This document is scheduled to be published in the
Federal Register on 03/18/2014 and available online at
http://federalregister.gov/a/2014-05960, and on **FDsys.gov**

Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 140307213-4213-01]

National Cybersecurity Center of Excellence (NCCoE) and Electric Power Sector Identity and Access Management Use Case

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 identity and access management for the electric power 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 Energy 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. 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 9600 Gudelsky Drive, Rockville, MD 20850. Letters of interest must be submitted to Energy_NCCoE@nist.gov; or via hardcopy to National Institute of Standards and Technology, NCCoE; 9600 Gudelsky Drive; MS 2002; 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/The-Center/Get_Involved/NCCoE_Consortium_CRADA_Example.pdf.

FOR FURTHER INFORMATION CONTACT: Nate Lesser via email at Energy_NCCoE@nist.gov; or telephone 240-314-6823; National Institute of Standards and Technology, NCCoE; 9600 Gudelsky Drive; MS 2002; Rockville, MD 20850. Additional details about the NCCoE Energy Sector program are available at http://nccoe.nist.gov/energy.

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). Interested parties should contact NIST using the information provided in the **FOR FURTHER INFORMATION CONTACT** section of this notice. Upon receiving statements of interest, NIST will provide each interested party with a letter of interest, which the party must complete and submit to NIST by the date provided in the DATES section of this notice. The letter of interest must be completed and submitted to NCCoE by the responding organization. NCCoE 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. NCCoE 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 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.

Use Case Objective: In order to protect power generation, transmission and distribution, energy companies need to be able to control physical and logical access to their resources, including buildings, equipment, information technology and Industrial Control Systems (ICS). They must be able to authenticate the individuals and systems to which they are giving access rights with a high degree of certainty, whether they are employees, contractors, vendors, or partners. In addition, energy companies must be able to enforce access control policies (e.g. allow, deny, inquire further) consistently, uniformly and in a timely way across all of their resources.

Requirements: Each organization must complete and execute the letter of interest 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. Services for authenticating and authorizing users based on identity, role, third-party affiliation (e.g., federation) or other attributes (e.g., attribute-based access control)
2. Services for authenticating and authorizing devices
3. Services for whitelisting applications
4. Identity and access governance capability that translates human-readable access needs into machine-readable authorizations
5. Security incident and event management (SIEM) or log analysis software for monitoring access management events

6. ICS equipment, such as Remote Terminal Units (RTUs), programmable logic controllers (PLC), and relays, along with associated software and communications equipment (e.g., radios, encryptors)
7. Physical access control devices that use standard communication interfaces
8. “Bump-in-the-wire” devices for augmenting Operational Technology (OT) with authentication, authorization, access control, encrypted communication and logging capabilities

Capability requirements of the Identity and Access Management for Electric Utilities Use Case are as follows:

1. Compatibility with various electric utility ICS equipment and software
2. Strong authentication of users, devices, and software, based on credentials or attributes, along with appropriate encryption to enable reasonably secure exchange of identity and access management information
3. Compatibility with protocols and communication media commonly used by electric utilities
4. Federated authorization for communication across security domains
5. Ease of use (e.g., installation, configuration, maintenance, provisioning, de-provisioning, credentialing, revoking credentials)

Organizational requirements of the Identity and Access Management for Electric Utilities Use Case are as follows:

1. Access by project staff to component interfaces and the organization's experts necessary to make functional connections among security platform components
2. Development and demonstration of use cases in NCCoE facilities

3. 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 Identity and Access Management for Electric Utilities Use Case are available at http://nccoe.nist.gov/energy.

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 agreement in the development of the Identity and Access Management for Electric Utilities 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 Identity and Access Management for Electric Utilities Use Case. These descriptions will be public information.

Under the terms of the consortium agreement, 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 Identity and Access Management for Electric Utilities 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 identity and access management on electric utility OT systems. 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/.

Dated: March 12, 2014.

Mary H. Saunders,
Associate Director for Management Resources.

[FR Doc. 2014-05960 Filed 03/17/2014 at 8:45 am; Publication Date: 03/18/2014]