Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 150917865-5865-01]

National Cybersecurity Center of Excellence (NCCoE) Domain Name System-Based Security (DNS) for Electronic Mail Building Block

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 Domain Name System-Based (DNS) Security for Electronic Mail Building Block. 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 Domain Name System-Based Security for

Electronic Mail Building Block. Participation in this building block 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 that identifies the organization requesting participation in the Domain Name System-Based Security for Electronic Mail Building Block and the capabilities and components that are being offered to the collaborative effort. 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 building block has been completed, NIST will post a notice on the Domain Name System-Based Security for Electronic Mail Building Block website at http://nccoe.nist.gov/DNSSecuredEmail announcing the completion of the building block and informing the public that it will no longer accept letters of interest for this building block.

ADDRESSES: The NCCoE is located at 9600 Gudelsky Drive, Rockville, MD 20850. Letters of interest must be submitted to dns-email-nccoe@nist.gov or via hardcopy to National Institute of Standards and Technology, NCCoE; 9600 Gudelsky Drive; 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 Cooperative Research and Development Agreement

(CRADA) with NIST. A CRADA template can be found at: http://nccoe.nist.gov/node/138.

FOR FURTHER INFORMATION CONTACT: William C. Barker via email to dns-email-nccoe@nist.gov; by telephone 301-975-3655; or by mail to National Institute of Standards and Technology, NCCoE; 9600 Gudelsky Drive; Rockville, MD 20850. Additional details about the Domain Name System-Based Security for Electronic Mail Building Block are available at http://nccoe.nist.gov/DNSSecuredEmail.

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 Domain Name System-Based Security for Electronic Mail Building Block. The full building block description can be viewed at: http://nccoe.nist.gov/DNSSecuredEmail.

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 and which identifies the organization requesting participation in the Domain Name System-Based Security for Electronic Mail Building Block and the capabilities and components that are being offered to the collaborative effort. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the building block objective or requirements identified below and to obtain additional information. 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 the Domain Name System-Based Security for Electronic Mail Building Block. 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.

Building Block Objective:

Both public and private sector business operations are heavily reliant on electronic mail (e-mail) exchanges. The need to protect business plans and tactics, the integrity of transactions, financial and other proprietary information, and privacy of employees and clients are only four of the factors that motivate organizations to secure their e-mail exchanges. Whether the security service desired is authentication of the source of an e-mail message, assurance that the message has not been altered by an unauthorized party, or confidentiality of message contents, cryptographic functions are usually employed in providing the service. Economies of scale and a need for uniform security implementation drive most enterprises to rely on mail servers to provide security to the members of an enterprise rather than end-to-end security mechanisms operated by individual users. Most current server-based e-mail security mechanisms are vulnerable to, and have been defeated by, attacks on the integrity of the cryptographic implementations on which they depend. The consequences frequently involve unauthorized parties being able to read or modify supposedly secure information, or to use e-mail as a vector for inserting malware into the system that is intended to deny access to critical information or processes or to damage or destroy system components and/or information. Improved e-mail security can help protect organizations and individuals against these consequences and also serve as a marketing discriminator for e-mail service providers as well as improve the trustworthiness of enterprise e-mail exchanges.

Domain Name System Security Extensions (DNSSEC) for the Domain Name System (DNS) are technical mechanisms employed by internet service providers to protect

against unauthorized modification to network management information and connections to devices operated by untrustworthy parties. DNS-based Authentication of Named Entities (DANE) is a protocol that securely associates domain names with cryptographic certificates and related security information so that they can't be fraudulently modified or replaced to breach the security of Internet exchanges. In spite of the dangers of failure to authenticate the identities of network devices, adoption of DNSSEC has been slow. Demonstration of DANE-supported applications such as reliably secure e-mail may support increased user demand for domain name system security. Follow-on projects might include HTTPS, IOT, IPSEC keys in DNS, and DNS service discovery.

The current project will demonstrate a proof of concept security platform composed of off the shelf components that provides trustworthy mail server-to-mail server e-mail exchanges across organizational boundaries. The DANE protocol will be used to authenticate servers and certificates in two roles in the DNS-Based Security for E-mail Project: 1) by binding the X.509 certificates used for Transport Layer Security (TLS) to DNS names verified by DNSSEC and supporting the use of these certificates in the mail server-to-mail server communication; and 2) by binding the X.509 certificates used for Secure Secure/Multipurpose Internet Mail Extensions (S/MIME) to email addresses encoded as DNS names verified by DNSSEC. These bindings support trust in the use of S/MIME certificates in the end-to-end email communication. The resulting building block will encrypt e-mail traffic between servers, allow individual email users to digitally sign and/or encrypt email messages to other end users, and allow individual email users to obtain other users' certificates in order to validate signed email or send encrypted email. The project will include an e-mail sending policy consistent with a stated privacy

policy that can be parsed by receiving servers so that receiving servers can apply the correct security checks and report back the correctness of the e-mail stream.

Documentation of the resulting platform will include statements of the security and privacy policies and standards (e.g., Executive Orders, NIST standards and guidelines, IETF RFCs) supported, technical specifications for hardware and software, implementation requirements, and a mapping of implementation requirements to the applicable policies, standards, and best practices.

The secure e-mail project will involve composition of a variety of components that will be provided by a number of different vendors. Client systems, DNS/DNSSEC services, mail transfer agents, and certificate providers (CAs) are generally involved.

Collaborators are being sought to provide components and expertise for DNS resolvers (stub and recursive) for DNSSEC, authoritative DNS servers for DNSSEC signed zones, mail servers and mail security components, extended validation and domain validation TLS certificates.

This project will result in one or more demonstration prototype DNS-based secure e-mail platforms, a publicly available NIST Cybersecurity Practice Guide that explains how to employ the platform(s) to meet security and privacy requirements, and platform documentation necessary to compose a DNS-based e-mail security platform from off the shelf components.

A detailed description of the Domain Name System-Based Security for Electronic Mail Building Block is available at: http://nccoe.nist.gov/DNSSecuredEmail.

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 eight of the Domain Name System-Based Security for Electronic Mail Building Block description (for reference, please see the link in the PROCESS section above) and include, but are not limited to:

- Client systems
- DNS/DNSSEC services
- Mail transfer agents
- DNS resolvers (stub and recursive) for DNSSEC validation
- Authoritative DNS servers for DNSSEC signed zones
- Mail server/mail security systems
- S/MIME certificates
- Extended validation and domain validation TLS certificates

Each responding organization's letter of interest should identify how their product(s) address one or more of the desired solution characteristics in section five of the Domain Name System-Based Security for Electronic Mail Building Block description (for reference, please see the link in the PROCESS section above).

Additional details about the Domain Name System-Based Security for Electronic Mail Building Block are available at: http://nccoe.nist.gov/DNSSecuredEmail.

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 Domain Name System-Based Security for Electronic Mail Building Block. 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. 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 Domain Name System-Based Security for Electronic Mail Building Block. These descriptions will be public information.

Under the terms of the consortium CRADA, participants will commit to providing:

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 Domain Name System-Based Security for Electronic Mail Building Block in NCCoE facilities which will be conducted in a manner consistent with Federal requirements (e.g., FIPS 200, FIPS 201, SP 800-53, and SP 800-63)

In addition, 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 Domain Name System-Based Security for Electronic Mail Building Block 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 domain name system-based security for electronic mail within the 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/.

Richard Cavanagh,
Acting Associate Director for Laboratory Programs.

[FR Doc. 2015-25304 Filed: 10/5/2015 08:45 am; Publication Date: 10/6/2015]