This document is scheduled to be published in the
Federal Register on 08/29/2019 and available online at
https://federalregister.gov/d/2019-18666, and on **govinfo.gov**

Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.:190605485-9485-01]

National Cybersecurity Center of Excellence (NCCoE) Securing Telehealth Remote Patient Monitoring Ecosystem

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 Securing Telehealth Remote Patient Monitoring Ecosystem for the healthcare sector use case. This notice is the initial step for the NCCoE in collaborating with technology companies to address cybersecurity challenges identified under the healthcare sector program. Participation in the use case 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: Letters of interest must be submitted to HIT_NCCOE@nist.gov or via hard copy to NIST, NCCoE, 9700 Great Seneca Highway, Rockville, Maryland 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 consortium Cooperative Research and Development Agreement (CRADA) with NIST. An NCCoE consortium CRADA template can be found at https://www.nccoe.nist.gov/sites/default/files/library/nccoe-consortium-crada-example.pdf.

FOR FURTHER INFORMATION CONTACT: Jennifer Cawthra via email at HIT_NCCOE@nist.gov; by telephone, 240-328-4584; or by mail to NIST, NCCoE, 9700 Great Seneca Highway, Rockville, Maryland 20850. Additional details about the healthcare sector program are available at https://www.nccoe.nist.gov/healthcare.

SUPPLEMENTARY INFORMATION: Interested parties must contact NIST to request a letter of interest template to be completed and submitted to NIST. Letters of interest will be accepted on a first-come, first-served basis. When the use case has been completed, NIST will post a notice on the NCCoE healthcare sector Securing Telehealth Remote Patient Monitoring Ecosystem project page at https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth announcing the completion of the use case and informing the public that NIST will no longer accept letters of interest for this use case.

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 CRADA to provide products and technical expertise to support and demonstrate security platforms for the Securing Telehealth Remote Patient Monitoring Ecosystem. The full use case can be viewed at https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth.

Interested parties should contact NIST by using the information provided in the FOR FURTHER INFORMATION CONTACT section of this notice. NIST will then provide each interested party with a template for a letter of interest, which the party must complete, certify that it is accurate, and submit to NIST. NIST 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. 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 use case. However, there may be continuing opportunity to participate even after initial activity commences. Selected participants will be required to enter 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.

Use Case Objective:

The objective of this use case is to provide an architecture that can be referenced and guidance for securing a telehealth remote patient monitoring (RPM) ecosystem in healthcare delivery organizations (HDOs) and patient home environments, including an example solution that uses existing, commercially, and open-source available cybersecurity products.

A detailed description of the Securing Telehealth Remote Patient Monitoring Ecosystem use case is available at https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth.

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 3 of the Securing Telehealth Remote Patient Monitoring Ecosystem project description (for reference, please see the link in the Process section above) and include, but are not limited to, those listed in the subsections below:

<u>Components for RPM Technologies</u>

- telehealth platform–a solution that enables data and communication flow from the patient monitoring device to the home monitoring device to the care providers
    - internet-based communications

    - transmission of telemetry data
    - videoconference
    - audioconference
    - email
    - secure text messaging
  - routing/triage functionality–The telehealth platform enables patients to identify an appropriate, networked team of care providers.
  - software development kits (SDKs) and application programming interfaces (APIs) that enable telehealth applications to interface with patient monitoring devices
  - patient monitoring devices that send telemetry data via the home monitoring device
    - blood pressure
    - heart monitoring
    - body mass index (BMI)/weight scales
    - other telemetry devices as appropriate
  - home monitoring device (e.g., specialized mobile application, stand-alone device) that transmits telemetry data to the telehealth platform and provides video connectivity

Components for Remote/Patient Home Environment

- 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 functions of a wireless access point
- endpoint protection (anti-malware)–a type of software program designed to prevent, detect, and remove malicious software (malware) on IT systems and on individual computing devices
- mobile device–a multimodal, small form factor communications mechanism that has characteristics of computing devices such as wireless network capability, memory, data storage, and processing. The device may provide real-time audio, video, and text communications as well as support email, web browsing, and other internet-enabled methods to interact with locally and remotely stored information and systems.
- modem–a device that provides a demarcation point for broadband communications access (e.g., cable, digital line subscriber [DSL], wireless, long-term-evolution [LTE], 5G) and presents an Ethernet interface to allow internet access via the broadband infrastructure
- wireless router–a device that provides wireless connectivity to the home network and provides access to the internet via a connection to the cable modem
- telehealth application–an application residing on a managed or unmanaged mobile device or on a specialized stand-alone device and that facilitates transmission of telemetry data and video connectivity between the patient and HDO

- patient monitoring device–a peripheral device used by the patient to perform diagnostic tasks (e.g., measure blood pressure, glucose levels, and BMI/weight) and to send the telemetry data via Bluetooth or wireless connectivity to the telehealth application

Components for HDO Environment

- network access control–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 access policy permits
- network firewall–a network security device that monitors and controls incoming and outgoing network traffic, based on defined security rules
- intrusion detection system (IDS) (host/network)–a device or software application that monitors a network or systems for malicious activity or policy violations
- intrusion prevention system (IPS)–a device that monitors network traffic and can take immediate action, such as shutting down a port, based on a set of rules established by the network administrator
- VPN–a secure endpoint access solution that delivers secure remote access through virtual private networking
- governance, risk, and compliance (GRC) tool–automated management for an organization's overall governance, enterprise risk management, and compliance with regulations

- network management tool–provides server, application-management, and monitoring services, as well as asset life-cycle management
- endpoint protection and security–provides server hardening, protection, monitoring, and workload micro-segmentation for private cloud and physical on-premises data-center environments, along with support for containers, and provides full-disk and removable media encryption
- anti-ransomware–helps enterprises defend against ransomware attacks by exposing, detecting, and quarantining advanced and evasive ransomware
- application security scanning/testing–provides a means for custom application code testing (static/dynamic)

Each responding organization's letter of interest should identify how its products address one or more of the following desired solution characteristics as outlined in Section 3 of the Securing Telehealth Remote Patient Monitoring Ecosystem project description (for reference, please see the link in the Process section above).

The primary security functions and processes to be implemented for this project are listed below and are based on the NIST Cybersecurity Framework.

IDENTIFY (ID)–*These activities are foundational to developing an organizational understanding to manage risk.*

- Asset management–includes identification and management of assets on the network and management of the assets to be deployed to equipment.

Implementation of this category may vary depending on the parties managing the equipment. However, this category remains relevant as a fundamental component in establishing appropriate cybersecurity practices.

- Governance–Organizational cybersecurity policy is established and communicated. Governance practices are appropriate for HDOs and their solution partners, including technology providers and those vendors that develop, support, and operate telehealth platforms.
- Risk assessment–includes the risk management strategy. Risk assessment is a fundamental component for HDOs and their solution partners.
- Supply chain risk management–The nature of telehealth with RPM is that the system integrates components sourced from disparate vendors and may involve relationships established with multiple supplies, including providers of cloud service.

PROTECT (PR)–*These activities support the ability to develop and implement appropriate safeguards based on risk.*

- identity management, authentication, and access control–includes user account management and remote access
  - controlling (and auditing) user accounts
  - controlling (and auditing) access by external users
  - enforcing least privilege for all (internal and external) users
  - enforcing separation-of-duties policies

        - privileged access management (PAM) with an emphasis on separation of duties
    - enforcing least functionality
- data security–includes data confidentiality, integrity, and availability
    - securing and monitoring storage of data–includes data encryption (for data at rest)
        - access control on data
        - data-at-rest controls should implement some form of data security manager that would allow for policy application to encrypt data, inclusive of access control policy
    - securing distribution of data—includes data encryption (for data in transit) and a data loss prevention mechanism
    - controls that promote data integrity
    - cryptographic modules validated as meeting NIST Federal Information Processing Standards (FIPS) 140-2 are preferred.
- information protection processes and procedures–includes data backup and endpoint protection
- maintenance–includes local and remote maintenance
- protective technology–host-based intrusion prevention, solutions for malware (malicious code detection), audit logging, (automated) audit log review, and physical protection

DETECT (DE)–*These activities enable timely discovery of a cybersecurity event.*

- security continuous monitoring–monitoring for unauthorized personnel, devices, software, and connections
  - vulnerability management–includes vulnerability scanning and remediation
  - patch management
  - system configuration security settings
  - user account usage (local and remote) and user behavioral analytics
  - security log analysis

RESPOND (RS)–*These activities support development and implementation of actions designed to contain the impact of a detected cybersecurity event.*

- Response planning–Response processes and procedures are executed and maintained to ensure a response to a detected cybersecurity incident.
- Mitigation–Activities are performed to prevent expansion of a cybersecurity event, mitigate its effects, and resolve the incident.

RECOVER (RC)–*These activities support development and implementation of actions designed to contain the impact of a detected cybersecurity event.*

- Recovery planning–Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
- Communications–Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, internet service providers, owners of

attacking systems, victims, other computer security incident response teams, vendors).

Responding organizations need to understand and, in their letters of interest, 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 Securing Telehealth Remote Patient Monitoring Ecosystem for the healthcare sector use case in NCCoE facilities, which will be conducted in a manner consistent with the following standards and guidance: NIST Special Publication (SP) 800-53, NIST FIPS 140-2, NIST SP 800-41, NIST SP 800-52, NIST SP 800-57 Part 1, NIST SP 800-77, NIST SP 800-121, NIST SP 800-146, Food and Drug Administration (FDA) Radio Frequency Wireless Technology in Medical Devices, FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, FDA Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, FDA Postmarket Management of Cybersecurity in Medical Devices.

Additional details about the Securing Telehealth Remote Patient Monitoring Ecosystem for the healthcare sector use case are available at https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth.

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 development of the Securing Telehealth Remote Patient Monitoring Ecosystem capability. Prospective participants' contributions to the collaborative effort will include assistance in establishing the necessary interface functionality, connection and setup 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 his or her 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 Securing Telehealth Remote Patient Monitoring Ecosystem for the healthcare sector use case. 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 Securing Telehealth Remote Patient Monitoring Ecosystem 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 improve telehealth RPM cybersecurity across an entire healthcare sector enterprise. Participating organizations will gain from the knowledge that their products are interoperable with other participants' offerings.

For additional information on the NCCoE's governance, business processes, and operational structure, visit the NCCoE website at https://nccoe.nist.gov/.

Kevin A. Kimball
Chief of Staff
[FR Doc. 2019-18666 Filed: 8/28/2019 8:45 am; Publication Date: 8/29/2019]