This document is scheduled to be published in the Federal Register on 04/17/2023 and available online at **federalregister.gov/d/2023-08079**, and on **govinfo.gov**

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 230302-0062]

RIN 0693-XC126

National Cybersecurity Center of Excellence *Mitigating Cybersecurity Risk in Telehealth Smart Home Integration*

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 *Mitigating Cybersecurity Risk in Telehealth Smart Home Integration* 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 *Mitigating Cybersecurity Risk in Telehealth Smart Home Integration* 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 [PLEASE 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. Interested parties can access the letter of interest template by visiting https://www.nccoe.nist.gov/healthcare/mitigating-cybersecurity-risk-telehealth-smart-home-integration and completing the letter of interest webform. NIST will announce the completion of the selection of participants and inform the public that it will no longer accept letters of interest for this project at https://www.nccoe.nist.gov/healthcare/mitigating-cybersecurity-risk-telehealth-smart-home-integration. 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 an NCCoE 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: Ronald Pulivarti via email to hit_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 *Mitigating Cybersecurity Risk in Telehealth Smart Home Integration* project are available at https://www.nccoe.nist.gov/healthcare/mitigating-cybersecurity-risk-telehealth-smart-home-integration.

SUPPLEMENTARY INFORMATION:

Background: The NCCoE, part of NIST, is a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity and privacy tools and technologies. The NCCoE brings together experts from industry, government, and academia under one roof to develop practical, interoperable cybersecurity and privacy 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 and privacy products and services.

Process: NIST is soliciting responses from all sources of relevant security and privacy capabilities (see below) to enter into an NCCoE Cooperative Research and Development Agreement (CRADA) to provide products and technical expertise to support and demonstrate security platforms for the *Mitigating Cybersecurity Risk in Telehealth Smart Home Integration* project. The full project can be viewed at: https://www.nccoe.nist.gov/healthcare/mitigating-cybersecurity-risk-telehealth-smart-home-integration.

Interested parties can access the template for a letter of interest by visiting the project website at https://www.nccoe.nist.gov/healthcare/mitigating-cybersecurity-risk-telehealth-smart-home-integration and completing the letter of interest webform. On completion of the webform, interested parties will receive a 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 desired requirements listed below, up to the number of participants in each category necessary to carry out this project. Once the project participant selection process is complete, NIST will post a notice on the *Mitigating Cybersecurity Risk in Telehealth Smart Home Integration* project website at https://www.nccoe.nist.gov/healthcare/mitigating-cybersecurity-risk-telehealth-smart-home-integration announcing the completion of the project participant selection and informing the public that it is no longer accepting letters of interest for this project. There may be continuing opportunity to participate even after initial activity commences. Selected participants will be required to enter into an NCCoE consortium CRADA with NIST (for reference, see ADDRESSES section above).

Project Objective:

The NCCoE will build an environment that will model patients' use of smart speakers in a telehealth ecosystem. The project's goal is to identify and mitigate cybersecurity and privacy risks associated with these ecosystems. The NCCoE environment will implement a "four-domain" ecosystem where solution components will be deployed in a patient's home, a cloud-hosted service provider, a health technology integration solution, and a healthcare delivery organization where each of these groupings represents a respective "domain." This project will apply concepts established in the NIST Risk Management Framework, NIST Cybersecurity Framework, and the NIST Privacy Framework to identify both cybersecurity and privacy challenges affecting the ecosystem. This project will describe risk assessment methodologies and will apply cybersecurity and privacy controls to mitigate risks that may be found in the ecosystem. The project environment will use commercially available technology and capabilities that enable patient-centric use cases described in the *Mitigating Cybersecurity Risk in Telehealth Smart Home Integration* project description available at: https://www.nccoe.nist.gov/healthcare/mitigating-cybersecurity-risk-telehealth-smart-home-integration. The project will result in a publicly available NIST Cybersecurity Practice Guide as a Special Publication 1800-series document that will describe an overview of the ecosystem, practical measures for health delivery organizations that include risk assessment approaches, mitigating control selection, reference architecture, and a detailed description on the lab environment construction.

Requirements for Letters of Interest: Each responding organization's letter of interest should identify which security and privacy platform component(s) or desired requirement(s) it is offering. Letters of interest should not include company proprietary information, and all components and desired requirements must be commercially available.

Components are listed in section 3 of the *Mitigating Cybersecurity Risk in Telehealth Smart Home Integration* project description at https://www.nccoe.nist.gov/healthcare/mitigating-cybersecurity-risk-telehealth-smart-home-integration. Components will align with each of the four domains that constitute the modelled ecosystem: the patient home environment, a cloud-hosted service provider, a health technology integration solution, and a healthcare delivery organization. Components for the respective domains include, but are not limited to:

- **Patient Home Environment**
    - **Smart home devices:** Devices (e.g., smart speakers) that have audio input and output capabilities. These devices are enabled to accept vocalized commands

involving natural language processing, speech-to-text, and text-to-speech that allow the user to access Internet-hosted resources.

  - **Personal firewall**: An application that controls network traffic to and from a computer, permitting or denying communications based on a security policy.
  - **Wireless access point router:** A device that performs the functions of a router and includes the ability for components to connect to the patient's network infrastructure, including having Internet communications.
  - **Internet router:** A device that provides a demarcation point for broadband communications access (e.g., cable, digital subscriber line [DSL], wireless, long-term-evolution [LTE], 5G) and presents an Ethernet interface to allow internet access via the broadband infrastructure. It may include wireless access point functionality or may allow for wireless access point routers to route network traffic through the Internet router.
- **Cloud-hosted Service Provider**
  - **Voice assist platform:** An environment that allows the cloud-hosted service provider and other organizations to develop applications that operate with smart home devices such as smart speakers. The voice assist platform enables applications by providing a natural language processing feature.
  - **Cloud platform:** A hosting environment where voice-enabled applications may be hosted and made available for patients to interact with health information systems.
- **Health Technology Integration Solution**
  - **Telehealth integration applications:** Code and applications that enable patient-driven functionality to interface with clinical systems. These should provide application logic that meets prevailing regulatory compliance requirements.

- **Healthcare Delivery Organization**
    - **Electronic health record (EHR) system:** A system that includes patient health history information.
    - **Patient portal:** A patient-facing application that allows the patient to retrieve their medical history information, schedule visitations, and request prescription refills.
    - **Network access control:** A capability or service that discovers and accurately identifies devices connected to wired networks, wireless networks, and Virtual Private Networks (VPNs) and provides network access controls to ensure that only authorized individuals with authorized devices can access the systems and data that the access policy permits.
    - **Network firewall**: A network security device that monitors and controls incoming and outgoing network traffic, based on defined security rules.
    - **VPN:** A secure endpoint access solution that delivers secure remote access through virtual private networking.

Each responding organization's letter of interest should identify how their products address one or more of the following desired requirements in section 3 of the *Mitigating Cybersecurity Risk in Telehealth Smart Home Integration* project description at https://www.nccoe.nist.gov/healthcare/mitigating-cybersecurity-risk-telehealth-smart-home-integration. The NCCoE intends to apply both the NIST Cybersecurity Framework and the NIST Privacy Framework. Both Frameworks apply a Function-Category-Subcategory paradigm. In this project, the NCCoE will use the Function and Category level concepts from both Frameworks to identify cybersecurity and privacy risk mitigation approaches. The NCCoE applies the Function and Category labelling found in both Frameworks. The Cybersecurity Framework labels Functions with a two-character identifier (e.g., the Function “Identify” is indicated by “ID”). Categories are labelled with the two-character identifier for the Function followed by a dot and a corresponding two-character identifier for the Category (e.g., the Category “Asset Management” within the Function “Identify” is indicated by “ID.AM”). Functions and Categories derived from the NIST Privacy Framework follow the same labelling conventions as those in the Cybersecurity Framework, except that "-P" is added to the character identifiers (e.g., the Function “Identify” is indicated by “ID-P”, and the Category “Inventory and Mapping” within the Function “Identify” is indicated by “ID.IM-P”).

Below are the desired requirements for this project; numbered items represent the Functions by which the NCCoE will examine this project, and the sub-bulleted points represent the corresponding Categories. The NCCoE will leverage these Functions and Categories in identifying cybersecurity and privacy risks and the corresponding risk mitigation approaches. All descriptions are specific to this project.

1. **IDENTIFY (ID and ID-P):** Organizations should ensure that they are aware of actors, components, integrating systems, and processes that are within or affect the environment. When examining a system, organizations should consider an enterprise view of the system's business value, drivers, outputs, and impact.
   - **Risk Assessment (ID.RA; ID.RA-P):** In context of this project, risk assessment activities examine a holistic reference architecture. Activities include assessing cybersecurity threats, vulnerabilities, problematic data actions, and both cybersecurity and privacy risks.
2. **CONTROL (CT-P):** These activities enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.
   - **Data Processing Management (CT.DM-P):** Data processing uses standardized formats to increase manageability and effectively manage privacy risk.

- **Disassociated Processing (CT.DP-P):** Data processing solutions permit selective collection or disclosure of data elements.

3. **<u>COMMUNICATE (CM-P):</u>** These activities enable organizations to convey design and build solution components to support predictability in data processing.

    - **Data Processing Awareness (CM.AW-P):** promotes a reliable understanding of data processes and privacy risks for both organizations and individuals that:
        - allows the patient visibility into how their data are processed and by which parties; and
        - enables traceability so that organizations and individuals understand where data originates and travels in the data processing ecosystem and information lifecycle.

4. **<u>PROTECT (PR and PR-P):</u>** These activities support the ability to develop and implement appropriate safeguards based on risk.

    - **Identity Management, Authentication, and Access Control (PR.AC; PR.AC-P):** includes user account management and remote access that:
        - implements controls that limit access to information systems, devices, and data only to authorized individuals, processes, and devices;
        - controls and audits accounts, e.g., administering and monitoring users, processes, and devices;
        - controls (and audits) access by external accounts and devices;
        - enforces least privilege for all (internal and external) accounts; and
        - enforces least functionality.
    - **Data Security (PR.DS; PR.DS-P):** includes data confidentiality, integrity, and availability assurance, as well as protecting individuals' privacy by:

    - securing data-at-rest and data-in-transit, i.e., communications between the smart home device and clinical systems should include data and hardware integrity and protections against unauthorized access and data leaks;
    - validating that cryptographic modules meet appropriate standards such as NIST Federal Information Processing Standards (FIPS) 140-2;
    - configuring systems to provide only essential functions; and
    - protecting communication and control networks.

5. **DETECT (DE):** These activities enable timely discovery of a cybersecurity event.
    - **Anomalies and Events (DE.AE):** this category ensures that the control environment establishes a baseline of expected behavior, monitors for unusual activity, and alerts appropriate individuals for event management.

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 and privacy platform components.
2. Support for development and demonstration of *the Mitigating Cybersecurity Risk in Telehealth Smart Home Integration* project for the healthcare sector in NCCoE facilities, which will be conducted in a manner consistent with the following standards and guidance: NISTIR 8228, NIST FIPS 140-3, NIST SP 800-41 Revision 1, NIST SP 800-52 Revision 2, NIST SP 800-57 Part 1 Revision 5, NIST SP 800-77 Revision 1, NIST SP 800-95, NIST SP 800-121, NIST SP 800-144, NIST SP 800-146, and NIST SP 1800-1.

Additional details about the *Mitigating Cybersecurity Risk in Telehealth Smart Home Integration* project are available at: https://www.nccoe.nist.gov/healthcare/mitigating-cybersecurity-risk-telehealth-smart-home-integration.

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 NCCoE consortium CRADA in the development of the *Mitigating Cybersecurity Risk in Telehealth Smart Home Integration* 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 and privacy platform and its performance characteristics sufficient to permit other organizations to develop and deploy security and privacy platforms that meet the security and privacy objectives of the *Mitigating Cybersecurity Risk in Telehealth Smart Home Integration* project. These descriptions will be public information.

Under the terms of the NCCoE 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 and privacy platform documentation, and demonstration activities. The dates of the project demonstration of the *Mitigating Cybersecurity Risk in Telehealth Smart Home Integration* project capability will be announced on the NCCoE website at least two weeks in advance at https://nccoe.nist.gov/. The expected outcome of the demonstration is to provide guidance on smart home device integration with healthcare information 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 https://nccoe.nist.gov/.

Alicia Chambers,
NIST Executive Secretariat.
[FR Doc. 2023-08079 Filed: 4/14/2023 8:45 am; Publication Date: 4/17/2023]