United States Attorney's Office
Northern District of Alabama
1801 Fourth Avenue North
Birmingham, AL 35203

Solicitation Number: 15JA01-19-Q-00000004

Agency: Department of Justice
Office: United States Attorney's Office, Northern District of Alabama

Contracting Officer/P.O.C.: Christopher J. Givens
Phone: 205-244-2050 Email: Christopher.Givens@usdoj.gov

Notice type:
Combined Synopsis/Solicitation

Original Posted Date:
August 2, 2019

Posted Date:
August 2, 2019 12:00pm Central

Response Date and Time:
August 7, 2019 12:00pm Central

Original Set Aside:
Total Small Business

Classification Code:
54 – Professional, Scientific, and Technical Services

NAICS Code:
541199 – All Other Legal Services

Synopsis:
August 2, 2019

This solicitation will be advertised as a **Total Small Business Set-Aside**. The NAICS code for this solicitation is 541199 (Small Business Size Standard of $11 Million).

This is a combined synopsis/solicitation for commercial items prepared in accordance with the format in Subpart 12.6, as supplemented with additional information included in this notice. This announcement constitutes the only solicitation; proposals are being requested and a written solicitation will not be issued.

The solicitation number 15JA01-19-Q-00000004 shall be used to reference any written quote provided under this request for quote.

The solicitation document and incorporated provisions and clauses are those in effect through Federal Acquisition Circular 2005-89.

Description of Services: This solicitation is for a firm fixed price contract, which consists of one part-time professional law enforcement paralegal, to provide litigation support services at the United States Attorney's Office, Northern District of Alabama located in Huntsville, Alabama. Proposals will be evaluated utilizing the evaluation of commercial items under FAR 52.212-2. **The deadline for submitting a response to this combined synopsis /solicitation is August 7, 2019, at 12:00pm Central.**

52.212-2 Evaluation – Commercial Items (Oct 2014)

(a) The Government will award a contract resulting from this solicitation to the responsible offeror whose offer conforming to the solicitation will be most advantageous to the Government, price and other factors considered. The following factors shall be used to evaluate offers:

Proposed Key Personnel
Past Performance
Experience
Price

(b) Options. The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that an offer is unacceptable if the option prices are significantly unbalanced. Evaluation of options shall not obligate the Government to exercise the option(s).

(c) A written notice of award or acceptance of an offer, mailed or otherwise furnished to the successful offeror within the time for acceptance specified in the offer, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.
(End of provision)

Period of Performance: September 21, 2019 through September 20, 2020

This solicitation requires registration with the System for Award Management (SAM) in order to be considered for award, pursuant to applicable regulations and guidelines. Registration information can be found at www.sam.gov. Registration must be "ACTIVE" at the time of award.

Contracting Office Address:
United States Attorney's Office
Northern District of Alabama
1801 Fourth Avenue North
Birmingham, AL, 35203

Place of Performance:
United States Attorney's Office
Northern District of Alabama
Huntsville Branch Office
400 Meridian Street, Suite 304

Huntsville, AL 35801

Contract Clauses

Local Clauses

Notice of Contractor Personnel Security Clearance Requirements (May 2016)

Where performance under this contract/task or delivery order/call requires contractor personnel to have access to Department of Justice (DOJ) information, systems or facilities, contractor personnel will be subject to the background clearance requirements of Homeland Security Presidential Directive (HSPD)-12, OMB Guidance Memorandum M-05-24, FIPS Publication 201 and DOJ policy implementing HSPD-12 requirements.

Background clearance requirements are determined by the risk level of each position, type of access and length of access required. Further information on background security clearance requirements applicable to contractor personnel proposed for performance on this contract/order/call may be obtained from the Contracting Officer.

All contractor personnel must meet the DOJ Residency Requirements. He/She must have lived in the United States three of the last five years immediately prior to start of performance on this contract/order/call, and/or worked for the United States overseas in a federal or military capacity, and/or be a dependent of a federal or military employee serving overseas. Specific limited waiver request requirements - contractor personnel performing duties for a cumulative total of 14 days or less where there is a critical need for their specialized and unique skills (as solely determined by the Government) may be proposed for a waiver of the Residency Requirement by the contractor. Contractor personnel who are non-US citizens proposed for such a waiver of the Residency Requirement must be from a country allied with the United States (Since the countries on the Allied Countries List are subject to change, the contractor may review the following website for current information:

http://www.opm.gov

For contracts/orders/calls where access to DOJ information systems is involved, non-US citizens are not permitted to have access to or assist in the development, operation, management or maintenance of any DOJ IT system, unless a waiver is granted by the head of the Component, with concurrence of the Department Security Officer (DSO) and DOJ Chief Information Officer (CIO). Any such waiver must be in writing and be obtained prior to allowing any contractor employee who is the subject of the waiver request to begin work under this contract/order/call.

The above requirements apply to any and all contractor employees requiring access to DOJ information systems or facilities, including subcontractor personnel, if applicable.
(End of clause)

Security of Department Information and Systems (April 2015)

I. Applicability to Contractors and Subcontractors

This clause applies to all contractors and subcontractors, including cloud service providers ("CSPs"), and personnel of contractors, subcontractors, and CSPs (hereinafter collectively,

"Contractor") that may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information. It establishes and implements specific DOJ requirements applicable to this Contract. The requirements established herein are in addition to those required by the Federal Acquisition Regulation ("FAR"), including FAR 11.002(g) and 52.239-1, the Privacy Act of 1974, and any other applicable laws, mandates, Procurement Guidance Documents, and Executive Orders pertaining to the development and operation of Information Systems and the protection of Government Information. This clause does not alter or diminish any existing rights, obligation or liability under any other civil and/or criminal law, rule, regulation or mandate.

II. General Definitions

The following general definitions apply to this clause. Specific definitions also apply as set forth in other paragraphs.

A. **Information** means any communication or representation of knowledge such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual. Information includes information in an electronic format that allows it be stored, retrieved or transmitted, also referred to as "data," and "personally identifiable information" ("PII"), regardless of form.

B. **Personally Identifiable Information (or PII)** means any information about an individual maintained by an agency, including, but not limited to, information related to education, financial transactions, medical history, and criminal or employment history and information, which can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

C. **DOJ Information** means any Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of the DOJ, including, without limitation, Information related to DOJ programs or personnel. It includes, without limitation, Information (1) provided by or generated for the DOJ, (2) managed or acquired by Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired in order to perform the contract.

D. **Information System** means any resources, or set of resources organized for accessing, collecting, storing, processing, maintaining, using, sharing, retrieving, disseminating, transmitting, or disposing of (hereinafter collectively, "processing, storing, or transmitting") Information.

E. **Covered Information System** means any information system used for, involved with, or allowing, the processing, storing, or transmitting of DOJ Information.

III. Confidentiality and Non-disclosure of DOJ Information

A. Preliminary and final deliverables and all associated working papers and material generated by Contractor containing DOJ Information are the property of the U.S. Government and must be submitted to the Contracting Officer ("CO") or the CO's Representative ("COR") at the conclusion of the contract. The U.S. Government has unlimited data rights to all such deliverables and associated working papers and materials in accordance with FAR 52.227-14.

B. All documents produced in the performance of this contract containing DOJ Information are the property of the U.S. Government and Contractor shall neither reproduce nor release to any third-party at any time, including during or at expiration or termination of the contract without the prior written permission of the CO.

C. Any DOJ information made available to Contractor under this contract shall be used only for the purpose of performance of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this contract. In performance of this contract, Contractor assumes responsibility for the protection of the confidentiality of any and all DOJ Information processed, stored, or transmitted by the Contractor. When requested by the CO (typically no more than annually), Contractor shall provide a report to the CO identifying, to the best of Contractor's knowledge and belief, the type, amount, and level of sensitivity of the DOJ Information processed, stored, or transmitted under the Contract, including an estimate of the number of individuals for whom PII has been processed, stored or transmitted under the Contract and whether such information includes social security numbers (in whole or in part).

IV. Compliance with Information Technology Security Policies, Procedures and Requirements

A. For all Covered Information Systems, Contractor shall comply with all security requirements, including but not limited to the regulations and guidance found in the Federal Information Security Management Act of 2014 ("FISMA"), Privacy Act of 1974, E-Government Act of 2002, National Institute of Standards and Technology ("NIST") Special Publications ("SP"), including NIST SP 800-37, 800-53, and 800-60 Volumes I and II, Federal Information Processing Standards ("FIPS") Publications 140-2, 199, and 200, OMB Memoranda, Federal Risk and Authorization Management Program ("FedRAMP"), DOJ IT Security Standards, including DOJ Order 2640.2, as amended. These requirements include but are not limited to:

1. Limiting access to DOJ Information and Covered Information Systems to authorized users and to transactions and functions that authorized users are permitted to exercise;

2. Providing security awareness training including, but not limited to, recognizing and reporting potential indicators of insider threats to users and managers of DOJ Information and Covered Information Systems;

3. Creating, protecting, and retaining Covered Information System audit records, reports, and supporting documentation to enable reviewing, monitoring, analysis, investigation, reconstruction, and reporting of unlawful, unauthorized, or inappropriate activity related to such Covered Information Systems and/or DOJ Information;

4. Maintaining authorizations to operate any Covered Information System;

5. Performing continuous monitoring on all Covered Information Systems;

6. Establishing and maintaining baseline configurations and inventories of Covered Information Systems, including hardware, software, firmware, and documentation, throughout the Information System Development Lifecycle, and establishing and enforcing security configuration settings for IT products employed in Information Systems;

7. Ensuring appropriate contingency planning has been performed, including DOJ Information and Covered Information System backups;

8. Identifying Covered Information System users, processes acting on behalf of users, or devices, and authenticating and verifying the identities of such users, processes, or devices, using multifactor authentication or HSPD-12 compliant authentication methods where required;

9. Establishing an operational incident handling capability for Covered Information Systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, and tracking, documenting, and reporting incidents to appropriate officials and authorities within Contractor's organization and the DOJ;

10. Performing periodic and timely maintenance on Covered Information Systems, and providing effective controls on tools, techniques, mechanisms, and personnel used to conduct such maintenance;

11. [Reserved]

12. Protecting Covered Information System media containing DOJ Information, including paper, digital and electronic media; limiting access to DOJ Information to authorized users; and sanitizing or destroying Covered Information System media containing DOJ Information before disposal, release or reuse of such media;

13. Limiting physical access to Covered Information Systems, equipment, and physical facilities housing such Covered Information Systems to authorized U.S. citizens unless a waiver has been granted by the Contracting Officer ("CO"), and protecting the physical facilities and support infrastructure for such Information Systems;

14. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards;

15. Assessing the risk to DOJ Information in Covered Information Systems periodically, including scanning for vulnerabilities and remediating such vulnerabilities in accordance with DOJ policy and ensuring the timely removal of assets no longer supported by the Contractor;

16. Assessing the security controls of Covered Information Systems periodically to determine if the controls are effective in their application, developing and implementing plans of action designed to correct deficiencies and eliminate or reduce vulnerabilities in such Information Systems, and monitoring security controls on an ongoing basis to ensure the continued effectiveness of the controls;

17. Monitoring, controlling, and protecting information transmitted or received by Covered Information Systems at the external boundaries and key internal boundaries of such Information Systems, and employing architectural designs, software development techniques, and systems engineering principles that promote effective security; and

18. Identifying, reporting, and correcting Covered Information System security flaws in a timely manner, providing protection from malicious code at appropriate locations, monitoring security alerts and advisories and taking appropriate action in response.

B. Contractor shall not process, store, or transmit DOJ Information using a Covered Information System without first obtaining an Authority to Operate ("ATO") for each Covered Information System. The ATO shall be signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under this contract. The DOJ standards and requirements for obtaining an ATO may be found at DOJ Order 2640.2, as amended. (For Cloud Computing Systems, see Section V, below.)

C. Contractor shall ensure that no Non-U.S. citizen accesses or assists in the development, operation, management, or maintenance of any DOJ Information System, unless a waiver has been granted by the by the DOJ Component Head (or his or her designee) responsible for the DOJ Information System, the DOJ Chief Information Officer, and the DOJ Security Officer.

D. When requested by the DOJ CO or COR, or other DOJ official as described below, in connection with DOJ's efforts to ensure compliance with security requirements and to maintain and safeguard against threats and hazards to the security, confidentiality, integrity, and availability of DOJ Information, Contractor shall provide DOJ, including the Office of Inspector General ("OIG") and Federal law enforcement components, (1) access to any and all information and records, including electronic information, regarding a Covered Information System, and (2) physical access to Contractor's facilities, installations, systems, operations, documents, records, and databases. Such access may include independent validation testing of controls, system penetration testing, and FISMA data reviews by DOJ or agents acting on behalf of DOJ, and such access shall be provided within 72 hours of the request. Additionally, Contractor shall cooperate with DOJ's efforts to ensure, maintain, and safeguard the security, confidentiality, integrity, and availability of DOJ Information.

E. The use of Contractor-owned laptops or other portable digital or electronic media to process or store DOJ Information covered by this clause is prohibited until Contractor provides a letter to the DOJ CO, and obtains the CO's approval, certifying compliance with the following requirements:

1. Media must be encrypted using a NIST FIPS 140-2 approved product;

2. Contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;

3. Where applicable, media must utilize antivirus software and a host-based firewall mechanism;

4. Contractor must log all computer-readable data extracts from databases holding DOJ Information and verify that each extract including such data has been erased within 90 days of extraction or that its use is still required. All DOJ Information is sensitive information unless specifically designated as non-sensitive by the DOJ; and,

5. A Rules of Behavior ("ROB") form must be signed by users. These rules must address, at a minimum, authorized and official use, prohibition against unauthorized users and use, and the protection of DOJ Information. The form also must notify the user that he or she has no reasonable expectation of privacy regarding any communications transmitted through or data stored on Contractor-owned laptops or other portable digital or electronic media.

F. Contractor-owned removable media containing DOJ Information shall not be removed from DOJ facilities without prior approval of the DOJ CO or COR.

G. When no longer needed, all media must be processed (sanitized, degaussed, or destroyed) in accordance with DOJ security requirements.

H. Contractor must keep an accurate inventory of digital or electronic media used in the performance of DOJ contracts.

I. Contractor must remove all DOJ Information from Contractor media and return all such information to the DOJ within 15 days of the expiration or termination of the contract, unless otherwise extended by the CO, or waived (in part or whole) by the CO, and all such information shall be returned to the DOJ in a format and form acceptable to the DOJ. The removal and return of all DOJ Information must be accomplished in accordance with DOJ IT Security Standard requirements, and an official of the Contractor shall provide a written certification certifying the removal and return of all such information to the CO within 15 days of the removal and return of all DOJ Information.

J. DOJ, at its discretion, may suspend Contractor's access to any DOJ Information, or terminate the contract, when DOJ suspects that Contractor has failed to comply with any security requirement, or in the event of an Information System Security Incident (see Section V.E. below), where the Department determines that either event gives cause for such action. The suspension of access to DOJ Information may last until such time as DOJ, in its sole discretion, determines that the situation giving rise to such action has been corrected or no longer exists. Contractor understands that any suspension or termination in accordance with this provision shall be at no cost to the DOJ, and that upon request by the CO, Contractor must immediately return all DOJ Information to DOJ, as well as any media upon which DOJ Information resides, at Contractor's expense.

V. Cloud Computing

A. **Cloud Computing** means an Information System having the essential characteristics described in NIST SP 800-145, The NIST Definition of Cloud Computing. For the sake of this provision and clause, Cloud Computing includes Software as a Service, Platform as a Service, and Infrastructure as a Service, and deployment in a Private Cloud, Community Cloud, Public Cloud, or Hybrid Cloud.

B. Contractor may not utilize the Cloud system of any CSP unless:

1. The Cloud system and CSP have been evaluated and approved by a 3PAO certified under FedRAMP and Contractor has provided the most current Security Assessment Report ("SAR") to the DOJ CO for consideration as part of Contractor's overall System Security Plan, and any subsequent SARs within 30 days of issuance, and has received an ATO from the Authorizing Official for the DOJ component responsible for maintaining the security confidentiality, integrity, and availability of the DOJ Information under contract; or,

2. If not certified under FedRAMP, the Cloud System and CSP have received an ATO signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under the contract.

C. Contractor must ensure that the CSP allows DOJ to access and retrieve any DOJ Information processed, stored or transmitted in a Cloud system under this Contract within a reasonable time of any such request, but in no event less than 48 hours from the request. To ensure that the DOJ can fully and appropriately search and retrieve DOJ Information from the Cloud system, access shall include any schemas, meta-data, and other associated data artifacts.

VI. Information System Security Breach or Incident

A. Definitions

1. **Confirmed Security Breach** (hereinafter, "Confirmed Breach") means any confirmed unauthorized exposure, loss of control, compromise, exfiltration, manipulation, disclosure, acquisition, or accessing of any Covered Information System or any DOJ Information accessed by, retrievable from, processed by, stored on, or transmitted within, to or from any such system.

2. **Potential Security Breach** (hereinafter, "Potential Breach") means any suspected, but unconfirmed, Covered Information System Security Breach.

3. **Security Incident** means any Confirmed or Potential Covered Information System Security Breach.

B. Confirmed Breach. Contractor shall immediately (and in no event later than within 1 hour of discovery) report any Confirmed Breach to the DOJ CO and the CO's Representative ("COR"). If the Confirmed Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call DOJ-CERT at 1-866-US4-CERT (1-866-874-2378) immediately (and in no event later than within 1 hour of discovery of the Confirmed Breach), and shall notify the CO and COR as soon as practicable.

C. Potential Breach.

1. Contractor shall report any Potential Breach within 72 hours of detection to the DOJ CO and the COR, unless Contractor has (a) completed its investigation of the Potential Breach in accordance with its own internal policies and procedures for identification, investigation and mitigation of Security Incidents and (b) determined that there has been no Confirmed Breach.

2. If Contractor has not made a determination within 72 hours of detection of the Potential Breach whether an Confirmed Breach has occurred, Contractor shall report the Potential Breach to the DOJ CO and COR within one-hour (i.e., 73 hours from detection of the Potential Breach). If the time by which to report the Potential Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call the DOJ Computer Emergency Readiness Team (DOJ-CERT) at 1-866-US4-CERT (1-866-874-2378) within one-hour (i.e., 73 hours from detection of the Potential Breach) and contact the DOJ CO and COR as soon as practicable.

D. Any report submitted in accordance with paragraphs (B) and (C), above, shall identify (1) both the Information Systems and DOJ Information involved or at risk, including the type, amount, and level of sensitivity of the DOJ Information and, if the DOJ Information contains PII, the estimated number of unique instances of PII, (2) all steps and processes being undertaken by Contractor to minimize, remedy, and/or investigate the Security Incident, (3)

any and all other information as required by the US-CERT Federal Incident Notification Guidelines, including the functional impact, information impact, impact to recoverability, threat vector, mitigation details, and all available incident details; and (4) any other information specifically requested by the DOJ. Contractor shall continue to provide written updates to the DOJ CO regarding the status of the Security Incident at least every three (3) calendar days until informed otherwise by the DOJ CO.

E. All determinations regarding whether and when to notify individuals and/or federal agencies potentially affected by a Security Incident will be made by DOJ senior officials or the DOJ Core Management Team at DOJ's discretion.

F. Upon notification of a Security Incident in accordance with this section, Contractor must provide to DOJ full access to any affected or potentially affected facility and/or Information System, including access by the DOJ OIG and Federal law enforcement organizations, and undertake any and all response actions DOJ determines are required to ensure the protection of DOJ Information, including providing all requested images, log files, and event information to facilitate rapid resolution of any Security Incident.

G. DOJ, at its sole discretion, may obtain, and Contractor will permit, the assistance of other federal agencies and/or third party contractors or firms to aid in response activities related to any Security Incident. Additionally, DOJ, at its sole discretion, may require Contractor to retain, at Contractor's expense, a Third Party Assessing Organization (3PAO), acceptable to DOJ, with expertise in incident response, compromise assessment, and federal security control requirements, to conduct a thorough vulnerability and security assessment of all affected Information Systems.

H. Response activities related to any Security Incident undertaken by DOJ, including activities undertaken by Contractor, other federal agencies, and any third-party contractors or firms at the request or direction of DOJ, may include inspections, investigations, forensic reviews, data analyses and processing, and final determinations of responsibility for the Security Incident and/or liability for any additional response activities. Contractor shall be responsible for all costs and related resource allocations required for all such response activities related to any Security Incident, including the cost of any penetration testing.

VII. Personally Identifiable Information Notification Requirement

Contractor certifies that it has a security policy in place that contains procedures to promptly notify any individual whose Personally Identifiable Information ("PII") was, or is reasonably determined by DOJ to have been, compromised. Any notification shall be coordinated with the DOJ CO and shall not proceed until the DOJ has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by Contractor shall be coordinated with, and subject to the approval of, DOJ. Contractor shall be responsible for taking corrective action consistent with DOJ Data Breach Notification Procedures and as directed by the DOJ CO, including all costs and expenses associated with such corrective action, which may include providing credit monitoring to any individuals whose PII was actually or potentially compromised.

VIII. Pass-through of Security Requirements to Subcontractors and CSPs

The requirements set forth in the preceding paragraphs of this clause apply to all subcontractors and CSPs who perform work in connection with this Contract, including any CSP providing

services for any other CSP under this Contract, and Contractor shall flow down this clause to all subcontractors and CSPs performing under this contract. Any breach by any subcontractor or CSP of any of the provisions set forth in this clause will be attributed to Contractor.
(End of clause)

Data Security Contract Clause for Contracts Involving the PII of 25 or Fewer Individuals (July 2016)

The following clause applies to all contracts involving the personally identifiable information (PII) of 25 or fewer individuals. PII refers to information that can be used to distinguish or trace an individual's identity, such as his or her name, social security number, biometric records, etc., whether alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. PII is defined at this link: http://www.gsa.gov/portal/content/104256.

Contractors using information systems that are subject to the data security requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) already are subject to the data security standards outlined below, and, therefore, only paragraphs (g), (h), and (i) apply.

(a) Contractors must ensure that computer hardware is secure and shall take the steps outlined below:

(1) **Keep your firewall turned on**: A firewall helps protect your computer from hackers who might try to gain access to crash it, delete information, or even steal passwords or other sensitive information. Software firewalls are widely recommended for single computers. The software is prepackaged on some operating systems or can be purchased for individual computers. For multiple networked computers, hardware routers typically provide firewall protection, although the contractor must verify this.

(2) **Computers must be protected by username/password logins and password-protected screensavers (after 15-min. idle).** Computer accounts cannot be shared with other users. Contractors must report an incident to the EOUSA Security Operations Center at 803-705-5533 within one hour if their account is accessed by another user.

(3) **Install and update your antivirus software**: Antivirus software is designed to prevent malicious software programs from embedding in your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it. Viruses can infect computers without users' knowledge. Most types of antivirus software can be set up to update automatically.

(4) **Install and update your antispyware technology**: Spyware is just what it sounds like—software that is surreptitiously installed on your computer to let others peer into your activities on the computer. Some spyware collects information about you without your consent or produces unwanted pop-up ads on your web browser. Some operating systems offer free spyware protection, and inexpensive software is readily available for download on the Internet or at your local computer store. Be wary of ads on the Internet offering

downloadable antispyware—in some cases these products may be fake and may actually contain spyware or other malicious code.

(5) **Maintain active and supported operating systems and application software.** Computer operating systems (e.g., Windows 8.0) and application software (e.g., Microsoft Word) have a lifecycle that begins when a product is released and ends when it's no longer supported. Install and maintain security updates and fixes updated to stay in tune with technology requirements and to fix security holes. Be sure to install the updates to ensure your computer has the latest protection.

(6) **Be careful what you download**: Carelessly downloading e-mail attachments can circumvent even the most vigilant anti-virus software. Never open an e-mail attachment from someone you don't know and be wary of forwarded attachments from people you do know. They may have unwittingly advanced malicious code.

(7) **Turn off your computer**: With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being "always on" renders computers more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker's connection—be it spyware or a botnet that employs your computer's resources to reach out to other unwitting users.

(b) You must encrypt files related to this project on your computer whenever you are not working on them using a standard software encryption product such as Winzip (Version 18.5 or later with the Windows FIPS 140-2 validated cryptographic modules enabled), Securezip, or any other product that meets Federal Information Processing Standard (FIPS) 140-2. If you do not already have a suitable encryption program on your computer, you can download one of these products easily.

(c) If the data under this contract will be accessed by more than one person, rules of behavior must be signed by users. These rules shall address at a minimum: authorized and official use; prohibition against unauthorized users; and protection of sensitive data and PII. You can comply by having all users sign these rules: 1. Keep all data and information received from the government confidential. 2. Do not leave it unattended in a place where an unauthorized person might read, copy, or take it. 3. Do not transmit it without encryption from one computer to another. 4. If confidentiality is breached, inform [name principal of the contractor] within one hour of suspected breach so the United States can fulfill its obligations.

(d) All PII data must be deleted from **all** contractor-owned devices within 15 days of contract termination or contractor completion. The Contracting Officer (CO) must receive a written certification, either via email or letter, that the contractor has deleted all PII. This bulletin outlines approved method of data destruction; please see Appendix 1, which begins on page 26: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

(e) All files related to this project, and contractor-owned removable media (such as removable hard drives, flash drives, CDs, or floppy disks containing DOJ data) shall not be removed from DOJ facilities (either physically or electronically, such as by email) unless encrypted using a NIST FIPS 140-2 approved product. Please note that this requirement refers to *transferring* information between systems and storage devices (such as back and forth between contractor and DOJ attorney), while paragraph (b) above applies to data while it is on your computer.
NOTE: As an alternative to media encryption, DOJ data may be securely exchanged between contractors and USAO personnel via the approved U.S. Attorneys' File Exchange (USAfx) web portal.

(f) Contractors shall keep an accurate inventory of DOJ-owned devices used on DOJ contracts. It is understood that not all users will receive a DOJ-owned device. If equipment is provided, then the contractor, as well as the USAO providing the devices, must maintain an inventory of accountable DOJ property.

(g) If a data breach is suspected, the contractor shall, within one hour of discovery, report the breach to the EOUSA Security Operations Center (SOC) at 803-705-5533.

(h) The contractor must coordinate with EOUSA and the Department on notifying any individual whose PII was, or is reasonably believed to have been, breached.

(i) The contractor must require that all subcontractors under this contract (if any) adhere to all applicable security contract requirements.

(end of clause)

Continuing Contract Performance During a Pandemic Influenza or other National Emergency (October 2007)

During a Pandemic or other emergencies we understand that our contractor workforce will experience the same high levels of absenteeism as our federal employees. Although the Excusable Delays and Termination for Default clauses used in government contracts list epidemics and quarantine restrictions among the reasons to excuse delays in contract performance, we expect our contractors to make a reasonable effort to keep performance at an acceptable level during emergency periods.

The Office of Personnel Management (OPM) has provided guidance to federal managers and employees on the kinds of actions to be taken to ensure the continuity of operations during emergency periods. This guidance is also applicable to our contract workforce. Contractors are expected to have reasonable policies in place for continuing work performance, particularly those performing mission critical services, during a pandemic influenza or other emergency situation.

The types of actions a federal contractor should reasonably take to help ensure performance are:

Encourage employees to get inoculations or follow other preventive measures as advised by the public health service.

Contractors should cross-train workers as backup for all positions performing critical services. This is particularly important for work such as guard services where telework is not an option.

Implement telework to the greatest extent possible in the workgroup so systems are in place to support successful remote work in an emergency.

Communicate expectations to all employees regarding their roles and responsibilities in relation to remote work in the event of a pandemic health crisis or other emergency.

Establish communication processes to notify employees of activation of this plan.
Integrate pandemic health crisis response expectations into telework agreements.

With the employee, assess requirements for working at home (supplies and equipment needed for an extended telework period). Security concerns should be considered in making equipment choices; agencies or contractors may wish to avoid use of employees' personal computers and provide them with PCs or laptops as appropriate.

Determine how all employees who may telework will communicate with one another and with management to accomplish work.

Practice telework regularly to ensure effectiveness.

Make it clear that in emergency situations, employees must perform all duties assigned by management, even if they are outside usual or customary duties.

Identify how time and attendance will be maintained.

It is the contractor's responsibility to advise the government contracting officer if they anticipate not being able to perform and to work with the Department to fill gaps as necessary. This means direct communication with the contracting officer or in his/her absence, another responsible person in the contracting office via telephone or email messages acknowledging the contractor’s notification. The incumbent contractor is responsible for assisting the Department in estimating the adverse impacts of nonperformance and to work diligently with the Department to develop a strategy for maintaining the continuity of operations.

The Department does reserve the right in such emergency situations to use federal employees. employees of other agencies, contract support from other existing contractors, or to enter into new contracts for critical support services. Any new contracting efforts would be acquired following the guidance in the Office of federal Procurement Policy issuance "Emergency Acquisitions", May, 2007 and Subpart 18.2. Emergency Acquisition Flexibilities, of the Federal Acquisition Regulations.
(End of clause)

Provisions and Clauses Incorporated by Full Text

52.212-2 Evaluation – Commercial Items (OCT 2014)

(a) The Government will award a contract resulting from this solicitation to the responsible offeror whose offer conforming to the solicitation will be most advantageous to the Government, price and other factors considered. The following factors shall be used to evaluate offers:

Proposed Key Personnel
Past Performance
Experience
Price

(b) Options. The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that an offer is unacceptable if the option prices are significantly unbalanced. Evaluation of options shall not obligate the Government to exercise the option(s).

(c) A written notice of award or acceptance of an offer, mailed or otherwise furnished to the successful offeror within the time for acceptance specified in the offer, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.
(End of provision)

52.217-5, Evaluation of Options (JUL 1990)
Except when it is determined in accordance with FAR 17.206(b) not to be in the Government's best interests, the Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. Evaluation of options will not obligate the Government to exercise the option(s).
(End of Provision)

52.217-8, Option to Extend Services (NOV 1999)
The Government may require continued performance of any services within the limits and at the rates specified in the contract. 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 7 days.
(End of Clause)

52.217-9, Option to Extend the Term of the Contract (MAR 2000)
(a) The Government may extend the term of this contract by written notice to the Contractor within 7 days*;* provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.
(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 42 months.
(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/these address(es):
http://www.acquisition.gov/far/ and http://farsite.hill.af.mil/vffar1.htm
(End of Provision)

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):
http://www.acquisition.gov/far/ and http://farsite.hill.af.mil/vffar1.htm
(End of Clause)

Provisions and Clauses Incorporated by Reference

52.209-2, Prohibition on Contracting with Inverted Domestic Corporations - Representation (NOV 2015).

52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (OCT 2015) (31 U.S.C. 6101 note).

52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015).

52.212-1 Instructions to Offerors – Commercial Items (AUG 2018)

52.212-3 Offeror Representations and Certifications – Commercial Items (AUG 2018)

52.212-4 Contract Terms and Conditions – Commercial Items (JAN 2017)

52.212-4 Alternate I Contract Terms and Conditions – Commercial Items (JAN 2017)

52.212-5 Contract Terms and Conditions Required to Implement Statutes or Executive Orders – Commercial Items (AUG 2018)

52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (OCT 2014) (15 U.S.C. 657a).

52.219-6 Notice of Total Small Business Set-Aside (NOV 2011)

52.219-28, Post Award Small Business Program Representation (JUL 2013) (15 U.S.C. 632(a)(2)).

52.222-3, Convict Labor (JUN 2003) (E.O. 11755).

52.222-17, Nondisplacement of Qualified Workers (MAY 2014).

52.222-21, Prohibition of Segregated Facilities (APR 2015).

52.222-26, Equal Opportunity (SEP 2016) (E.O. 11246).

52.222-36, Equal Opportunity for Workers with Disabilities (JUL 2014) (29 U.S.C. 793).

52.222-41 Service Contract Labor Standards (AUG 2018)

52.222-42 Statement of Equivalent Rates for Federal Hires (MAY 2014)

52.222-50, Combating Trafficking in Persons (MAR 2015) (22 U.S.C. 7104(g)).

52.223-18, Encouraging Contractor Policies to Ban Text Messaging while Driving (AUG 2011) (E.O. 13513).

52.224-3, Privacy Training (JAN 2017)

52.225-13, Restrictions on Certain Foreign Purchases (JUN 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

52.232-33, Payment by Electronic Funds Transfer— System for Award Management (JUL 2013) (31 U.S.C. 3332).

52.239-1, Privacy or Security Safeguards (AUG 1996) (5 U.S.C. 552a).

JAR 2852.233-70 Unsafe Conditions Due to the Presence of Hazardous Material (JUN 1996)

STATEMENT OF WORK
PART-TIME PARALEGAL III/SENIOR PARALEGAL
(HUNTSVILLE BRANCH OFFICE) CONTRACTOR SUPPORT FOR THE UNITED STATES ATTORNEYS' OFFICE, NORTHERN DISTRICT OF ALABAMA

1. INTRODUCTION AND SCOPE

Background/Purpose

The mission of the US Attorney's Office (USAO) is to prosecute and defend cases on behalf of the federal government.

2. Contract Term

Base Year: September 21, 2019 to September 20, 2020

3. Pricing Schedule

CLIN	Description	Unit	Estimated Hours	Hourly Rate	Total
0001	Part-Time Paralegal III or Senior Paralegal	HR	616 (Est.)		
0002	Travel	LOT	---	---	$1,500.00

4. Place of Performance

United States Attorney's Office
Northern District of Alabama
Huntsville Branch Office
400 Meridian Street, Suite 304
Huntsville, AL 35801

5. Scope of Work

The Contractor shall provide Legal Support. The District needs one Part-Time Paralegal:

- 1 Criminal Division - Huntsville

The Contractor shall provide all paralegal services required to perform the tasks related to the support of the USAO's Criminal Division by providing a variety of direct assistance to AUSAs, legal assistants, administrative staff, and other USAO personnel.

6. Statement of Work/Tasks

The Contractor is responsible for directly and independently supporting one or more program areas by providing a wide variety of administrative and data entry functions. Work requires knowledge of office skills, personal computers, scanners, copy and fax machines, and an ability to work as a team member and facilitate work processes among other staff members.

Communication skills are extremely important. Works and interacts professionally and effectively with all levels of staff. Ability to meet established deadlines and work as a team player in a professional office setting. Skill in meeting and dealing with people in a courteous and tactful manner.

Applicants must have the ability to use MS Excel, MS Outlook, MS Word, Adobe Acrobat Professional or other department specific databases, VNS, CDCS, FMIS, E2 Travel.

The positions will require the contractor to perform duties or support various divisions of the United States Attorney's office.

Paralegal III/Senior Paralegal

Typical assignments include:

I. Examines, prepares and processes a variety of technical legal documents. Reviews incoming material and determines the need for assembly and preparation of a variety of legal documents, e.g., complaints, motions, orders, answers, pleadings, and subpoenas. Obtains needed information from files, law enforcement agencies, or other sources, and submits completed legal documents to the appropriate Assistant United States Attorney (AUSA). In preparation of documents, considers the nature and the status of the case involved. With limited instructions from the AUSA, prepares such legal actions as indictments, criminal complaints, search warrants, judgments, applications, notices, affidavits, summonses, grand jury subpoenas, rules to show cause, proofs of claim, and satisfaction of judgment. Completes variable aspects of recurring legal documents in conformance with the rules governing their style and format.

Assists with interviews of agents and potential witnesses to assist the AUSA in preparation for grand jury or trial; reviews, summarizes and outlines grand jury and or trial testimony to assist the AUSA in preparation for grand jury or trial; researches, analyzes and summarizes relevant legal precedents for applicability to assigned cases; and prepares digest of points of law involved; analyzes appellate records to isolate facts pertinent to distinct legal issues. Utilizes a variety of automated legal research tools as well as public information databases and other automated resources to research case- or program-specific legal matters, and to participate in assigned areas of criminal or civil proceedings, e.g. electronic discovery.

Reviews documents and other materials produced pursuant to subpoena; maintains inventory of materials produced pursuant to subpoena; and prepares outline of substance of documents/materials produced pursuant to grand jury subpoena.

II. Provides a variety of support assistance services to AUSA staff. Typical assignments are:

Provides litigative case management and organizes cases for court presentation by preparing and organizing exhibits containing a variety of visual material, e.g., statistical charts and photographs. Notes deficiencies in case materials, e.g., missing documents, conflicting statements, and requests further investigation by investigative personnel to correct deficiencies, or personally conducts limited investigations at the pre-trial stage.

Monitors the progress of pending cases and initiates action to insure that legal pleadings, forms, reports, correspondence, and other documents are prepared and submitted within established deadlines. Keeps appropriate staff members informed about the current status of cases.

Compiles, organizes and indexes various discovery and evidence exhibits for trial, witness testimony as it relates to specific criminal charge evidence, and develops and compiles jury instructions to assist AUSA in preparing for trial. Works closely with assigned attorney(s) to insure material is efficiently arranged. Produces and provides to the attorney the appropriate legal documents, information, exhibits, or witnesses at the appropriate time during those court proceedings.

Performs docketing duties such as opening, updating and closing cases through use of the automated case tracking system. As necessary, searches database for required information. Using established databases, performs data searches, report design, and other data retrieval assignments. Reports may be of a recurring nature or of a special, one-time nature based on user information requirements.

Maintains calendar of assigned active cases. Tracks filing, hearing, and trial dates, and scheduling conferences and interviews. Develops and maintains suspense system for ongoing cases and informs the AUSA of pending dates and deadlines. Maintains calendar(s) of the AUSA(s), scheduling appointments, interviews, and conferences, and provides reminders of commitments and court appearances.

Arranges travel by preparing itinerary, and securing transportation and hotel reservations. Prepares travel authorizations and vouchers for signature by authorized government personnel.

III. Produces a variety of written documents and materials utilizing a wide range of office software applications. For example, assignments may include integrating output from different software types, e.g., tables produced by database applications and charts and graphs produced by electronic spreadsheet applications, into word processing or desk top publishing text. Products include complicated tables, graphs and charts which may be incorporated into legal documents or courtroom presentations. Ensures proper format, spelling, punctuation, capitalization, and grammar.

IV. Provides automated litigation assistance to attorney(s). Utilizes various software applications and graphics hardware such as scanners and plotters.

V. Communication skills are extremely important. Works and interacts professionally and effectively with all levels of staff. Ability to meet established deadlines and work as a team player in a professional office setting. Skill in meeting and dealing with people in a courteous and tactful manner.

7. Deliverables/Performance Standards

The Contractor shall prepare and deliver to the Contracting Officer, or other designated government representative, weekly activity reports which detail daily tasks completed and program related activities.

Contractor performance will be monitored and assessed by the Contracting Officer, or other designated government representative, by periodically sampling and reviewing documentation and records for quality and timeliness of work accomplished. The Contracting Officer shall inform the Contractor of any problems as they arise.

The performance standards for successfully completing the activities described above is 95 percent accuracy.

8. Personnel Requirements

The Contractor shall provide qualified personnel who have sufficient experience, education, training, and skills to satisfactorily perform the requirements of this Statement of Work.

Contractor personnel assigned by the contractor in performance of this contract shall be acceptable to the USAO in terms of personal/professional conduct, technical knowledge, and experience.

9. Labor Categories/Personnel Qualifications

Contract employees shall be responsible for the myriad tasks needed to support the USAOs in the area of witness management. Contractors shall perform a variety of tasks related to witness management to include, maintain witness files, complete and process travel vouchers, arrange travel and lodging, enter data in relevant computer systems, and other witness management related duties.

10. Certifications, License, Physical Requirements or Other Expertise Required

The contractor must possess a paralegal certificate.

The contractor must have good communication and organizational skills, the ability to deliver highest quality work under pressure, and knowledge of software used by the USAO (or the ability to acquire knowledge about the USAO's computer systems).

The contractor must have the ability to prove U.S. citizenship and that the contractor personnel meet the Department of Justice residency requirements.

11. Contracting Officer

The Contracting Officer for this contract is:

United States Attorney's Office
Northern District of Alabama
1801 Fourth Avenue North
Birmingham, AL 35203-2101
Attn: Christopher J. Givens, Contracting Officer

Written communications shall make reference to the contract number and shall be emailed to Christopher.Givens@usdoj.gov or mailed to the above-address.

12. Operational Hours

Work will be performed on a full time (40 hours per week) basis as applicable over a five-day work week, with Federal holidays provided in accordance with the Service Contract Act. A list of paid legal holidays observed by the Government is as follows:

1. New Year's Day;
2. Martin Luther King's Birthday;
3. Presidents' Day;
4. Memorial Day;
5. Independence Day;
6. Labor Day;
7. Columbus Day;
8. Veteran's Day;
9. Thanksgiving Day;
10. Christmas Day

Evening and weekend work may be required at times. Overtime is authorized only with prior approval from the USAO and the Contractor.

Holidays and other non-work days are not billable unless work is requested by the Government and performed on these days. No work shall be performed by the Contractor personnel on Government facilities on Federal holidays or other non-work days without prior approval. Work performed on holidays, weekends or other non-work days shall be billable at regular approved rates.

There are certain types of irregularly occurring circumstances that prompt the Government to close its offices where Contractor personnel are working, either on a national or local basis (i.e., bomb threats, inclement weather, power outages, death of a national figure, or funding lapses). Contractor staff shall not work if the Government is closed. Non-work due to the Government closing its facility is not an expense directly reimbursable to the Contractor. However, in those rare instances when the Government operations are curtailed for the balance of a workday that has already commenced, the Contractor may bill for the balance of the scheduled workday with the written acknowledgement of the Contracting Officer's Representative (COR) and the final approval of the Contracting Officer. Employees of the Contractor will not be paid by the Department of Justice for times when, prior to the employee arriving at the workplace, the operations of the Federal agency have been shut-down or curtailed due to unusually severe weather, other Acts of God, budgetary reasons, or other unforeseeable circumstances. The Contractor's Management Plan shall address how the contract employees will be compensated during these periods of time.

13. Travel

All Contractor travel required in the performance of these requirements contained in this contract shall comply with the Federal Travel Regulation, as applicable, in effect on the date(s) the travel is performed. Local travel is considered to be within a fifty-mile radius of the place of performance. For local travel, mileage will be reimbursed at the government rate for local car travel from the USAO where the contractor will be assigned with accurate documentation. Contractor travel will generally entail travel to/from the branch offices, but other travel may also be required, such as attending training provided by EOUSA in Washington, DC. In instances where travel is required, it must be pre-approved in writing by the COR or Contracting Officer. If travel is required overseas in the performance of the

requirements in this contract, it shall be the responsibility of the Contractor to obtain passports, visas, and airline tickets and travel accommodations. Travel requirement will be established as a separate line item with a projected monetary amount for a set period of time. The Contractor shall only invoice against the line item after travel has occurred. All receipts of costs incurred must be submitted with the invoice. It is advised that the Contractor maintains copies of all travel receipts.

14. Contract Type

This will be a firm fixed price contract with hourly rates.

15. Government Furnished Support/Information

The Government will provide contractor personnel with an office environment typically provided to Government personnel that includes workstations, facsimile, telephones, copiers, and computers with relevant software and access to the Internet and local area network (LAN). The Government will provide contractor personnel with materials, documentation, case files, and other items required to perform tasks as delineated herein. The Government will provide each contractor personnel with an identification badge upon successful completion of a National Agency Check with Inquiries (NACI) in accordance with Homeland Security Presidential Directive-12 (HSPD-12) or, in the event of a waiver, an "interim" badge may be issued.

16. Training of Contractor Staff

The Contractor shall be responsible for providing trained, experienced staff for performing the work ordered under this contract, and for continuously monitoring, managing and controlling the work.

The Contractor shall ensure its employees on this contract are trained on "contract-specific" issues such as Department of Justice ethics, standards of conduct, individual conflict of interest, confidentiality requirements, Department of Justice security requirements, understanding the function of reporting, and the importance of quality control and quality assurance. In addition, Contractor managers shall be educated in the terms and conditions of the contract.

No commercial training is authorized.

DOJ Ethics - All contract employees must view the Department of Justice ethics presentation entitled, "Pardon the Ethics Interruption," within the first two weeks of employment. Copies of his presentation may be obtained from the on-site USAO employee in charge of directing the work of the contract employee. The employee should notify the government manager upon completion task. The government manager will notify the COR, who will maintain a record of completion of this training in the official file.

All contract employees must complete the U.S. Office of Government Ethics online training module entitled, "Interacting with Government Employees for Contractors," within the first two weeks of employment. The contractor should notify the government manager upon completion of this training module. The government manager will notify the COR, who will maintain a record of completion of this training in the official file.

Confidentiality Requirements – Signature of a Nondisclosure Agreement is required of all contractor employees. This Agreement must be signed the first day of employment. All signed forms shall be retained in the official file by the CO.

17. Employee Qualifications and Conduct

The Government reserves the right to require the Contractor to reassign from this contract any Contractor employee(s) who is deemed incompetent, careless, unsuitable or otherwise objectionable, or whose continued use under the contract is deemed contrary to the best interests of the Government.

The Contractor shall remove any employee from performance of contract work within five (5) working days of receiving notice from the Contracting Officer that the employee's performance is unsatisfactory. The Contractor shall immediately remove any Contractor employee found to represent a threat to the safety of government records, government employees, or other Contractor employees. In instances where the removal of an employee is for substandard performance or behavior negatively impacting delivery of services, the Contractor will be given an opportunity to address the situation prior to removing the employee.

18. Invoicing Instructions

To constitute a proper invoice, invoices must be submitted on a monthly basis in accordance with FAR 52.212-4(g). The Government will not pay for services not yet received, accepted or pre-approved, as applicable.

Invoices should be addressed to:

United States Attorney's Office
Northern District of Alabama
ATTN: BUDGET OFFICE
1801 Fourth Avenue North
Birmingham, AL 35203-2101

19. Required Proposal Content:

All proposals/quotes shall be broken out into FOUR separate volumes and contain the following information:

(A) Volume I: Proposed Key Personnel

Provide resumes of prospective key personnel. **The proposed key personnel are the Paralegals that will perform the tasks identified in the Statement of Work.** The resume(s) shall demonstrate the key personnel's qualifications to provide the requested services and demonstrate experience in projects of similar size, scope, complexity and results. The resume(s) shall list the Key Personnel's security clearance level, training and certifications, if any.

Provide up to three (3) professional references for each proposed key personnel that can provide past performance information related to the type of work described in the Statement of Work.

Key Personnel references must be clearly labeled "Key Personnel references" and be included in Volume I. If the key personnel do not have references, the offeror must so state (explicitly) in Volume I.

(B) Volume II: Past Performance

Provide up to three (3) **organizational** past performance references for commensurate projects that are in progress or were completed **within the last three (3) years of the Solicitation Issue Date.** If a Contractor will be using a subcontractor, up to three (3) references must be provided for the subcontractor as well.

Past performance references submitted for work that were not in progress or were not completed within the last three (3) years of the Solicitation Issue Date will be accepted; however, these will be considered less relevant than the references within the three year period of the Solicitation Issue Date.

Past performance references may be from commercial or federal/state/local Government contracts; however, similar support services performed for federal government customers generally will be considered more relevant than those done for commercial or state/local government customers. The Contracting Officer has the discretion to retrieve information via offeror supplied references, commercial sources and federal sources including, but not limited to: Past Performance Information Retrieval System and Systems for Award Management.

Organizational past performance references must be clearly labeled "Organizational References" and be included in Volume II. If the organization does not have references, the offeror must so state (explicitly) in Volume II.

The following information is required for each reference:

(a) Customer name and address
(b) Point of contact (name, telephone number) for contractual/administrative matters and technical performance.
(c) Period of contract performance

(d) Description of work performed

If the prime contractor is submitting subcontractor(s) as part of the proposal/quote, include the subcontractor's signed written consent to allow the Government to discuss subcontractor's past performance with the prime contractor.

(C) Volume III: Experience

A summary of the Contractor's **organizational** experience demonstrating the Contractor's knowledge and ability to perform the duties and tasks reflected in the Statement of Work. **This summary shall not exceed two (2) pages.** Specifically address work history to determine whether the vendor has relevant work experience performing similar work to the SOW specific task requirements and staffing accessibility.

If the offeror's experience is not federal experience, the offeror must clearly demonstrate how its non-federal experience relates to the needs in the Statement of Work. The offeror must demonstrate the knowledge and understanding of the Government's needs.

If the offeror exceeds the page limitation or otherwise does not clearly label this summary under Volume III, it will be at the discretion of the contracting officer to select the intended pages for evaluation purposes.

(D) Volume IV: Price

Submit a price proposal as reflected in Section 3, Pricing Schedule, to be evaluated for reasonableness. Do not include asterisks with exceptions or comments on these pages. Only state the price for the CLIN item based on the description of work provided. Any additions to the pricing page other than the CLIN price in the space provided will not be considered.

END OF DOCUMENT