INTEGRITY

NASWA UI Integrity Center

In Partnership with USDOL

Request for Proposal

Information Systems Risk Assessment

March 20, 2020

Contents

Introduction 2

Purpose of This RFP 2

Background 3

Project Scope 3

System and Data Security 6

Background Checks ..... 8~~9~~

Timeline 9

Period of Performance 10

Proposal Submission Elements 10

Past Performance ..... 11~~10~~

PART I – TECHNICAL 11

Factor A. APPROACH 11

Factor B: SYSTEM AND DATA SECURITY 12

Factor C: STAFF EXPERIENCE AND QUALIFICATIONS 12

Factor D - PAST PERFORMANCE 12

Factor E: MANAGEMENT PLAN 12

PART II - BUSINESS 13

Factor F – COST/PRICE 13

Evaluation Criteria 13

Basis for Award (Best Value) 13

Proposal Description and Process 14

Confidentiality 14

Instruction and Response Guidelines 14

Introduction

The Unemployment Insurance (UI) Integrity Center (Center) was established to develop "innovative UI program integrity strategies to reduce improper payments, prevent and detect fraud, and recover any improper payments made." [http://wdr.doleta.gov/directives/attach/UIPL/UIPL_28_12_Acc.pdf] The efforts of the Center are managed by the National Association of State Workforce Agencies (NASWA), Center for Employment Education and Research (CESER) under a cooperative agreement with the US Department of Labor (USDOL).

One of the Center's current tasks is to evaluate the System Security Plan (SSP) of the Integrity Data Hub (IDH) system and the IDH's adherence to the SSP and appropriate security standards.

Purpose of This RFP

The Center seeks to secure a contract for an Information Systems Security Risk Assessment for the IDH. The purpose of this engagement is to request an independent assessment of the IDH's operations, internal controls, and its policies and procedures as well as an assessment of the hosted environment (AWS) that is under the IDH's control.

During the course of the engagement it is expected that the selected vendor will:

- Create a System Security Assessment Plan (SSAP) based upon the Center's existing System Security Plan (SSP) that will include:
  - An initial assessment to review the complete SSP (18 control groups);
  - An annual assessment schedule to review the SSP over a subsequent 3-year period;
  - A vulnerability assessment (penetration testing) to coincide with subsequent annual assessments;
- Execute the SSAP to examine the critical systems security model and workflows in conjunction with the SSP to identify vulnerabilities and threats;
- Recommend modifications to existing policies and procedures;
- Establish a baseline for ongoing annual Risk Assessments;
- Develop Planned Objectives and Milestones (POAMs) and/or Corrective Action Plans (CAPs) for any deficiencies established; and
- Perform penetration testing (Black-box and Grey-box) of the publicly facing IDH systems.

Reponses must be received electronically by 8:00 p.m. Eastern Standard Time on April 17, 2020 at DataHubRFP@naswa.org.

Questions regarding this RFP and additional information on the Data Hub technical architecture should be submitted to DataHubRFP@naswa.org.

Background

The IDH is a secure, centralized, multi-state data analysis tool that allows participating State Workforce Agencies (SWAs) to submit Unemployment Insurance (UI) claims to the IDH where the information can be cross matched with various data sources to identify potentially fraudulent activity. Successful matches are returned to the states for further analysis/investigation in accordance with state-specific policies and procedures.

Participating SWA's can select between various manual and automated communications channels based on the varying levels of resources and technology available to their UI agency. Communication channels include manual processes such as one-off lookups using the IDH website, or spreadsheet upload. More automated channels such as secure FTP and web services are also available.

The IDH is hosted in an AWS Cloud Environment. It has been configured to operate as a Virtual Private Cloud (VPC) within the AWS Cloud. Within the VPC the IDH is implemented as three tiers. The first tier is the front end that handles user input and can be delivered either manually or in batch mode. The second tier is the application tier where comparisons between claims records and the IDH records occur. The third tier is the data tier where the records associated with suspicious activity are maintained.

In 2019 the IDH developed an initial SSP and undertook a security self-assessment as part of this effort. This SSP will serve as the basis for the security assessment that is the subject of this RFP.

The FIPS 199/200 evaluation undertaken as part of SSP established the IDH as a System Sensitivity Level Moderate designation. The SSP was developed using the publication NIST 800-53, Rev 4 as guidance.

Project Scope

The Center is issuing this solicitation to perform an assessment of security controls on an annual ongoing basis to systematically identify programmatic weaknesses and where necessary, establish targets for continuing improvement of the IDH's security, operations, internal controls, and current policies and procedures pertaining to the IT environment. The Center is seeking a comprehensive and best practice Security Assessment to include, but not limited to, the project scope below. Additional materials and documentation can be referenced and attached with the vendor's submission for consideration.

For the purposes of this evaluation the IDH will be considered a security classification of "Moderate", in accordance with the Federal Information Security Management Act (FISMA) and NIST Special Publication 800-60.

It is anticipated that an assessment will occur annually, with the initial assessment covering the complete SSP (18 control groups). This initial assessment will utilize the penetration testing performed in Q1 2020.

Subsequent annual assessments will include an identified sub-set of the control groups contained in the SSP to allow a complete control group assessment to be completed over a 3-year period. Penetration testing will occur annually as a portion of the ongoing assessments. This is a preferred approach, with the vendor submission specifying the proposed solution.

The projects scope includes:

1. **Third Party Security Assessment**: Perform a 3rd party security assessment to confirm that security and data protection controls are in place and compliant to the Center's business needs and in alignment with industry standards such as NIST 800-53, Public Law 113-283, OMB Circular No. A-130, NIST Special Publication 800-70, and/or other applicable industry acceptable standards.

2. **Review existing IT Security Policies/Practices and Procedures** The vendor will review current state of Information security policies and standards and benchmark against the Integrity Data Hub operational needs and commonly accepted industry standards.
   Deliverables:
   a. Review currently implemented information security policies and standards;
   b. Benchmark current policies and standards against industry standards including NIST, FISMA and OMB standards;
   c. Review the discovered gaps and observations with IDH and Integrity Center management; and
   d. Develop and finalize revised information security policies and standards

3. **Vulnerability Assessment –** Perform in-depth cybersecurity vulnerability assessment and penetration testing of IDH's publicly facing application and infrastructure:
   - All external public facing systems to include firewalls, load balancers, web servers, ftp servers, and web service interface points.
   - Review the service level agreement with AWS for physical access controls. Determine if the current physical security is effective and meets required standards;
   - Social Engineering - perform social engineering procedures to verify the existence and effectiveness of procedural controls to prevent unauthorized physical and electronic access to the IDH. These procedures should be performed without the knowledge of systems staff at a time to be coordinated with the IDH management team.
   - Penetration testing – perform exploit procedures designed to determine the resistance of the IDH systems to malicious exploits launched via the Internet. This testing will attempt to compromise systems, networks, and operating systems to identify vulnerabilities. Penetration testing should be performed from two perspectives:
     1. An outside attacker with no approved system access (Black Box)
     2. A malicious insider who has access to the system (Grey Box)
     3. Evidence as proof of compromised must not impact the confidentiality, integrity, availability, or operation of the systems, data, and applications.

   Deliverables
   1. An executive summary including overall severity of findings and risk exposure.
   2. Provide a detailed report on test and attack scenarios utilized, the vulnerabilities, if any, discovered, and assign a risk score to these vulnerabilities.
   3. Remediation recommendations to address any deficiencies identified.

4. **Virus and Malware Protection –** evaluate the software, systems, and procedures used to prevent impact from viruses and malware. Perform threat analysis to identify any potential vulnerabilities.

5. **Logon Security –** evaluate logon methodology and policies for internal IDH systems users, administrators, developers, and external application users and provide input on improvements to address any deficiencies identified.

6. **Develop a Vulnerability Assessment Plan -** The vendor will conduct a comprehensive Cybersecurity Program Maturity Assessment using an objective and independent framework developed by the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) including IDH's people, organizational structure, processes, and supporting technology.

The overall objectives of this phase will be to assist the IDH in improving the understanding of the existing maturity of the Cybersecurity program in comparison to industry standards, develop a sustainable risk management program, and provide observations and recommendations for overall program improvement.

Key Tasks – Assess the IDH's ability to protect its information assets and its preparedness against cyber-attack on the following items:

- *Leadership and governance:* management, their due diligence, ownership, and effective management of risk within the context of the organization's goals, objectives and the external threat/risk landscape.
- *Human factors*: The level of security-focused culture that empowers and ensures the right people, skills, culture, and knowledge.
- *Information risk management*: Organization's approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners.
- *Operations and technology*: The level of control measures implemented within the organization to address identified risks and minimize the impact of compromise.
- *Business continuity*: Organizations preparations for a security incident and its ability to prevent or minimize the impact through successful crisis and stakeholder management.

Deliverables:

- Maturity and risk rating, including but not limited to:
  - Highlight successes and identify gaps ;
  - Security maturity comparison against similar organizations (public/non-profit sector) and similarly sized organizations; and
  - Rank criticality of gaps.

- Identify security/privacy risks in current practices inclusive of:
  - Organizational/Personnel (Skill/Knowledge Level)
  - Policy/Process/Procedures;
  - Tools, Methods, Implementation and Operations specific issues; and
  - Access, implementation of industry/leading practices.

- Develop detailed recommendations to close gaps which includes:
    - o Recommend mitigation solutions; and
    - o Estimated deployment timelines.

The vendor shall propose a recommended ongoing risk management and vulnerability review in which the vendor will be participate in annual subsequent security evaluations to determine progress and suitability of remediation efforts.

7. **Final report** – The vendor will develop a report of the vendor's assessment of the IDH's IT risk, management policies, and SSP and present a written report to the IDH and Integrity Center management team. Included in the final report and presentation will be a prioritized list of recommended or required improvements. The final report shall include and executive summary and presentation for non-technical management.

System and Data Security

During the assessment of the IDH systems the Vendor shall integrate Cybersecurity Risk Management into the service planning, delivery, and management to stay consistent with the NIST Cybersecurity Framework.

The Vendor is subject to all federal security laws, rules, regulations, guidance and standards applicable to the product and/or services offered, pursuant to the following authorities (including but not limited to):

The confidentiality, integrity, and accessibility of information and information systems:

(a) Public Law 113-283, Federal Information Security Modernization Act (FISMA) of 2014
(b) OMB Circular No. A-130, Managing Information as a Strategic Resource

The use of common security configurations:

(c) Federal Acquisition Regulation (FAR), Part 39 of Federal Acquisition Regulation
(d) NIST Special Publication 800-70, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers

The IDH implementation, in accordance with the Federal Information Security Management Act (FISMA) and NIST Special Publication 800-60, shall be considered a security classification of "Moderate". Therefore, Vendor interactions with the IDH systems shall be required to follow the corresponding minimum-security controls, processes, and protocols defined in NIST Special Publication 800-53[1]. These controls include, but are not limited to:

1. Data Transmission and Storage:
    - Use of encryption for all data at rest and during transmission
    - Ensure all data provided by the IDH for assessment purposes is purged from the system following analysis
    - Data from the IDH is not shared with any other entity, and are only available to the IDH
    - Ensure that all data stored using cloud-based infrastructure resides on servers based in the United States

[1] https://nvd.nist.gov/800-53

2. System Access and Monitoring:
    - Access to the IDH system and associated data is restricted to authorized users
        - The Vendor shall comply with personal identity verification procedures for staff and include this requirement in all contracts/subcontracts when the contractor/subcontractor has access to Center data
        - Restrict access of Vendor staff to production system/data and limit access to Center data by contractors and/or subcontractors
        - Functionality available to Vendor's users will be based on user role
        - Bi-annual validation and re-certification of all system user accounts
    - Ensure user access and all transactions are monitored
        - Maintenance of system logs to track user activity and transactions, including user ID and timestamp

3. Adhere to Privacy Breach Notification Requirements:
    - Definitions
        - "Breach" is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where--
        - A person other than an authorized user accesses or potentially accesses PII; or
        - An authorized user accesses or potentially accesses PII for an unauthorized purpose.
        - "Information" is defined as any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms (See Office of Management and Budget (OMB) Circular No. A-130, Managing Federal Information as a Strategic Resource).
        - "Information System" is defined as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).
        - "Personally Identifiable Information (PII)" is defined as 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. (See Office of Management and Budget (OMB) Circular No. A-130, Managing Federal Information as a Strategic Resource).
    - Requirements:
        - Contractors and subcontractors who collect or maintain claimant information on behalf of the Center or uses or operates an information system on behalf of the Center, shall comply with Federal law e.g., FISMA 2014, E-Government Act and the Privacy Act. Additionally, the Vendor shall meet OMB directives and National Institute of Standards and Technology Standards to ensure processing of PII is adequately managed, including:

            a) Properly encrypt PII in accordance with appropriate laws, regulations, directives, standards or guidelines;
            b) Report to the Center any suspected or confirmed breach in any medium or form, including paper, oral, and electronic within one hour of discovery;
            c) Cooperate with and exchange information with IDH as well as allow for an inspection, investigation, forensic analysis, as determined necessary by the

Center, in order to effectively report and manage a suspected or confirmed breach;

d) Maintain capabilities to determine what information was or could have been compromised and by whom, construct a timeline of user activity, determine methods and techniques used to access Center information, and identify the initial attack vector;

e) Ensure staff that have access to systems or information are regularly trained to identify and report a security incident;

f) Take steps to address security issues that have been identified, including steps to minimize further security risks to those individuals whose PII was lost, compromised, or potentially compromised; and

g) Report incidents in accordance with the Center's incident management policy and US-CERT notification guidelines.

- Remedy:

a) A report of a breach shall not, by itself, be interpreted as evidence that the Vendor or its subcontractor (at any tier) failed to provide adequate safeguards for PII. If the Vendor is determined to be at fault for the breach, the Vendor may be financially liable for Center costs incurred in the course of breach response and mitigation efforts;

b) The Vendor shall take steps to address security issues that have been identified, including steps to minimize further security risks to those individuals whose PII was lost, compromised, or potentially compromised; Additionally, the individual or individuals directly responsible for the data breach shall be removed from the contract within 45 days of the breach of data;

c) The Center reserves the right to exercise all available contract remedies including, but not limited to, a stop-work order on a temporary or permanent basis in order to address a breach or upon discovery of a Vendor's failure to report a breach as required by this clause. If the Vendor is determined to be at fault for a breach, the Vendor shall provide credit monitoring and privacy protection services for one year to any individual whose private information was accessed or disclosed. The individual shall be given the option, but the decision is theirs. Those services will be provided solely at the expense of the Vendor and will not be reimbursed by the Center.

Background Checks

All contract/subcontract employees with access to PII data related to the IDH solution will require background investigation. The Vendor will certify to the Center that all staff including contract/subcontract employees have successfully completed the appropriate level of background investigation for each position used by the vendor on this project. The Vendor and its subcontractors, if any, will ensure that investigation requirements for employees are based on the risk or sensitivity level designation of the position. The Center informs the Contractor of the risk or sensitivity level for each contractor employee position. The minimum level of investigation for each risk or sensitivity level is:

Position Risk/Sensitivity Level:	Minimum Investigation Requirement:
Low Risk/Non-sensitive:	National Agency Check & Inquiries (NACI)
Moderate Risk:	Minimum Background Investigation (MBI)
High Risk:	Background Investigation (BI)
Noncritical-Sensitive:	Minimum Background Investigation (MBI)
Critical-Sensitive:	Single Scope Background Investigation (SSBI)

For positions with significant security responsibilities such as the ability change security controls, bypass and/or manipulate audit logs, and directly access and extract large amounts of data outside of normal user interfaces, the minimum risk designation shall be “High Risk”. Occupations that frequently have significant security responsibilities include, but are not limited to, system administrators, database administrators, and developers.

Timeline

The RFP timeline of events:

RFP Activity	Timeline
Risk Assessment RFP Issued	March 30, 2020
Final Clarification Questions	April 15, 2020
Questions and Responses Posted	April 30, 2020
Proposals Due	May 6, 2020
Award (anticipated)	May 20, 2020

The Center reserves the right to invite offerors to participate in detailed discussions, clarifications to responses, and presentations/demonstrations subsequent to the proposal due date.

Deliverable timeline:

Project Activity	Timeline	Suggested
Project Plan Due		15 Days from Award
Assessment Start		30 Days from Award
Assessment Complete		90 Days from Award
First Assessment Report Delivered		120 Days from Award
First Penetration Testing Start	May, 2021	
Penetration Testing Complete		30 Days from Start
Second Assessment Start	June, 2021	
Assessment Complete		90 Days from 2nd Start
Second Assessment Report Delivered		120 Days from 2nd Start
Second Penetration Testing Start	May 2022	
Penetration Testing Complete		30 Days from Start
Third Assessment Start	June, 2022	
Assessment Complete		90 Days from 3rd Start
Third Assessment Report Delivered		120 Days from 3rd Start
Third Penetration Testing Start	May, 2023	
Penetration Testing Complete		30 Days from Start
Forth Assessment Start	June, 2023	
Assessment Complete		90 Days from 4th Start
Forth Assessment Report Delivered		120 Days from 4th Start

Period of Performance

The Period of Performance for this procurement is from the date of the execution of the contract through the 2023 Final Report Presentation tentatively scheduled for August 2023.

Proposal Submission Elements

The offeror's proposal submitted in response to this RFP shall include two parts - Part I – Technical and Part II – Business, as listed below. The proposal shall include a transmittal letter. The transmittal letter shall identify the solicitation name/number. The transmittal letter shall include the name and DUNS number of the firm submitting the proposal, the firm's address, and a contact name and phone number. The transmittal letter shall also identify any proposed subcontractors. The transmittal letter must contain a statement to the effect that the proposal is guaranteed for a period of at least one hundred and twenty (120) days from the date of proposal receipt by the Center.

Part I **Technical**		**FORMAT**	**PAGE LIMIT**
Factor A	Approach	Written	20 pages total
Factor B	System and Data Security	Written	5 pages total
Factor C	Staff Experience and Qualifications	Written	10 pages total

Part II **Business**		**FORMAT**	**PAGE LIMIT**
Factor D	Past Performance	Written	3 References, 6 pages total
Factor E	Management Plan	Written	8 pages total
Factor F	Cost/Price	Written	No Limit

Offerors must not exceed the page limits cited above. Proposals submitted in excess of the prescribed page limits shall be considered non-responsive and shall be removed from consideration. Written parts of the proposal shall be formatted as follows:

Page Size:	8 ½ x 11" with at least 1" margins on all sides
Font Size:	12 point or larger
Page Numbering:	Pages consecutively numbered within each section
Page Count:	Title pages, tables of contents, and section dividers are <u>not included in the page count</u>
Format:	Two-column format is allowable

The Center takes seriously the intent of the Procurement Integrity and Ethics statutes. Any proposal found to be copied from a potential competitor is subject to disqualification and, therefore, ineligible for contract award. Price and Cost information must not be included in the Technical Proposal.

PART I – TECHNICAL

Factor A. APPROACH

The offeror shall provide a detailed technical approach for performing and executing each of the tasks listed below for the security evaluation project in a manner that will provide the Center with cost effective and quality services.

1. System Security Assessment Plan (SSAP)
2. System Security Plan (SSP)Evaluation

3. SSP compliance and applicability
4. System Security Assessment based on the SSP and the SSAP
5. Final assessment report, including corrective actions required
6. Penetration Testing Plan as part of assessments to be completed in 2021, 2022, and 2023.

7. Implementation and project management:
   - Provide examples of previous engagements providing security assessments and penetration testing;
   - Provide description for preferred methods of the following for assessment:
     - Assessment Plan requirements gathering;
     - System Security Assessment Planning;
     - Assessment methodologies and anticipated timelines;
     - Estimating implementation timeline post requirements finalization; and
   - Ongoing communications with the IDH security manager, project manager, and project team.

Factor B: SYSTEM AND DATA SECURITY

The offeror shall affirm compliance with all items listed in the System and Data Security Section, with any exceptions noted.

Factor C: STAFF EXPERIENCE AND QUALIFICATIONS

The offeror shall provide three resumes (two pages maximum per resume) for key personnel to be assigned to the project for implementation of proposed solution. Resumes should include: name, proposed labor category, percentage of time allocated to the security assessment project, and relevant work experience. The resume(s) shall include educational and training accomplishments, as well as past work and other relevant experience, including any special accomplishments and skills. Resumes shall include dates of employment, education, etc. Resumes may not exceed six total pages.

Factor D - PAST PERFORMANCE

The offeror shall provide three references, which include the Company/Agency name, address, contact, contact's phone number and the name of the project completed. The work shall be similar in scope (nature and size) to this RFP's statement of work. References must be in relation to work that was performed within the last five years.

Performance information will be used for both responsibility determinations and as an evaluation factor against which offerors' relative rankings will be compared to assure best value to the Center. The Center will focus on information that demonstrates quality of performance. References other than those identified by the offeror may be contacted by the Center. Names of individuals providing reference information about an offeror's past performance shall not be disclosed. References may not exceed six total pages.

Factor E: MANAGEMENT PLAN

A management plan shall include the following:

- A chart showing how the project will be organized, including all tasks and deliverables and the overall leadership, business management, task or team leaders, and staff for each part;
- A timeline or schedule of task and subtask starts, endings, and milestones; and
- A brief overview of how the project will be managed.

PART II - BUSINESS

Factor F – COST/PRICE

Responders should provide a cost estimate to conduct the initial annual assessment and two subsequent annual assessments that include an identified sub-set of the control groups contained in the SSP to allow a complete control group assessment to be completed over a 3-year period.

A cost estimate to conduct annual Penetration testing in years two and three should be included. The Penetration testing will occur annually as a portion of the ongoing assessments. This is a preferred approach, with the vendor submission specifying the proposed solution.

Offerors shall submit their quote with any and all costs. Quote is a fixed price cost, expected resources annotated. Costs will include the initial assessment, three annual assessments, including penetration testing as a separate line item.

Evaluation Criteria

The NASWA project team will evaluate all proposals using the following evaluation criteria and award base contracts to the contractor(s) that represents the best value for NASWA.

The factors are presented in the order of importance (i.e., Factor A has the greatest weight, Factor B the second greatest weight, etc.). Non-price factors, when combined, are significantly more important than price.

Please be advised that offerors will be evaluated under these factors based on the following:

- Factor A: Technical Approach
- Factor B: Information Security
- Factor C: Staff Experience and Qualifications
- Factor D: Management Plan
- Factor E: Past Performance
- Factor F: Price

Basis for Award (Best Value)

The Center intends to evaluate proposals based on the evaluation criteria listed above and make award without discussions to the offerors. However, the Center reserves the right to conduct discussions if later determined to be necessary. Therefore, each offer should contain the best terms from a cost or price and technical standpoint.

Award will be based on the combined evaluations of Technical, Past Performance, and Price. The contract resulting from this competition will be awarded to the responsible offeror whose offer, conforming to the requirements, is determined to provide the "best value" to the Center, which may not necessarily be the proposals offering the lowest price nor receiving the highest technical rating.

Although non-price factors, when combined, are significantly more important than price, price is an important factor and should be considered when preparing responsive offers (proposals).

When offerors are considered essentially equal in terms of non-price factors or when price is so significantly high as to diminish the value of the technical superiority to the Center, price may become the determining factor for contract award. In summary, price/non-price trade offs will be made, and the extent to which one may be sacrificed for the other is governed only by the tests of rationality and consistency with the established factors.

Proposal Description and Process

Participation in this RFP process is voluntary. All costs incurred in responding to, or in participating in this RFP, will be the responsibility of the vendors, or other third-party organizations participating in the RFP, and not that of the Center.

Confidentiality

Any document submitted in response to this RFP that contains confidential information must be marked by a watermark on the appropriate pages as “Confidential.” The confidential information must be clearly identifiable to the reader as confidential. All other information will not be treated as confidential. Note all confidential information is for the Center’s use evaluating proposals in response to this RFP.

Instruction and Response Guidelines

Responses to this RFP shall adhere to the page limits specified and must be in narrative form and provide details on vendor product capabilities. Responses must be viewable with Microsoft Word or Adobe Acrobat and printable on 8.5” x 11” paper, must use 12-point font, the margins of each page should be at least ½ inch, and each page should contain a page number in the footer.

Reponses must be received electronically by 8:00 p.m. Eastern Daylight Time on May 6, 2020. Responses will be sent to the email address of the sender along with any additional email addresses included in the submittal.

Please ensure that the submittal is in Microsoft Word or PDF format. All responses must be submitted electronically to the following email address: DataHubRFP@naswa.org

Telephone calls regarding this RFP will not be accepted. Questions may be submitted by email up to 5:00 p.m. Eastern Daylight Time, May 15, 2020. The Center will review post questions and answers to the RFP website.