Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 180319295-8295-01]

National Cybersecurity Center of Excellence (NCCoE) Securing Picture Archiving and Communication System (PACS) Cybersecurity for the Healthcare 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 Securing Picture Archiving and Communication System (PACS) Cybersecurity for the healthcare 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 healthcare sector program. Participation in the use case is open to all interested organizations.

DATES: 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 [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to HIT_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: Andrea Arbelaez via email to HIT_NCCOE@nist.gov; by telephone 301-975-0214; or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the healthcare sector program are available at https://nccoe.nist.gov/projects/use-cases/health-it/pacs.

SUPPLEMENTARY INFORMATION: 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. When the use case has been completed,

NIST will post a notice on the NCCoE healthcare sector program website at https://nccoe.nist.gov/projects/use-cases/health-it/pacs announcing the completion of the use case and informing the public that it will no longer accept letters of interest for this use case.

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 Securing Picture Archiving and Communication System (PACS) Cybersecurity for the healthcare sector. The full use case can be viewed at: https://nccoe.nist.gov/projects/use-cases/health-it/pacs.

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:

To provide guidance and a referenceable architecture for securing the Picture Archiving and Communication System (PACS) ecosystem in Healthcare Delivery Organizations (HDOs), and to include an example solution using existing, commercially and open-source available cybersecurity products.

A detailed description of the Securing Picture Archiving and Communication System (PACS) Cybersecurity for the healthcare sector is available at: https://nccoe.nist.gov/projects/use-cases/health-it/pacs.

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 2 of the Securing Picture Archiving and Communication System (PACS) Cybersecurity for the healthcare sector use case (for reference, please see the link in the PROCESS section above) and include, but are not limited to:

- PACS Servers, special applications (including web services), and workstations
- Vendor Neutral Archive (VNA)
- data storage
- modality or modality simulator
- radiology information system (RIS) or RIS simulator
- notification system
- Electronic Health Record (EHR) / Electronic Medical Record (EMR)
- load balancer
- managed service model and remote service connectivity

- certificate management
- authentication mechanism
- session management
- data encryption
- endpoint protection
    - encryption
    - malware/virus protection
    - Host Intrusion Prevention System (HIPS)/Host Intrusion Detection System (HIDS)
- logging, monitoring, security information and event management (SIEM)
- network infrastructure controls
- asset management
- web services

Each responding organization's letter of interest should identify how their products address one or more of the following desired security characteristics in section 2 of the Securing Picture Archiving and Communication System (PACS) Cybersecurity for the healthcare sector use case (for reference, please see the link in the PROCESS section above):

The primary security functions and processes to be implemented for this project are listed below and are based on the NIST Cybersecurity Framework (CSF).

IDENTIFY (ID):

- Asset Management – includes identification of assets on network and management of the assets to be deployed to workstations
- Risk Assessment – includes risk management strategy

PROTECT (PR)

- Access Control – includes user account management, remote access
    - controlling (and auditing) user accounts
    - controlling (and auditing) access by external users
    - enforcing least privilege for all (internal and external) users
    - enforcing separation of duties policies
        - Privileged Access Management (PAM) with an emphasis on the segregation of duties
    - enforcing least functionality
- User Identification and Authentication
    - multifactor authentication for the system that aligns with the sensitive information and function that PACS performs; NIST-recommended algorithms; usability; impact on system performance; and raising the assurance profile, and higher NIST Special Publication (SP) 800-63-3 levels, bring a higher level of assurance
    - viable federated identity management

- credential management

- Data Security – includes data confidentiality, integrity, and availability
  - securing and monitoring storage of data – includes data encryption (for data at rest)
    - access control on data
    - data-at-rest controls should implement some form of a data security manager that would allow for policy application to encrypted data, inclusive of access control policy
  - securing the distribution of data—includes data encryption (for data in transit) and data loss prevention mechanism
  - controls that promote data integrity
  - cryptographic modules validated as meeting NIST Federal Information Processing Standard (FIPS) 140-2 are preferred
  - physical security provided by an access controlled data center to host the PACS servers and storage
- Information Protection Processes and Procedures – includes data backup, endpoint protection for workstations
- Maintenance – local and remote maintenance
- Protective Technology – host-based intrusion prevention, solutions for malware (malicious code detection), audit logging, (automated) audit log review, and physical protection

- Communications and Network Security – communications and control networks are protected (e.g., firewall, network access control, network infrastructure controls)
    - Securing and monitoring connections with the Health Delivery Organization (HDO) ecosystem
        - Network segmentation
    - Securing and monitoring connections to and from external systems

DETECT (DE)

- Anomalies and Events – analysis of detected events (from logs, monitoring results, SIEM)
    - Centralized mechanism to capture and analyze system and network events
- Security Continuous Monitoring – monitoring for unauthorized personnel, devices, software, connections
    - vulnerability management – includes vulnerability scanning and remediation
    - patch management
    - system configuration security settings
    - user account usage (local and remote) and user behavioral analytics

RESPOND (RS)

- Response Planning – response plan executed after an event, mitigation of security issues

RECOVER (RC)

- Recovery and Restoration – recovery and restoration activities executed after an event
    - business continuity and business resumption processes
        - In addition to restoration capability from archival media, the project should consider high availability and continuity for data storage. Implicitly, disk arrays used for image storage should have the capability to implement various Redundant Array of Independent Disks (RAID) configurations. RAID 0, 1, 5, 6, and 1+0 should be supported. Disk arrays should also be made available for cold or warm restore/failover capability. Other data storage solutions that provide the same (or better) reliability and durability are considered.

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 Securing Picture Archiving and Communication System (PACS) Cybersecurity for the healthcare sector use case in NCCoE facilities which will be conducted in a manner consistent with the following standards and guidance: FIPS 200, FIPS 201, SP 800-53 and FIPS 140-2, SP 800-30, SP 800-37, SP 800-39, SP 800-41, SP 800-52, SP 800-57, SP 800-63-3, SP 800-66, SP 800-77, SP 800-95, SP 800-144, SP 800-146, SP 800-171,

SP 800-181, ISO 12052:2011 Health Informatics – Digital Imaging and Communication in Medicine (DICOM) including Workflow and Data Management, AAMI TIR57, ANSI/AAMI/IEC 80001-1:2010, IEC Technical Report 80001-2-1, IEC Technical Report 80001-2-2, Internet Engineering Task Force Request for Comments 4301, Food & Drug Administration (FDA) Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, FDA Postmark Management of Cybersecurity in Medical Devices, FDA Guidance for Industry – Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software, FDA Guidance for Submission of Premarket Notifications for Medical Image Management Devices, FDA Medical Device Data Systems, Medical Image Storage Devices, Medical Image Communications Device, Department of Health & Human Services Office for Civil Rights Health Insurance Portability and Accountability Act Security Rule Crosswalk to NIST Cybersecurity Framework, Department of Homeland Security Attack Surface: Healthcare and Public Sector, Integrating the Healthcare Enterprise Radiology Technical Framework.

Additional details about the Securing Picture Archiving and Communication System (PACS) Cybersecurity for the healthcare sector use case are available at: https://nccoe.nist.gov/projects/use-cases/health-it/pacs.

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 Securing Picture Archiving and Communication System

(PACS) Cybersecurity for the healthcare 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 healthcare 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 Securing Picture Archiving and Communication System (PACS) Cybersecurity for the healthcare 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 Securing Picture Archiving and Communication System (PACS) Cybersecurity for the healthcare 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 securing picture archiving and communications system (PACS) cybersecurity across an entire healthcare 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 A. Kimball,
Chief of Staff.

[FR Doc. 2018-09897 Filed: 5/8/2018 8:45 am; Publication Date: 5/9/2018]