

**Justification and Approval**  
For  
Other Than Full and Open Competition

1. Contracting Agency: Defense Human Resource Activity- Procurement Support Office  
4040 N. Fairfax Dr., Suite 120, Arlington, VA 22203.

2. Authority Cited: 41 U.S.C. 251, *et seq.* and Title 40 U.S.C. 501, FAR 8.405-6 –  
Limited Sources – Brand Name, Multiple Award Schedule Program.

3. Description of Supplies and Services: The Defense Manpower Data Center (DMDC) requires a SafeNet ProtectServer External (PSE) Hardware Security Module (HSM) device and associated training to support one of DMDC's most critical missions, the Common Access Card (CAC) program. The HSM device is needed to secure audit events and cryptographic keys in the CAC infrastructure. The major product criteria that the vendor must meet are as follows:

- Keys must be stored within the HSM, not anywhere in a server file system.
- The device must support certain NIST cryptographic standards
- The device must be network connected
- The devices must be FIPS 140-2 certified to Level 3 or above.

Additionally, HSM training is needed to train the CAC group on how to configure, maintain and troubleshoot these HSM devices.

4. Description of Action: A Firm Fixed Price contract is planned for approximately [REDACTED]. The period of performance will include a 12-month base period and three (3) 12-month option periods. FY11 Operating and Maintenance (O&M) funds are available for the base period in the estimated amount of [REDACTED].

5. Reason for Authority Cited: ActivIdentity (AI) supplies all of the software DMDC uses to track the CAC cardstock lifecycle and inject the data onto the CAC at issuance time. The CAC program requires HSM devices to implement the latest version of AI's Key Lifecycle Management System (KLMS). The KLMS will only support the SafeNet PSE as the primary HSM device. In addition, SafeNet's HSM is the only brand that stores cryptography keys in the HSM, as opposed to other brands that store the cryptography keys on the server file system which is less secure. Lastly, the SafeNet HSM product is the only one that meets the Federal Information Processing Standard (FIPS) Publication 140-2 (FIPS PUB 140-2) compliance requirements used to accredit cryptographic modules. Therefore, no other brand or service will satisfy the Government's requirement.

6. Effort to Obtain Competition: Market research was conducted and the only product compliant with AI's KLMS was the SafeNet PSE HSM. DMDC found that purchasing any other product would be a significant cost DMDC in terms of productivity, budget,

and retraining customers. The requirement will be posted on GSA e-buy as a Brand Name requirement.

7. Effort to remove barriers to/increase competition: The program office will continue to conduct market research after award to explore other brand capabilities and product/service solutions that could meet DMDC's requirement.

8. Market Research: Market research was conducted through simple internet searches, known leaders in the cryptographic industry, and within GSA schedules.

See Market Research Report.

#### 9. Interested Sources

SafeNet  
4690 Millennium Drive  
Belcamp, MD 21017  
410-931-7500  
GS-35F-737M

Thales Communications, Inc. (formerly  
nCipher)  
22605 Gateway Center Drive  
Clarksburg, Maryland 20871  
(240) 864-7000  
GS-35F-0001L

10. Other Factors: N/A