140R3026Q0079 – Key Inventory for Davis, Hoover & Parker Dams
Combined Synopsis/Solicitation

(i) This is a combined synopsis/solicitation for commercial products or commercial services prepared in accordance with RFO FAR Part 12. This announcement constitutes the only solicitation. Quotes are being requested and a separate written solicitation will not be issued.

Solicitation number 140R3026Q0079 is issued as a request for quotation (RFQ) for a key inventory for Davis, Hoover and Parker Dams.

This acquisition is a 100% set-aside for small business concerns. This solicitation incorporates provisions and clauses by reference. The full text of provisions and clauses may be accessed electronically at www.acquisition.gov.

The North American Industry Classification System (NAICS) Code for this acquisition is: 561990, Inventory Computing Services.
The small business size standard for NAICS Code 561990 is $16.5 Mil.

(ii) For a list of line-item number(s), descriptions, and quantities please see the SF 1449.

(iii) The U.S. Bureau of Reclamation (Reclamation), Lower Colorado Basin, Lower Colorado Dams Office (LCDO) Davis, Hoover and Parker Dams requires a comprehensive inventory of all doors, gates, and specialty access points across Davis Dam in Bullhead City, Arizona, Hoover Dam in Boulder City, Nevada and Parker Dam in Parker, California. This effort will support accurate planning and cost estimation for a full rekeying initiative, ensuring continued security and operational efficiency. The survey will provide:

• Documentation of door-opening deficiencies related to proper hardware installation and operation.
• Cataloging of all relevant details for each opening, including (but not limited to) photographs and cutsheets.
• Recording of existing lock types to support planned upgrades to the key system.
• A survey limited to documenting installed locking and latching devices, controlling hardware (such as closers and operators), and access-control components.
• The ability to produce a complete and actionable cost estimate for a rekeying request.
• Exclusion of documentation related to installed hardware dimensions and physical locations.

The contractor will perform onsite inventories, document hardware conditions, apply QR tags, and upload all data into Openings Studio™, integrated with SimpleK software. This requirement specifically excludes measurement of physical dimensions and precise hardware locations.
All survey and inventory data will be accessible through the Openings Studio desktop platform. The software will interface with LCDO's existing Assa Abloy SimpleK system, which is currently used for key issuance and management.

Please see Attachment 1, Statement of Work. Please see Attachment 3, Brand Name Justification.

(iv) Places of delivery and acceptance: Davis Dam in Bullhead City, Arizona; Hoover Dam in Boulder City, Nevada; Parker Dam in Parker, California. Delivery addresses will be specified at award.

(v) THE FOLLOWING PROVISIONS ARE APPLICABLE TO THIS COMMERCIAL ITEM ACQUISITION:

FAR provision 52.212-1, Instructions to Offerors - Commercial Products and Commercial Services.

a. Addendum to FAR 52.212-1 –Quote Submission Instructions

This addendum replaces the term “offer” with “quote” within the provision 52.212-1.

In addition to the requirements of the Instructions to Offerors – Commercial Products and Commercial Services provision of this RFQ, each offeror shall submit a quote in accordance with the instructions contained in this provision.

b. Offerors shall complete and submit pricing on Attachment 2, Price Schedule, located within this solicitation.

c. Submit the following information:

Unique Entity Identifier (UEI):
Contractor E-mail Address:

FAR provision 52.212-2, Evaluation.

(a) The Government will evaluate quotes using the Lowest-Priced Technically Acceptable (LPTA) process. One firm-fixed price award will be made to the responsible offeror whose quotation is the lowest-priced and is determined to be technically acceptable. Technical acceptability will be evaluated in accordance with the solicitation requirements. An offeror’s quote must meet all minimum technical requirements to be considered for award. Quotes that are not technically acceptable will not be further evaluated. Price will not be evaluated for any offeror deemed technically unacceptable.

(b) Technical Acceptability includes evaluation of:
(1) Conformance to all requirements of the Statement of Work (SOW) and solicitation instructions;
(2) Evidence of the ability to perform the required work, and
(3) Past performance information indicating acceptable performance on similar work, or in the absence of past performance, a Neutral rating. A Neutral past performance rating will not be evaluated favorably or unfavorably.
Award will be made to the lowest-priced offeror that is rated as technically acceptable

The following additional FAR provisions are applicable to this acquisition:

52.204-7 System for Award Management – Registration (RFO Deviation Mar 2026)
52.240-90 Security Prohibitions and Exclusions Representations and Certifications (RFO Deviation Mar 2026)
52.252-1 Solicitation Provisions Incorporated by Reference (Feb 1998)
52.252-5 Authorized Deviations in Provisions (Nov 2020)

(vi) THE FOLLOWING CLAUSES ARE APPLICABLE TO THIS COMMERCIAL ITEM ACQUISITION:

52.203-17 Contractor Employee Whistleblower Rights (Nov 2023)
52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements of Statements (Jan 2017)
52.204-13 System for Award Management Maintenance (RFO Deviation 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 (RFO Deviation May 2026)
52.209-10 Prohibition on Contracting With Inverted Domestic Corporations (RFO Deviation May 2026)
52.212-4 Terms and Conditions – Commercial Products and Commercial Services (RFO Deviation Nov 2025)

52.219-6 Notice of Total Small Business Set-Aside (RFO Deviation Jan 2026)
52.219-28 Post Award Small Business Program Representation (RFO Deviation Jan 2026)
52.222-50 Combatting Trafficking in Persons (RFO Deviation May 2026)
52.222-54 Employment Eligibility Verification RFO Deviation May 2026)
52.222-3 Convict Labor (RFO Deviation May 2026)
52.222-41 Service Contract Labor Standards (RFO Deviation May 2026)
52.222-42 Statement of Equivalent Rights for Federal Hires (May 2014)
52.222-55 Minimum Wages for Contractor Worker Under Executive Order 14026 (RFO Deviation May 2026)
52.222-62 Paid Sick Leave Under Executive Order 13706 (RFO Deviation May 2026)
52.222-90 Addressing DEI Discrimination by Federal Contractors (RFO Deviation May 2026)
52.225-13 Restrictions on Certain Foreign Purchases (Feb 2021)
52.226-8 Encouraging Contractor Policies to Ban Text Messaging While Driving (May 2024)
52.232-33 Payment by Electronic Funds Transfer-System for Award Management (Oct 2018)
52.240-91 Security Prohibitions and Exclusions (RFO Deviation Mar 2026)
52.204-93 Basic Safeguarding of Covered Contractor Information Systems (RFO Deviation May 2026)
52.244-6 Subcontracts for Commercial Products and Commercial Services (RFO Deviation May 2026)
52.252-2 Clauses Incorporated by Reference (Feb 1998)
52.252-6 Authorized Deviations in Clauses (Nov 2020)

DOI-AAAP-0028 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:

None

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.

DOI-AAAP-0055 Internet Protocol version 6 (Jun 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 boundaries utilizing 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 500-267) and corresponding declarations of conformance defined in the USGv6 Test Program. In addition, this system shall maintain interoperability with IPv4 systems and provide at least the same level of performance and reliability 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 and fielded product management.
3. As IPv6 evolves, the Contractor commits to upgrading or providing an appropriate migration path for each item developed, delivered or utilized at no additional cost to the Government. The Contractor shall retrofit all non-IPv6 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 supports both.
6. Any product whose non-compliance 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 to the Government.

DIAR 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.

WBR 1452.201-80 Contracting Officer Representative's Authorities and Limitations – Bureau of Reclamation (May 2018)

(a) Performance of the work under this contract shall be subject to the technical direction of the Reclamation Contracting Officer's Representative (COR). The term "technical direction" is defined to include, without limitation:

(1) Inspecting and accepting or rejecting work performed under the contract.

(2) Representing the Government in technical phases of the work. The COR is responsible for the technical administration of the contract and will provide instructions and interpretations to the Contractor on all technical matters relating to the contract. The COR will supervise or oversee all Government technical and administrative personnel assigned to assist the COR.

(3) Reviewing and, where required by the contract, approving submittals of technical data, shop drawings, samples, literature, plans, or other data required to be delivered by the Contractor to the Government.

(b) The Contractor will receive a copy of the written COR designation from the Contracting Officer. It will specify the extent of the COR's authority to act on behalf of the Contracting Officer.

(c) Technical direction must be within the scope of work stated in the contract. Only the Contracting Officer is authorized to determine if a change is within the scope of the contract; therefore, the COR does not have the authority to, and may not, issue any technical direction that –

(1) Constitutes a direction of additional work outside the Contract requirements;
(2) Constitutes a change as defined in the contract clause entitled "Changes;"

(3) In any manner causes an increase or decrease in the total contract cost, or the time required for contract performance;
(4) Changes any of the expressed terms, conditions or specifications of the contract; or

(5) Interferes with the Contractor's right to perform the terms and conditions of the contract.

(d) All technical direction shall be issued in writing by the COR.

(e) The Contractor must proceed promptly with the performance of technical direction duly issued by the COR in the manner prescribed by this clause and within its authority under the provisions of this clause. If, in the opinion of the Contractor, any instruction or direction by the COR falls within one of the categories defined in (c)(1) through (c)(5) of this clause, the Contractor must not proceed and must notify the Contracting Officer in writing within five (5) working days after receipt of any such instruction or direction and must request the Contracting Officer to modify the contract accordingly. Upon receiving the notification from the Contractor, the Contracting Officer must –

(1) Advise the Contractor in writing after receipt of the Contractor's letter that the technical direction is within the scope of the contract effort and does not constitute a change under the Changes clause of the contract; or

(2) Advise the Contractor that the Government will issue a written change order.

(f) A failure of the Contractor and Contracting Officer either to agree that the technical direction is within the scope of the contract or to agree upon the contract action to be taken with respect to the technical direction will be subject to the provisions of the clause entitled "Disputes."

WBR 1452.223-81 Safety and Health – Bureau of Reclamation (Oct 2022)

(a) The Contractor shall not require any person employed in the performance of this contract (including subcontracts) to work under conditions which are unsanitary, hazardous, or dangerous to an employee's health or safety.
(b) Contractor shall comply with the most current version of the Bureau of Reclamation's Reclamation Safety and Health Standards (RSHS) and, if incorporated, 52.236-13 Accident Prevention.
The RSHS manual shall be obtained at:
http://www.usbr.gov/safety/rshs/index.html
(c) Comply with the standards (29 CFR) issued by the Occupational Safety and Health Administration (OSHA), U.S. Department of Labor, www.osha.gov.
(d) In the event there is a conflict between the requirements contained in paragraphs (b) and (c) referenced herein, or in the Statement of Work (SOW) or Performance Work Statement (PWS), the more stringent requirement shall prevail.
(e) If required in the SOW or PWS, the Contractor shall submit a written proposed safety program as prescribed in the RSHS and the written specifications.
(f) The Contractor shall maintain an accurate record of and shall report to the Contracting Officer (or authorized representative) in the manner prescribed by the Contracting Officer, all cases of death, occupational diseases, or traumatic injury to employees or the public involved, and property damage in accordance with the RSHS and OSHA guidelines.
(g) If the contractor deems that an updated version of the RSHS constitutes a substantive change to the contract, affecting price or time (or both), the contractor may request a contract modification in accordance with the terms of the contract.

WBR 1452.2370-80 Security Requirements – Bureau of Reclamation (Mar 2022) – Alternate VI (Mar 2022)

(a) General Security Requirements:
(1) This clause addresses security requirements, including general procedural requirements, information security requirements, contractor employee suitability requirements, identification card requirements, site security requirements, vessel exclusion barriers, and information technology security requirements. Within this clause, COR means Contracting Officer's Representative. If there is no COR appointed and identified to the Contractor, the term instead will mean the Program Manager or any other authorized individual responsible for technical oversight under the contract. "Work site" means the Government facility, office, construction site, and any other area within the Government office or facility that the Contractor must access to accomplish work under this contract.
(2) The work performed under this contract shall only be accomplished by individuals (in the employment of the Contractor or any subcontractors) whose conduct and behavior is consistent with the efficiency of the Federal Service and the requirements of this contract, and who are acceptable to the contracting officer. If Reclamation finds a Contractor employee to be unsuitable or unfit for his or her assigned duties, the contracting officer will direct the Contractor to remove the individual from the contract and access to the Federal facility at which the contract activities are occurring.
(3) The Contractor's employees governed by this contract may need access to sensitive information and/or sensitive areas. The Federal Government (Government) reserves the right, in its sole discretion, to determine suitability of Contractor personnel and deny access to any sensitive information or project specific area to any personnel for any cause.
(4) The Contractor is responsible for informing and ensuring compliance by its employees with any applicable security procedures of the Government facility where work may be performed under this contract.
(5) Any Contractor employee that will have access to a Federally-controlled facility or information system will be required to have a Government-issued identification card, consisting of a Personal Identity Verification (PIV) Card, a temporary identification card, or a visitor badge. (Note: within the Department of the Interior this card is known as a DOI Access Card.) During performance of the contract, the Contractor shall keep the COR apprised of any changes in personnel, or changes in personnel access or duration, to ensure that performance is not delayed by compliance with credentialing processes.
(6) A Contractor employee will not be provided access to a Government facility or information system until a Government PIV Card, temporary identification card, or visitor identification badge has been issued to the Contractor employee. For those individuals that will be receiving a PIV Card, the

Government may, at its discretion, issue a temporary identification card or visitor identification badge after the electronic background investigation forms have been received and the investigation is initiated.
(7) All Contractor employees shall access the facility via the facility's entry screening system and visibly display the Government-issued PIV Card, temporary identification card, or visitor identification badge at all times. Contractor employees must visibly wear the Government-issued identification card at all times they are on Government facilities. Contractor employees are responsible for the safekeeping of all Government-issued identification cards, whether on-site or off-site. Cards that have been lost, damaged, or stolen must be reported to the COR and DOI Access Sponsor immediately, but not later than within 24 hours. The Contractor shall return all identification cards and card keys and any other Government property and information upon completion of performance or when personnel depart permanently or for a period of 7 days or more. The Contractor may be required to turn in access control cards or identification cards on a daily basis.
(8) Misuse or loss of access control or identification cards, or failure to comply with required surrender of such cards may, at Government discretion, result in Contractor personnel being denied access to the work site, at no cost to Government. The Contractor may be charged up to $500 for each occurrence for any required replacement of Government-issued access control or identification cards due to loss or misuse. At the end of contract performance, or when a Contractor employee is no longer working under this contract, the Contractor shall ensure that all access control and identification cards are returned to the COR.
(9) All Contractor personnel, including subcontractor personnel, with access to the work site shall be U.S. citizens or foreign individuals legally residing in, or legally admitted to, the U.S. For all non-U.S. citizens working under this contract, irrespective of length of time working on the contract, the Contractor shall provide to the COR, legible and valid copies of the individual's passport and visa (unless individual is on the Visa Waiver Program) a minimum of 14 calendar days prior to beginning work or arriving at the facility. A driver's license is not acceptable identification. In addition, a completed form I-94 shall be submitted to the COR upon the individual's arrival at the work facility and prior to beginning work.
(10) The Contractor shall report all contacts with entities, individuals, and counsel/representatives (including foreign entities and foreign nationals) who seek in any way to obtain unauthorized access to sensitive information or areas. The Contractor shall report any violations of contract provisions, laws, executive orders, regulations, and guidance to the contracting officer. The Contractor shall report any information raising a doubt as to whether an individual's eligibility for continued employment or access to sensitive information is consistent with the interests of National Security and the Public Trust.
(11) Unsanctioned, negligent, or willful inappropriate action on the part of the Contractor (or its employees) may result in termination of the contract or removal of some Contractor employees from Reclamation facilities at no cost to the Government. These actions include, but are not limited to, exploration of a sensitive system and/or information, introduction of unauthorized and/or malicious software, inappropriate release of sensitive information, or failure to follow prescribed access control policies and/or security procedures. Failure to comply with Reclamation policies, procedures, or other published security requirements may result in termination of the contract or removal of some contracted employees from Reclamation buildings and/or facilities at no cost to the Government.
(12) All provisions of this clause shall equally apply to all subcontractors. The Contractor shall incorporate the substance of this clause in all subcontracts.
(13) These security requirements apply to all sections of this Contract including Contract Drawings and other Contract Specifications as applicable. Related documents include other general provisions of Construction or Operations and Maintenance type Contracts, including FAR clauses by reference or as amended by related documents.
(b) Information Security Requirements.
(1) Sensitive Information. The term "sensitive information" means any information which warrants a degree of protection and administrative control as defined by Reclamation or that meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act. Sensitive information is generally categorized as CONTROLLED UNCLASSIFIED INFORMATION (CUI), but in some cases may include other unclassified information. (The protection of National Security information is beyond the scope of this clause. If any work on National Security information is required under this contract, it is addressed under other contract clauses.) The Contractor shall protect this type of information from unauthorized release into public domain, or to unauthorized persons, organizations, or subcontractors. Information which,

either alone or in aggregate, is deemed sensitive by Reclamation shall be handled and protected in accordance with Reclamation Directives and Standards SLE 02-01 Identifying and Safeguarding Controlled Unclassified Information (CUI), which is available from the COR or at http://www.usbr.gov/recman/DandS.html#sle.

(i) Any Government-furnished information or material does not become the property of the Contractor and may be withdrawn at any time. Upon expiration or termination of the contract, all documents released to the Contractor and any material created using data from such documents shall be returned to the COR for final disposition. Government-furnished information residing on any electronic systems (laptops, servers, desktops, media) shall be deleted from those systems using a COR-approved data erasure solution. Only with prior authorization from the contracting officer may the Contractor retain the material. The Contractor or subcontractor shall 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 shall be protected from public or private disclosure in accordance with the markings printed on them. All other information relating to the items to be delivered or the services to be performed under this contract shall not be disclosed by any means without prior approval of the contracting officer. Prohibited dissemination or disclosure includes, but is not limited to: permitting access to such information by foreign nationals or by immigrant aliens who may be employed by the Contractor, publication of technical or scientific papers, advertising, disclosure to Contractor staff not investigated and deemed acceptable at the appropriate information sensitivity level, and any other public release. The Contractor shall maintain, and furnish upon request of the contracting officer, records of the names of individuals who have access to sensitive material in its custody and the sensitive material to which the individuals had access. All questions regarding information security, access, and control shall be referred to the COR.

(ii) The Contractor shall not release to anyone outside the Contractor’s organization any sensitive, or otherwise protected information, regardless of medium in which it is contained (for example, film, tape, document, electronic), pertaining to any part of this contract or any Reclamation program or activity, unless the contracting officer 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 shall 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 shall submit its request to the contracting officer ten business days before the proposed date for release. Subcontractors shall submit requests for authorization to release through the prime Contractor to the contracting officer.

(iii) The Contractor shall notify the COR immediately when known or suspected loss/compromise of sensitive information or other documents, notes, drawings, sketches, reports, photographs, exposed film or similar information which may affect the security interests of Government has occurred. This requirement extends to employees and other personnel working on behalf of the Contractor, and expands responsibility to include prompt reporting of security issues, including observed or subsequently discovered efforts by unauthorized persons to gain unauthorized access to sensitive information.

(2) Classified Information.

(i) The disclosure of U.S. Government documents by third parties can result in damage to our national security. While this contract may not deal directly with classified information, each contractor is obligated to protect classified information pursuant to all applicable laws and to use Government information technology systems in accordance with agency procedures so that the integrity of such systems is not compromised.

(ii) Unauthorized disclosures of classified documents (whether in print, on a blog, or on websites, or other electronic or non-electronic media) do not alter the documents' classified status or automatically result in declassification of the documents. To the contrary, classified information, whether or not already posted on public websites or disclosed to the media, remains classified, and must be treated as such by Federal employees and contractors, until it is declassified by an appropriate U.S. Government authority. Executive Order 13526, Classified National Security Information (December 29, 2009), Section 1.1.(c) states, "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." Although the Department has taken steps to prevent access to publicly disclosed classified materials from Departmental computers, it is important to understand our continuing duties and responsibilities in this regard.

(iii) Contractors (which include all employees of the contractor, as well as subcontractors and its

employees performing work for the contractor) are reminded of the following obligations with respect to the treatment of classified information and the use of unclassified government information technology systems:
(iv) The contractor shall not, while using unclassified Government computers or other devices (such as phones or tablets) access documents that are marked classified (including classified documents made publicly available by a third party), as doing so risks that material still classified will be placed onto unclassified systems. This requirement does not restrict contractor access to unclassified, publicly available news reports (and other unclassified material) that may in turn discuss classified material, as distinguished from access to underlying documents that themselves are marked classified (including if the underlying classified documents are available on public web sites or otherwise in the public domain).
(v) For contracts that require access to classified information, the contractor is responsible for obtaining the required national security clearance through the Department of the Defense National Industrial Security Program Operating Manual (NISPOM). Any classified contracts will be coordinated through the Reclamation Chief Security Officer, or for IT requirements, the Bureau Chief Information Security Officer. No contractor shall access classified information unless proper clearances have been obtained and transmitted to Reclamation. For further information, refer to 443 DM 1 or DOD NISPOM 5220.22-M dated February 28, 2006 (incorporating change 2 dated May 18, 2016).
(vi) Classified information shall not be removed from official premises.
(vii) Classified information shall not be disclosed without proper authorization.
(c) Reserved
(d) Reserved
(e) Reserved
(f) Information Technology Security – Basic Security Requirements:
(1) The Contractor shall ensure that its employees, in performance of the contract, receive annual U.S. Department of the Interior (DOI) Federal Information Systems Security Awareness (FISSA) training that also includes Privacy, Records Management and Section 508 Compliance Awareness. The Contractor may use web-based training available from Reclamation to meet this requirement.
(2) The Contractor shall afford Reclamation, including DOI Office of Inspector General, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out a program of IT inspection, investigation, assessment or audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of Reclamation data or to the function of computer systems operated on behalf of Reclamation, and to preserve evidence of computer crime. If the Contractor has a question regarding the access rights or identity of Government employees requesting access to Contractor-operated IT facilities, it should be referred to the COR for resolution before access is granted.
(3) In addition to the notification requirements (b)(4), the Contractor shall immediately notify the COR, of all cyber-related incidents (including the compromise of Contractor- or Government-owned systems for which the Contractor bears operational or management responsibility), regardless of location.
(4) Contractor staff with significant IT security responsibilities associated with systems connected to or being delivered to Reclamation (such as those responsible for supporting or developing Internet accessible systems, supporting or developing systems containing personal identification information, or supporting or developing systems containing financial information), must complete annual role-based IT security training (over and above that required in (e)(1).) If requested by the Contractor, Reclamation will assist on-site Contractor staff in identifying suitable annual role-based training options throughout the contract performance period.
(5) The Contractor shall be responsible for the Information Technology security for all non-Government-owned systems used in the development of turn-key applications (not including Commercial-off-the-Shelf [COTS] software) and systems intended for eventual turn-key delivery to the Bureau of Reclamation in fulfillment of contract requirements. This clause is applicable to all or any part of the contract that includes information technology resources the Contractor is developing on behalf of Reclamation. This includes information technology, hardware, software, databases, networks, and telecommunications systems. Examples of tasks that require these security provisions include:
(i) The design of IT systems or applications that meet overall data processing performance criteria described elsewhere in this contract. Security designs shall be consistent with the requirements of Federal Information Processing Standards (FIPS) Publication 200 and the security categorization of the system.
(ii) The development of turn-key control systems, such as Supervisory Control and Data Acquisition

(SCADA) or similar systems where improper security functionality and performance of the system could result in misoperation of Government resources; and
(iii) The development of or integration of applications (including COTS) and/or hardware, networks, and telecommunications systems into turn-key products where the improper security functionality and performance of the integrated system could result in loss of integrity, confidentiality, or availability of electronic information or data.
(6) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, stored, or used under this contract. For Contractor developed or operated IT systems, an IT System Security Plan must also be developed in compliance with the Federal Information Cybersecurity Modernization Act of 2014 (P.L. 113-283) and all relevant Federal and Reclamation policies and procedures that include, but are not limited to:
(i) Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources; and
(ii) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Guide for Developing Security Plans for Federal Information Systems and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.
(7) Within **15** days after contract award, the Contractor shall submit to the COR its IT Security Plan, and IT System Security Plan (if applicable), for Reclamation approval. This plan must be consistent with and further detail the approach contained in the offeror's quotation, proposal, or sealed bid that resulted in the award of this contract and in compliance with the requirements stated in this clause. The plan, as approved by the CO, shall be incorporated into the contract as a compliance document.

(vii) Quotes are due July 16, 2026 at 2:00 PM, local time (PST). All responsible sources may submit a quote which will be considered by the agency. Quotes shall be submitted via email to Kristen Turner at Kristen_turner@ios.doi.gov .

(viii) Attachments to this RFQ:

Attachment 1 – Statement of Work (SOW)
Attachment 2 – Price Schedule
Attachment 3 – Wage Determinations 2015-5467 Rev 31; 2015-5629 Rev 29; 2015-5593 Rev 31
Attachment 4 – Brand Name Justification