

## **Questions and Answers**

### **Question #49: Per RFP section 5.3 #5:**

*“Tool shall be capable of working in Personal Identity Verification (PIV) and non-PIV credentialed environments. For testing, the tool shall be capable of performing in a two factor authentication environment. NOTE: VA applications have multiple types of authentication ranging from no authentication on public facing web sites (internet), no authentication on websites or applications behind the firewall that are not publicly available (intranet), websites or applications that require a username/password to access, and websites or applications that require a VA-issued PIV card to access. The automated tool needs to function in each of these environments.”*

### **Our Question:**

Our application user interface supports both PIV and non-PIV credentialed environments. For automated crawling through PIV-protected web content, our application's server leverages a soft token that resides in the secure server's certificate store. Will the VA be able to provide this soft token for secure, automated batch administrative processing of protected web content?

### **Supporting Notes:**

Our application use of a soft token for automated batch crawling through protected web content is the most secure means to automate the scanning of large web properties from a multi user solution that reside within PIV credentialed environments without human involvement. Our Application will be installed on secured servers that are wholly owned and managed by the VA and accessed only by individuals with appropriate PIV two factor credentials. The soft token stored in the server's certificate store is also wholly managed by the VA, providing the server's batch administrative process controlled access to protected web content so that it can more rapidly be scanned for accessibility compliance standards with Our Application. Our Application does not - at any time – store a copy of the elevated credential or any authentication mechanism used to perform the work.

**Answer:** The way that certificates are managed by VA currently, the automated batch processing of PIV-enabled applications is not permitted; planning is underway for a solution for this need and hopefully will be completed soon. Meanwhile, the 508 Office has a workaround. A temporary exemption allows an assessment to be done with a combination of scripting (if desired by the test team) and tester authentication using a username and password. The contractor will not be held responsible for technical capabilities that are not yet available in the VA environment.

**Question #53:** IAW FAR 15.403-3(a.1.i) How does the government intend to determine fair and reasonableness on pricing when pricing for a TRM approved commercial product is not being provided?

By bundling the service and the software/maintenance and the unwillingness of existing software commercial vendors to provide equal cost estimate, the government has hindered the contractor community and gives an advantage to the approved vendors. It is under the pretense that VA is favoring a single vendor and using the process of solicitation to obtain a sole source solution.

**Answer:** Competition will help determine the price is fair and reasonable.

This solicitation has been issued in an effort to find the best tool and allow services to proceed using it. The current solicitation is not sole source because the VA believes the competition will result in the best solution.

If a product has not been approved at time of contract award, submission for approval by the TRM group can be completed within 1 week of beginning of the contract's period of performance.

**Question #54:** Reference PWS Section 5.3 #5, “Tool shall be capable of working in Personal Identity Verification (PIV) and non-PIV credentialed environments. For testing, the tool shall be capable of performing in a two factor authentication environment. NOTE: VA applications have multiple types of authentication ranging from no authentication on public facing web sites (internet), no authentication on websites or applications behind the firewall that are not publicly available (intranet), websites or applications that require a username/password to access, and websites or applications that require a VA-issued PIV card to access. The automated tool needs to function in each of these environments.”

The user interface of our proposed tool supports both PIV and non-PIV credentialed environments. For automated crawling through PIV-protected web content, our server leverages a soft token that resides in the secure server’s certificate store. Will VA be able to provide this soft token for secure, automated batch administrative processing of protected web content?

**Answer:** The way that certificates are managed by VA currently, the automated batch processing of PIV-enabled applications is not permitted; planning is underway for a solution for this need and hopefully will be completed soon. Meanwhile, the 508 Office has a workaround. A temporary exemption allows an assessment to be done with a combination of scripting (if desired by the test team) and tester authentication using a username and password. The contractor will not be held responsible for technical capabilities that are not yet available in the VA environment.

**Question #55:** Reference PWS Section 5.3 #9, “Tool and plug-ins/browser extensions shall be VA Technical Reference Model (TRM) approved. If the products are not approved at time of contract award, submission for approval by the TRM group must be completed within 1 week of beginning of the contract’s PoP.”

Please provide the TRM approval criteria.

**Answer:** If the products are not TRM-approved at time of contract award, within 1 week of award the contractor must submit the tool and plug-ins/browser extensions to be approved by the TRM. The specific TRM criteria vary depending on the technology being assessed, and the Section 508 Office will assist as needed during the TRM process.