Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 120823388-2388-01]

National Cybersecurity Center of Excellence (NCCoE) Secure Exchange of Electronic Health Information Demonstration Project.

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 exchange of electronic health care information by healthcare providers. This notice is the initial step for the National Cybersecurity Center of Excellence (NCCoE) in the Secure Exchange of Electronic Health Information project. Participation in the project is open to all interested organizations.

DATES: Interested parties must contact NIST to request a certification letter. Completed and signed certification letters must be received by NIST by 5:00 PM Eastern time on [PLEASE INSERT DATE 45 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER.].

ADDRESSES: The NCCoE is located at 9600 Gudelsky Drive Rockville, MD 20850. Certification letters must be submitted to Karen Waltermire via email at NCCoE@nist.gov; or via hardcopy to NCCoE, National Institute of Standards and Technology; 100 Bureau Drive; MS 2000 Gaithersburg, MD 20899.

FOR FURTHER INFORMATION CONTACT: Karen Waltermire via email at NCCoE@nist.gov; or telephone 301-975-4500; NCCoE, National Institute of Standards and Technology; 100 Bureau Drive; MS 2000; Gaithersburg, MD 20899. Additional details about the Secure Exchange of Electronic Health Information project will be available at: http://nccoe.nist.gov/hit.

SUPPLEMENTARY INFORMATION:

Background: The NCCoE, hosted by NIST, is a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. The NCCoE will bring 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; lower risk for companies and individuals in the use of IT systems; and encourage development of innovative, job-creating cybersecurity products and services. The project is not restricted to organizations required to comply with the standards and implementation specifications promulgated under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 or to organizations using EHR technology that complies with the standards, implementation specifications, and certification criteria promulgated under the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. NIST expects that participation in the project will help participating organizations gain knowledge that will help them comply with these requirements.

Process: NIST is soliciting responses from all sources of relevant security capabilities (e.g., vendors, academia, and integrators). Interested parties should contact NIST using the information provided in the FOR FURTHER INFORMATION CONTACT section of this notice. Each interested party will be provided with a certification letter, which the party must complete and submit to NIST by the date provided in the DATES section of this notice. The certification letter must be completed and submitted to NIST by the responding organization. NIST will contact interested parties if there are questions regarding the responsiveness of the certification letters to the project objective or project requirements identified below. NIST will select participants who have submitted complete certification letters 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 project. Selected participants will be required to enter into a consortium Cooperative Research and Development Agreement (CRADA) with NIST. 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.

Project Objective: Healthcare providers increasingly need to securely exchange electronic health information with each other. The confidentiality, integrity, and availability of this information must be protected. Secure exchange of electronic health information is often particularly challenging for small healthcare providers, who may lack the security infrastructure or expertise that larger healthcare providers possess. Other challenges with secure electronic health information exchange include the variety of client devices (desktops, laptops, and mobile devices) and the range of healthcare data exchange standards.

Major security concerns for secure electronic health information exchange include, but are not limited to, the following categories:

- Lack of physical security controls (e.g., increased risk of loss or theft for mobile devices, public proximity to client devices)
- Use of untrusted client devices (lack of security features or circumvention of those features)
- Use of untrusted networks (e.g., broadband, WiFi, WiMAX, cellular networks)
- Interaction with other systems in terms of data synchronization and storage

Although a number of components are available to address some of these concerns in some healthcare environments, security platforms that are composed of available capabilities in a secure, usable, and affordable manner to provide comprehensive solutions are needed for the very large number of small healthcare providers. The goal for this project is to provide a security platform to enable small healthcare providers to exchange electronic health information in support of the U.S. federal government and the health IT community.

Requirements: Each organization must complete and execute the certification letter and certify that it is accurate and complete.

Each organization will be asked to identify which security platform components or capabilities it is offering. Product components or capabilities include one or more of the following:

1. Electronic health information entry and display devices,
2. Authentication and authorization mechanisms,
3. Data transfer/communications components,
4. Electronic health information storage and retrieval components,
5. Forms generation capabilities, and
6. Printer devices or interfaces.

Specific requirements of the Secure Exchange of Electronic Health Information demonstration project are as follows:

1. Compatibility with various electronic health record (EHR) systems in use by small healthcare providers;
2. Use of, or compatibility with, healthcare data exchange standards and implementation specifications (e.g., HL7, DICOM, IHE), including the transport standards adopted by the Department of Health and Human Services at 45 CFR 170.202;
3. Access by project staff to component interfaces and the organization's experts necessary to make functional connections among security platform components;
4. Enterprise security policy enforcement on the client devices through a hardware root of trust, such as implementing secure configuration baselines for operating systems and applications; automatically continuously monitoring, detecting, and reporting policy violations; and performing system health checks;
5. Support for standardized security automation technologies (e.g., SCAP);
6. Strong encryption of data communications and local storage;
7. User authentication, including support of directory services, multi-factor authentication, and key management;
8. Use of secure infrastructure components (e.g., DNSSEC, IPv4, and IPv6);
9. Development and demonstration of use cases in NCCoE facilities; and
10. Development and demonstration activities will be conducted in a manner consistent with Federal requirements (e.g., FIPS 200, FIPS 201, SP 800-53, and SP 800-63.

Additional details about the Secure Exchange of Electronic Health Information Use Case project will be available for organizations to look at specifics that are relevant to capability and component identification, at: http://nccoe.nist.gov/hit.

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 Secure Exchange of Electronic Health Information 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 prospective 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 Secure Exchange of Electronic Health Information Demonstration project. These descriptions will be public information.

Under the terms of the consortium CRADA, NIST will support development of interfaces among participants' products, including 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 Secure Exchange of Electronic Health Information capability to the healthcare community will be announced on the NCCoE website at least two weeks in advance at: http://csrc.nist.gov/nccoe. The expected outcome of the demonstration is to enable healthcare providers to exchange electronic health information. 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 website http://csrc.nist.gov/nccoe.

Dated: January 10, 2013

Willie E. May
Associate Director for Laboratory Programs

[FR Doc. 2013-00724 Filed 01/14/2013 at 8:45 am; Publication Date: 01/15/2013]