Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Docket No. [171205999-7999-01]

National Cybersecurity Center of Excellence (NCCoE) Privileged Account Management for the Financial Services Sector

AGENCY: National Institute of Standards and Technology, Department of Commerce.

ACTION: Notice.

SUMMARY: The National Institute of Standards and Technology (NIST) invites organizations to provide products and technical expertise to support and demonstrate security platforms for the Privileged Account Management for the Financial Services sector. This notice is the initial step for the National Cybersecurity Center of Excellence (NCCoE) in collaborating with technology companies to address cybersecurity challenges identified under the Financial Services sector program. Participation in the use case is open to all interested organizations.

DATES: Interested parties must contact NIST to request a letter of interest template to be completed and submitted to NIST. Letters of interest will be accepted on a first come, first served basis. Collaborative activities will commence as soon as enough completed and signed letters of interest have been returned to address all the necessary components and capabilities, but no earlier than [PLEASE INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. When the use case has been completed, NIST will post a notice on the NCCoE Financial Services sector program website at https://nccoe.nist.gov/projects/use-cases/privileged-account-management announcing the completion of the use case and informing the public that it will no longer accept letters of interest for this use case.

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to Financial_NCCoE@nist.gov or via hardcopy to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Organizations whose letters of interest are accepted in accordance with the process set forth in the SUPPLEMENTARY INFORMATION section of this notice will be asked to sign a consortium Cooperative Research and Development Agreement (CRADA) with NIST. An NCCoE consortium CRADA template can be found at: http://nccoe.nist.gov/node/138.

FOR FURTHER INFORMATION CONTACT: James Banoczi via email to Financial_NCCoE@nist.gov; by telephone 301-975-0200; or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD

20850. Additional details about the Financial Services sector program are available at https://nccoe.nist.gov/projects/use-cases/privileged-account-management.

SUPPLEMENTARY INFORMATION:

Background: The NCCoE, part of NIST, is a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. The NCCoE brings together experts from industry, government, and academia under one roof to develop practical, interoperable cybersecurity approaches that address the real-world needs of complex Information Technology (IT) systems. By accelerating dissemination and use of these integrated tools and technologies for protecting IT assets, the NCCoE will enhance trust in U.S. IT communications, data, and storage systems; reduce risk for companies and individuals using IT systems; and encourage development of innovative, job-creating cybersecurity products and services.

Process: NIST is soliciting responses from all sources of relevant security capabilities (see below) to enter into a Cooperative Research and Development Agreement (CRADA) to provide products and technical expertise to support and demonstrate security platforms for the Privileged Account Management for the Financial Services Sector. The full use case can be viewed at: https://nccoe.nist.gov/projects/use-cases/privileged-account-management.

Interested parties should contact NIST using the information provided in the FOR FURTHER INFORMATION CONTACT section of this notice. NIST will then provide each interested party with a letter of interest template, which the party must complete,

certify that it is accurate, and submit to NIST. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the use case objective or requirements identified below. NIST will select participants who have submitted complete letters of interest on a first come, first served basis within each category of product components or capabilities listed below up to the number of participants in each category necessary to carry out this use case. However, there may be continuing opportunity to participate even after initial activity commences. Selected participants will be required to enter into a consortium CRADA with NIST (for reference, see ADDRESSES section above). NIST published a notice in the Federal Register on October 19, 2012 (77 FR 64314) inviting U.S. companies to enter into National Cybersecurity Excellence Partnerships (NCEPs) in furtherance of the NCCoE. For this demonstration project, NCEP partners will not be given priority for participation.

Use Case Objective: Privileged Account Management (PAM) is a domain within Identity and Access Management (IdAM) that focuses on monitoring and controlling the use of privileged accounts. Privileged accounts are the IT system accounts that include local and domain administrative accounts, emergency accounts, application management, and service accounts. These powerful accounts provide elevated, often nonrestricted access to the underlying IT resources and technology, which is why attackers or malicious insiders seek to gain access to them. Hence, it is critical to monitor, audit, control, and manage privileged account usage. Many organizations, including financial sector companies, face challenges managing privileged accounts. To address these challenges, the National Cybersecurity Center of Excellence (NCCoE) plans to

demonstrate a PAM capability that effectively protects, monitors, and manages privileged account access. The project addresses privileged account life cycle management, authentication, authorization, auditing, and access controls.

A detailed description of the Privileged Account Management is available at: https://nccoe.nist.gov/projects/use-cases/privileged-account-management.

Requirements: Each responding organization's letter of interest should identify which security platform component(s) or capability(ies) it is offering. Letters of interest should not include company proprietary information, and all components and capabilities must be commercially available. Components are listed in section 3 of the Privileged Account Management for the Financial Services sector use case (for reference, please see the link in the PROCESS section above) and include, but are not limited to:

- Privileged account control
- Privileged account command filtering (allow or deny specific comments, such as disk formatting)
- Multifactor authentication capability
- Access logging/database system
- Password management
- Separation of duties management
- Support least privileged policies

- Password obfuscation (hiding passwords from PAM users)
- Temporary accounts
- Log management (analytics, storage, alerting)

Each responding organization's letter of interest should identify how their products address one or more of the following desired solution characteristics in section 3 of the Privileged Account Management for the Financial Services sector use case (for reference, please see the link in the PROCESS section above):

1. Is easy to use for both PAM system administrators and PAM system users.
2. Provides protection for data at rest and data in transit.
3. Is complementary to existing access management.
4. Integrates with directories.
5. Provides account use control (policy enforcement and decision making).
6. Provides system command control.
7. Counters password obfuscation (hidden passwords).
8. Supports password management (vaults, changes, storage).
9. Supports activity logging (textual and video).
10. Supports real time activity monitoring.
11. Includes support functions needed by the typical user.
12. Supports privilege escalation management.
13. Supports forensic investigation data management.
14. Provides support for workflow management.
15. Enables emergency (break glass) scenario support.

16. Includes policy management support.
17. Supports single sign-on.
18. Permits system and privileged account discovery.

Responding organizations need to understand and, in their letters of interest, commit to provide:

1. Access for all participants' project teams to component interfaces and the organization's experts necessary to make functional connections among security platform components
2. Support for development and demonstration of the Privileged Account Management for the Financial Services sector use case in NCCoE facilities which will be conducted in a manner consistent with the following standards and guidance: FIPS 140-2, FIPS 199, FIPS 200, FIPS 201, SP 800-53, and SP 800-63.

Additional details about the Privileged Account Management for the Financial Services sector use case are available at: https://nccoe.nist.gov/projects/use-cases/privileged-account-management.

NIST cannot guarantee that all of the products proposed by respondents will be used in the demonstration. Each prospective participant will be expected to work collaboratively with NIST staff and other project participants under the terms of the consortium CRADA in the development of the Privileged Account Management for the Financial Services sector capability. Prospective participants' contribution to the collaborative effort will include assistance in establishing the necessary interface functionality, connection and set-up capabilities and procedures, demonstration harnesses, environmental and safety

conditions for use, integrated platform user instructions, and demonstration plans and scripts necessary to demonstrate the desired capabilities. Each participant will train NIST personnel, as necessary, to operate its product in capability demonstrations to the Financial Services community. Following successful demonstrations, NIST will publish a description of the security platform and its performance characteristics sufficient to permit other organizations to develop and deploy security platforms that meet the security objectives of the Privileged Account Management for the Financial Services sector use case. These descriptions will be public information.

Under the terms of the consortium CRADA, NIST will support development of interfaces among participants' products by providing IT infrastructure, laboratory facilities, office facilities, collaboration facilities, and staff support to component composition, security platform documentation, and demonstration activities.

The dates of the demonstration of the Privileged Account Management for the Financial Services sector capability will be announced on the NCCoE Web site at least two weeks in advance at http://nccoe.nist.gov/. The expected outcome of the demonstration is to improve privileged account management across an entire Financial Services sector enterprise. Participating organizations will gain from the knowledge that their products are interoperable with other participants' offerings.

For additional information on the NCCoE governance, business processes, and NCCoE operational structure, visit the NCCoE Web site http://nccoe.nist.gov/.

Kevin Kimball,

NIST Chief of Staff.

[FR Doc. 2017-27869 Filed: 12/26/2017 8:45 am; Publication Date: 12/27/2017]