DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 210915-0187]

National Cybersecurity Center of Excellence (NCCoE) *Data Classification Practices: Facilitating Data-Centric Security Management*

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 letters of interest describing products and technical expertise to support and demonstrate security platforms for the *Data Classification Practices: Facilitating Data-Centric Security Management* project. 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 *Data Classification Practices: Facilitating Data-Centric Security Management* project. Participation in the project 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 data-nccoe@nist.gov or via hardcopy to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Interested parties can access the letter of interest template by visiting https://www.nccoe.nist.gov/projects/building-blocks/data-classification and completing the letter of interest webform. NIST will announce the completion of the selection of participants and inform the public that it is no longer accepting letters of interest for this project at https://www.nccoe.nist.gov/projects/building-blocks/data-classification. Organizations whose letters of interest are accepted will be asked to sign a consortium Cooperative Research and Development Agreement (CRADA) with NIST. An NCCoE consortium CRADA template can be found at: https://nccoe.nist.gov/library/nccoe-consortium-crada-example.

FOR FURTHER INFORMATION CONTACT: William Newhouse via telephone at 301--975-0232; by email to data-nccoe@nist.gov; or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the *Data Classification Practices: Facilitating Data-Centric Security Management* project are available at https://www.nccoe.nist.gov/projects/building-blocks/data-classification.

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 *Data Classification Practices: Facilitating Data-Centric Security Management* project. The full project can be viewed at: https://www.nccoe.nist.gov/projects/building-blocks/data-classification.

Interested parties can access the template for a letter of interest by visiting the project website at https://www.nccoe.nist.gov/projects/building-blocks/data-classification and completing the letter of interest webform. On completion of the webform, interested parties will receive access to the letter of interest template, which the party must complete, certify as accurate, and submit to NIST by email or hardcopy. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the project 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 project. When the project has been completed, NIST will post a notice on the *Data Classification Practices:*

Facilitating Data-Centric Security Management project website at https://www.nccoe.nist.gov/projects/building-blocks/data-classification announcing the completion of the project and informing the public that it will no longer accept letters of interest for this project. Completed letters of interest should be submitted to NIST and will be accepted on a first come, first served basis. There may be continuing opportunity to participate even after initial activity commences for participants who were not selected initially or have submitted the letter of interest after the selection process. Selected participants will be required to enter into a consortium CRADA with NIST (for reference, see ADDRESSES section above).

Project Objective: Data-centric security management aims to enhance protection of information (data) regardless of where the data resides or with whom it is shared. This requires that organizations know what data they have, what its characteristics are, and what security and privacy requirements it needs to meet so the necessary protections can be achieved. Standardized mechanisms for communicating data characteristics and protection requirements are needed to support zero trust architectures by making data-centric security management feasible at scale.

The project's objective is to develop technology-agnostic recommended practices for defining data classifications and data handling rulesets and for communicating them to others. This project will inform, and may identify opportunities to improve, existing cybersecurity and privacy risk management processes by helping with communicating data classifications and data handling rulesets. It will not replace current risk management practices, laws, regulations, or mandates. The project will define the approach for the solution, independent of the supporting technologies, services, architectures, operational environments, etc. As part of this, a proof-of-concept implementation of the defined approach will be attempted. The proof-of-concept will

include limited data discovery, analysis, classification, and labeling capabilities, as well as a rudimentary method for expressing how data with a particular label should be handled for each use case scenario. In support of this phase of the project, basic terminology and concepts will be defined based on existing practices and guidance to provide a common language for discussing data classification. The proposed proof-of-concept solution(s) will integrate commercial and open source products that leverage cybersecurity standards and recommended practices to demonstrate the use case scenarios detailed in the *Data Classification Practices: Facilitating Data-Centric Security Management* project description available at: https://www.nccoe.nist.gov/projects/building-blocks/data-classification. This project will result in a publicly available NIST Cybersecurity Practice Guide as a Special Publication 1800 series, a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses this challenge.

Requirements for Letters of Interest: 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 *Data Classification Practices: Facilitating Data-Centric Security Management* project description at https://www.nccoe.nist.gov/projects/building-blocks/data-classification and include, but are not limited to:

Core Components:

- Endpoints:
    - Client Devices – Various PCs (desktops or laptops) and mobile devices will be involved in data creation, storage, transmission, retention, and destruction, as well as data-centric security management. Some client

devices will be managed by the organization. Some will be used by the organization's employees, while others will be used by people from other organizations.

    - Client Device Apps – The client devices will have commercial-off-the-shelf (COTS) apps used for data lifecycle activities, such as word processing software and email client software.
    - Additional Devices – Examples of additional types of devices that could be utilized are networked printers and Internet of Things (IoT) devices.

- Network/Infrastructure Devices – The architecture will include devices such as firewalls, routers, or switches that are needed for network functionality and network traffic restriction, as well as the software for managing those devices.
- Services and Applications – The architecture will include several types of services and applications that are involved in data lifecycle activities for one or more of the scenarios. The following are examples of possible service and application types:
    - Enterprise Services/Applications: Email, collaboration, file sharing, web conferencing, file/data backup, code repositories, content management systems
    - Data Services/Applications: Data processing, data analytics, artificial intelligence/machine learning services
    - Business Services/Applications: A variety of system-to-system and human-to-system business applications, both COTS and custom-written, including those that produce and/or consume data
- Data Classification Solutions – The architecture will include several types of components used to perform data classification responsibilities, such as data discovery, inventory, analysis, classification, and labeling.

Each responding organization's letter of interest should identify how its products help address one or more of the following desired security characteristics and properties in section 3 of the *Data Classification Practices: Facilitating Data-Centric Security Management* at https://www.nccoe.nist.gov/projects/building-blocks/data-classification:

- All data is discovered and analyzed to determine how it should be classified.
- All data classification and data handling ruleset creation, modification, and deletion is restricted to authorized personnel only, with all actions logged and auditable and with all communications protected.
- For all data classifications and data handling rulesets, there is a mechanism for verifying the integrity of the policy or ruleset.
- Data classification labels or tags are assigned to all data.
- For all data classification labels or tags assigned to data, there is a mechanism for verifying the integrity of the label or tag.

In their letters of interest, responding organizations need to acknowledge the importance of and 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 *Data Classification Practices: Facilitating Data-Centric Security Management* project, which will be conducted in a manner consistent with the following standards and guidance: FIPS 199, NISTIR 8112, FIPS 200, SP 800-37, SP 800-53, SP 800-60, SP 800-63, SP 800-154, SP 800-171, SP 800-207, the NIST Cybersecurity Framework, and the NIST Privacy Framework.

Additional details about the *Data Classification Practices: Facilitating Data-Centric Security Management* project are available at https://www.nccoe.nist.gov/projects/building-blocks/data-classification.

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 *Data Classification Practices: Facilitating Data-Centric Security Management* project. 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 *Data Classification Practices: Facilitating Data-Centric Security Management* project. 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 *Data Classification Practices: Facilitating Data-Centric Security Management* project capability will be announced on the NCCoE website at least two weeks in advance at https://nccoe.nist.gov/. The expected outcome will demonstrate how the components of the *Data Classification Practices: Facilitating*

Data-Centric Security Management project architecture can provide security capabilities to mitigate identified risks related to data throughout its lifecycle. 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 https://nccoe.nist.gov/.

Alicia Chambers,
NIST Executive Secretariat.
[FR Doc. 2021-21979 Filed: 10/7/2021 8:45 am; Publication Date: 10/8/2021]