Act data. All required privacy training shall be completed within 30 days of contract award and prior

to granting access to DOI information systems or any PII, and must be completed on an annual basis thereafter, not later than September 30th of each year. Any new Contractor employees assigned to the contract shall also meet these privacy training requirements. Privacy training shall meet the requirements of FAR 52.224-3 Privacy Training (January 2017).

The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than 30 days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 30th of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

Section 4.0 – Accessibility Requirements (Section 508)

Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C § 794 (d)) requires that when federal agencies develop, procure, maintain, or use information and communication technology (ICT), it must be accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to and use of information and data that is comparable to people without disabilities.

When ICT conforming to one or more requirements in the Revised 508 Standards is not commercially available, the agency shall procure the ICT that best meets the agency's business needs and the Revised 508 Standards, in accordance with 36 CFR 1194 E202.7 and FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DOI Section 508 Office according to 375 DM 8.

A. Applicability

This term applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall use these terms in all subcontracts.

B. Requirements

1. Products, platforms, and services delivered as part of a statement of work that are ICT, or contain ICT, shall conform to the Revised 508 Standards, which are located at 36 CFR § 1194.1 and Appendices A, C and D and available at https://www.access-board.gov/ict/. In the revised regulation, ICT replaced the term Electronic and Information Technology (EIT) used in the original 508 standards.

    a. Applicable Functional Performance Criteria: All functional performance criteria in chapter 3 of the Revised 508 Standards apply when using an alternative design or technology that results in substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in chapters 4 and 5 of the Revised 508 Standards, or when chapters 4 or 5 do not address one or more functions of ICT.

    b. Applicable 508 requirements for electronic content features and components (including electronic training materials): All requirements in E205 of the revised

508 Standards apply, including all Web Content Accessibility Guidelines (WCAG) 2.0 Level AA Success Criteria.

c. Applicable 508 requirements for software features and components (including Software infrastructure): All requirements in chapter 5 apply, including all WCAG 2.0 Level AA Success Criteria, 502 Interoperability with Assistive Technology, and 503 Application.

d. Applicable 508 requirements for hardware features and components: All requirements in chapter 4 apply.

e. Applicable 508 requirements for support services and documentation: All requirements in chapter 6 apply.

2. When providing installation, configuration or integration services for ICT, the Contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.

3. When providing maintenance upgrades, substitutions, and replacements to ICT, the Contractor shall not reduce the original ICT's level of Section 508 conformance prior to upgrade, substitution, or replacement. The agency reserves the right to request an Accessibility Conformance Report (ACR) for proposed substitutions and replacements prior to acceptance.

4. Contractors shall provide an ACR for each commercially available ICT item offered through this contract. The ACR should be created using the Voluntary Product Accessibility Template (VPAT) Version 2.4 Rev 508 (or later), located at https://www.itic.org/policy/accessibility/vpat.

5. When developing or modifying ICT for the government, the Contractor shall ensure the ICT fully conforms to the applicable Section 508 Standards. When modifying a commercially available or government-owned ICT, the Contractor shall not reduce the original ICT item's level of Section 508 conformance.

6. When developing or modifying web and software ICT, the Contractor shall demonstrate Section 508 conformance by providing Section 508 test results based on the versions of the DHS Trusted Tester Methodology currently approved for use, as defined at https://www.dhs.gov/compliance-test-processes. The Contractor shall use testers who are certified by DHS on how to use the DHS Trusted Tester Methodology (e.g., "DHS Certified Trusted Testers") to conduct accessibility testing. Information on how testers can become certified is located at https://www.dhs.gov/publication/trusted-tester-resources.

7. Contractor personnel shall possess the knowledge, skills, and abilities necessary to address the applicable revised Section 508 Standards for each ICT.

8. Exceptions for statements of work have been determined by DOI and only the exceptions described in 375 Departmental Manual (DM) 8 DOI Section 508 Program and Responsibilities, dated February 5, 2016, may be applied. Any request for additional exceptions shall be sent to the COR and a determination will be made according to 375 DM 8.

Section 5.0 – Records Management Requirements

When federal agencies acquire goods or services, they need to determine what federal records management requirements should be included in the contract. Federal contractors often create, send, or receive federal records. Federal contracts should provide clear legal obligations describing how the contract employees must handle federal records.

Agency records officers, procurement counsel, and acquisitions officers must discuss how to integrate records management obligations into their existing procurement processes. The National Archives and Records Administration (NARA) has developed language to be included as an agency-specific term and condition in federal contracts for a variety of services and products. Most contracts should include language on records management obligations, but each contract should be evaluated individually as not all conditions will be appropriate for all contracts. For example, the data-rights paragraph may not be appropriate for all contracts. Instead, agencies may be better served by one of the established data-rights clauses in the Federal Acquisition Regulations.

This language should not replace specific records management requirements included within federal information system contracts.

A. Applicability

This term applies to all Contractors whose employees create, work with, or otherwise handle federal records, as defined in section B, regardless of the medium in which the record exists. The Contractor shall use these terms in all subcontracts.

B. Definitions

Federal record – (as defined in 44 U.S.C. § 3301) includes all recorded information, regardless of form or characteristics, made or received by a federal agency under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

The term federal record:

- includes all departmental records
- does not include personal materials
- applies to records created, received, or maintained by Contractors pursuant to their Department contract
- may include deliverables and documentation associated with deliverables

C. Requirements

1. Contractors shall comply with all applicable records management laws and regulations, as well as NARA records policies, including but not limited to the Federal Records Act (44 U.S.C. chapters 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and Departmental policy.

2. The Contractor shall coordinate with the appropriate Departmental and Bureau Records Management Programs to ensure the identification, storage, retrieval, preservation, access, control markings, and disposition of records using the official Departmental record keeping system(s). This includes the implementation of all technical aspects to appropriately interconnect and or transfer records to the system(s). Any exceptions to using this system must be expressly presented by the Contractor in writing to and approved by the Departmental and/or Bureau Records Management Programs. Thereafter, each major or minor variance must be expressly presented in writing.
3. When the Department or a bureau contracts for the design, development, or operation of a system on behalf of the Department, the Contractor must make and preserve records to sufficiently document all planning, design, development, or operation of the system.
4. In accordance with 36 CFR 1222.32, all data created for government use and delivered to, or falling under the legal control of, the government are federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, the Privacy Act of 1974 (5 U.S.C. 552a), as amended, and Executive Order 13556 Controlled Unclassified Information. Contractors shall maintain all records created for government use or created while performing the contract and/or delivered to, or under the legal control of the government and must manage them in accordance with federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data and must be managed and scheduled for disposition only as permitted by statute or regulation.
5. The Department and its Contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of DOI or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity and the Bureau Records Officer. The routine disposition of records created and maintained by DOI and the Contractor may be suspended through coordination of the Departmental Records Officer, Bureau or Office Records Officer, Records Management Contact, Program Manager, or Site Manager. Willful and unlawful destruction, damage or alienation of federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, the Contractor must report to DOI. The agency must report promptly to NARA in accordance with 36 CFR 1230.
6. The Contractor shall immediately notify the appropriate CO upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records, or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the contract vehicle. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from government facilities or

systems, or facilities or systems operated or maintained on the government's behalf, without the express written permission of the Head of the Contracting Activity which the Contractor requests from the CO. When information, data, documentary material, records and/or equipment is no longer required, the Contractor shall return it to DOI control or must hold it until otherwise directed. Items returned to the government shall be hand carried, mailed, emailed, or securely electronically transmitted to the CO or address prescribed in the contract vehicle. The Contractor shall provide a mechanism for reliably deleting DOI data upon request by the Department.

7. The Contractor is required to obtain the CO's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by government and DOI guidance for protecting sensitive, proprietary information, classified, and CUI.
8. The Contractor shall only use government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with DOI policy.
9. The Contractor shall not create or maintain any records containing any non-public DOI information that are not specifically tied to or authorized by the contract.
10. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.
11. The Department owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which DOI shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.
12. Training. All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take DOI-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

Section 6.0 – Contractor Personnel Security Requirements

Acquired services shall comply with the following regulations and requirements. Homeland Security Presidential Directive-12 requires that all federal entities ensure that all Contractors gaining physical access to federally controlled facilities or logical access to federally controlled information systems have current and approved security background investigations that are equivalent to investigations performed on federal employees; see section 1.0, part C of this document. The Contractor shall comply with the contract terms and conditions. The Office of Personnel Management (OPM) will perform background investigations.

Section 7.0 – Controlled Unclassified Information Requirements

A. Applicability

This term applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall use these terms in all subcontracts.

B. Definitions

1. Sensitive Information - any information that warrants a degree of protection and administrative control as defined in law, regulation, governmentwide policy, or judicial opinion.
2. Controlled Unclassified Information (CUI) - information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law regulation or governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. Legacy materials may retain For Official Use Only (FOUO), Sensitive But Unclassified (SBU), or other markings until the artifact is no longer considered "data at rest;" it is revised, reused, or goes in motion.
3. Personally Identifiable Information (PII) - a subset of information designated as CUI. See section 3.0, Privacy Requirements, for additional requirements.
4. Sensitive PII - subset of PII that requires additional controls and safeguards. See section 3.0, Privacy Requirements, for additional requirements.

C. Authorities

1. EO 13556, Controlled Unclassified Information, November 4, 2010
2. 32 CFR 2002, Controlled Unclassified Information (Implementing Directive)
3. The Federal CUI Registry
4. Departmental standards

D. Requirements

1. The Contractor must manage CUI in accordance with applicable laws, regulations, executive orders, and policies.
2. The Contractor must identify, and safeguard controlled information from unauthorized release into public domain, or to unauthorized persons, organizations, or subcontractors.
3. The Contractor or subcontractor must not disclose or release the materials provided to the Contractor to any individuals of the Contractor's organization not directly engaged in providing services under the contract or that do not have a valid need-to-know. All technical data provided to the Contractor by the government must be protected from public or private disclosure in accordance with the markings printed on them.
4. The Contractor must not release to anyone outside the Contractor's organization any sensitive information unless the CO has given prior written approval. This includes, but is not limited to, news releases, marketing promotions, articles, interviews,

reports, social media posts, and any other media releases. Requests for approval must identify the specific information to be released, the medium to be used, the purpose for the release, and a description of the need-to-know. The Contractor must submit its request to the CO at minimum ten business days before the proposed date for release. Subcontractors must submit requests for authorization to release through the prime Contractor to the CO.

5. Contractor controlled computer systems housing CUI must follow the NIST SP 800-171 Rev. 2 (or current Rev); SP 800-171A; and SP 800-172 (or current Rev).
6. If the Contractor believes that CUI information has been compromised, they will follow the incident response procedures in the DOI Incident Response Policy and Plan.

E. Training

Individuals originating or working with sensitive information must complete CUI training to become an authorized holder. CUI must only be disseminated to authorized holders in the furtherance of a lawful government purpose.

Section 8.0 – Paperwork Reduction Act of 1995

If a portion of the contract seeks information from ten or more members of the public, the contactor will work with the Bureau Information Collection Clearance Officer to obtain a Paperwork Reduction Act clearance from the OMB.

Section 9.0 – Reference Documents

All DOI-specific documents referenced in this document necessary for Contractor review and reference can be provided by the CO/COR.

Section 10.0 – Glossary

Please refer to the NIST online glossary at: https://csrc.nist.gov/glossary.