LIMITED-SOURCES JUSTIFICATION

1. Contracting Activity: Department of Veterans Affairs (VA)
Office of Acquisition Operations
Technology Acquisition Center
23 Christopher Way
Eatontown, NJ 07724

2. Description of Action: The proposed action is a non-competitive firm-fixed-price delivery order with Verizon Business Services (VzB) under it's General Services Administration (GSA) Federal Supply Schedule (FSS) Information Technology 70 contract number GS-35-F-0382T for Public Key Infrastructure (PKI) Shared Service Provider (SSP) support for VA's Office of Information and Technology (OI&T), Service Delivery and Engineering (SDE), Enterprise Systems Engineering (ESE), Enterprise Messaging and Collaboration Services.

3. Description of the Supplies or Services: The proposed action will continue current PKI SSP services in support of the PKI certificates issued by VzB under Contract Number GS-35-F-0382T. PKI SSP Services are required to meet the technical specifications and requirements associated with compliance to Homeland Security Presidential Directive 12 and Federal Information Processing Standard 201-1. VA requires a recovery capability for all stored PKI encryption certificates issued. Additionally, VA requires a source to provide revocation for any previously issued certificates that are currently active. The required support shall include configuration, certificate validation, software certificate registration, and device certificate registration. The Period of Performance (PoP) will consist of the base PoP of nine months and one 12 month option period. The total estimated value of the proposed action is $4,182,500.00, inclusive of the option.

4. Authority: This acquisition is conducted under the authority of the Multiple-Award Schedule Program. The specific authority providing for a limited source award is Federal Acquisition Regulation (FAR) Subsection 8.405-6(a)(1)(i)(B), "Only one source is capable of providing the supplies or services required at the level of quality required because the supplies or services are unique or highly specialized."

5. Rationale Supporting Use of Authority Cited Above: The proposed source for this action is VzB, 22001 Loudoun County Parkway, Ashburn, VA 20147. VzB is the current SSP of PKI certificates for VA under delivery order VA118-14-F-0306; contract GS-35F-0382T. Under this order, VzB issues PKI encryption certificates to VA employees and contractors, as well as provides certificate revocation and recovery support. In addition, VzB is the current host and operator of VA's PKI certificate authority. VzB holds PKI encryption certificate key pairs in escrow storage on VA's behalf in accordance with X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework. Hence, when a PKI encryption key is created VzB issues the key pair to the user, and stores a copy of the private key

in a separate data store under its control. This escrow storage is unique and specific to VzB where other vendors do not have access to the data and it cannot be transitioned to another provider due to the requirements to maintain PKI certificate trust relationships with the existing VzB certificate issuing authority.

VA does not possess the ability to retain encryption keys due to the fact that only VzB retains the proprietary rights to the PKI certificates they issue. Only VzB's hosting certificate authority software can provide the required decryption capability and compatibility with encrypted certificates and keys issued to VA employees and contractors. Therefore, only VzB can provide the required PKI certificate recovery and revocation services since only VzB has access to the proprietary data and enterprise databases supporting automated PKI certificate issuance and administration functions for VA. In December 2014, VA contacted VzB to ascertain if its proprietary data was for sale. VzB advised that this data is not for sale. All PKI certificates previously issued by VzB to VA employees and contractors can only be revoked and recovered using VzB's current certificate authority. VzB is the sole provider capable of operating the current proprietary certificate authority that maintains and controls all VA PKI issued by VzB. No other source other than VzB can host the complete PKI currently used to issue, recover or revoke certificates. VzB is the only source capable of operating the current PKI and publishing the verification information for credentials to recover or revoke certificate key pairs from the current system.

The current VzB delivery order ends on April 9, 2015 and a break in service would immediately invalidate VA secure email PKI certificates provisioned on personal identification verification (PIV) cards issued to employees and contractors eliminating ability to access critical VA systems and severely disrupting delivery of healthcare and benefits to Veterans. VA is currently in the process of transitioning from PKI services provided by VzB to services provided by the Department of Treasury (Treasury). The transition of PKI services is a complex task requiring coordination between VA, VzB, and Treasury; nonetheless, VA previously anticipated these tasks would be completed before the current order expires. However, the migration of the PKI services to Treasury continues to be delayed by unforeseen technical issues. Specifically, during a migration of VA's PIV card management system, it was discovered that the Treasury's Entrust software product did not function as expected with regards to maintaining user key history. User key history permits PIV card holders to access their old encrypted email. Treasury's Entrust configuration tool is currently unable to retrieve VA key history from VzB. As a result, it was determined that VA needs to modify the Entrust software to allow it to transfer key pairs, which will not be completed before the end of the current VzB delivery order. After the Entrust software is modified, additional testing is needed to verify that the software is able to retrieve the VA key history. The modification of the Entrust software is expected to begin in October 2015. Accordingly, this proposed action provides the nine month base period and 12 month option to continue the current services provided by VzB and provides time to complete the

modifications to the Entrust software, perform testing, and reassess VA's ability to complete the PKI SSP Services transfer to Treasury.

6. Efforts to Obtain Competition: Market research was conducted, details of which are in the market research section of this document. This effort did not yield any additional sources that can meet the Government's requirements. There is no competition anticipated for this acquisition. In accordance with FAR Subsection 8.405-6(a)(2) and FAR Section 5.301 a copy of this Limited-Sources Justification will be posted along with a synopsis of the award to the Federal Business Opportunities website within 14 days of award.

7. Actions to Increase Competition: VA does not anticipate any future need for continuation of VzB PKI issuance support once the transition to Treasury is complete and expect future procurements will be done on a competitive basis. VA has completed the transitioning of the existing contractor-hosted and maintained Card Management System (CMS) from VzB's data centers to a VA-hosted and maintained system located in VA data centers. Additionally, VA currently has multiple PKI contracts that are administered by the application owners which they support. On August 30, 2013, VA established an Interagency Agreement (IA) with Treasury for enterprise-wide PKI certification as current PKI contracts do not meet VA's overarching needs. VA's technical transition to being fully supported by Treasury is currently incomplete, thus driving the need for continuation of VzB PKI certificate issuance, recovery and revocation services. Once the technical transition is complete there should not be a need for future follow-on PKI certificate issuance contracts.

8. Market Research: Market Research was conducted in December 2014 and January 2015 by OI&T SDE ESE representatives that queried GSA FSS 70 product catalogs and National Aeronautics and Space Administration Solutions for Enterprise-Wide Procurement IV Governmentwide Acquisition Contracts for companies to fulfill VA's PKI needs. While multiple companies are certified to issue new PKI certificates under existing guidelines, none have the capability to operate the current infrastructure supporting VA. VzB is the only source capable of operating the current infrastructure, publishing the certificate verification information for credentials, and conducting maintenance of all previously issued certificates, since VzB retains the proprietary rights to PKI certificates issued. No other vendor has the capability of recovering PKI encryption certificates and keys issued by VzB. Therefore, a new delivery order with VzB is required to maintain ability to issue, revocate, and recover PKI encryption certificates and keys.

9. Other Facts: VA requires the ability to issue, revocate, and recover PKI encryption keys in order to maintain access to key material that allows for the decryption of email. This process is required by the policies under which the certificates were issued, and supports users' access to legacy data. There are also numerous legal and law enforcement initiatives that require VA to maintain

access to the escrowed key material for seven to ten years. A break in service would render VA unable to issue and recover previously issued encrypted certificates and would not meet the PKI requirements.