Enterprise Cybersecurity Awareness and Training Program Support (ECATPS)

Pursuant to FAR Subpart 5.2 - Synopses of Proposed Contract Actions, the Department of Health and Human Services (HHS), Centers for Medicare and Medicaid Services (CMS) hereby gives notice of a proposed Service-Disabled Veteran-Owned Small Business (SDVOSB) set-aside procurement for the program entitled, "Enterprise Cybersecurity Awareness and Training Program Support (ECATPS)."

This opportunity will be tracked as Advance Procurement Plan (APP) #220509; a solicitation number will be assigned when the formal solicitation is released.

This acquisition will be conducted under the authority of 15 U.S.C. § 657f using the competitive procedures of FAR 6.206, FAR 19.1405 and FAR Part 15.

Requirements Description

The Centers for Medicare & Medicaid Services (CMS) is a federal agency of the U.S. Department of Health & Human Services (HHS) that is responsible for administering Medicare, Medicaid, the Children's Health Insurance Program (CHIP), and the Health Insurance Marketplace programs. A key initiative of the agency is to help the approximately 100 million people covered under these programs receive high quality, better healthcare that results in lower costs.

CMS is responsible for the payment of approximately $1 trillion each year for medical services rendered to over 100 million program beneficiaries and recipients. The organization carries out its mission through employment of approximately 4,500 employees located at its central office site in Baltimore, and in 10 regional offices located in major cities throughout the United States. The agency contracts with numerous companies to process claims for reimbursement for medical services rendered under the Medicare program, and works with all 50 states, the District of Columbia and the Territories in the administration of the Medicaid and CHIP programs.

In the administration of these programs, CMS utilizes many assets, including buildings, facilities, communications equipment, computer systems, employees, Contractors, public trust, and information. A loss to any one of these assets could negatively affect the goals, the mission or the quality of support necessary for CMS to deliver and provide to its customers, stakeholders, and to the American public. Additionally, CMS collects, uses, and stores information that is defined as Personally Identifiable Information (PII), Protected Health Information (PHI), proprietary data, procurement data, inter-agency data, sensitive information, and / or privileged system information. Access to and the necessary protections of information can be controlled by the Privacy Act of 1974 (as amended), the Computer Security Act of 1987 (as amended), the E-Government Act, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Federal Information Security Management Act (FISMA) of 2002, as well as many other important and relevant rules, regulations, policies, and guidelines promulgated by HHS, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). As a result, CMS has a responsibility to collect, use, and / or disclose information properly and in accordance with federal regulations, to safeguard it at all times, and

to maintain the confidentiality, integrity, and availability (CIA) of information and information systems.

To safeguard the CIA of its information and information systems effectively, CMS has established an enterprise-wide cybersecurity and privacy program led by the Information Security and Privacy Group (ISPG). ISPG is charged with protecting CMS data as it "*provides leadership to CMS in managing information security and privacy risks appropriate for evolving cyber threats*". ISPG executes this vision utilizing an innovative approach to provide optimal visibility, situational awareness, resilience and incident response readiness across all CMS FISMA Systems.

The ISPG Security and Privacy program is responsible for defining policy, providing security and privacy services, and leading compliance and oversight of the program. The ISPG is comprised of five divisions: Division of Security and Privacy Compliance (DSPC), Division of Cyber Threat and Security Operations (DCTSO), Division of Security, Privacy Policy and Governance (DSPPG), Division of Strategic Information (DSI), and Division of Implementation and Reporting (DIR); and supported by the Front Office.

ISPG is looking for a contractor with knowledge in Cybersecurity and Privacy Awareness and Training Program support, which is needed to consolidate existing ISPG training efforts and support the continuation of the program's training activities of ISPG. Tasks and activities completed by the contractor will service ISPG, as well as ISPG's OIT Group partners and customers, to promote transparency, accountability, less duplication of effort, and improved program and cost efficiency. To meet these objectives, the contractor will have responsibilities in the following task areas:

- Project management
- Supporting the ISPG training team
- Consulting expertise to address emerging challenges and operation requirements within the awareness and training program
- Providing training content development services and delivery
- Providing subject matter expert support for the development, delivery and maintenance of a comprehensive information security and privacy awareness and training program
- Developing and implementing curriculum using the cognitive apprenticeship learning model
- Recommending, employing, and managing a unified learning management solution
- Actively participating in the support, refinement, and delivery of the CyberVet-cohort program, monitor, as well as providing feedback on the progress and results of both the cohorts and the program with recommendations to ISPG.

Training and Awareness Development Support

The contractor will review the current training program and emerging draft materials within ISPG and OIT to gain an understanding of the scope of the programs, materials, infrastructure, desired organizational and individual learning outcomes and supporting training goals and objectives. The outcome of the review should inform a plan or strategy for aligning work efforts underway, future developmental work, existing curriculum and supporting materials, and

learning strategies for a cohesive approach across all the various programs. All learning and performance outcomes should align with the current version of the NIST National Initiative for Cybersecurity Education (NICE) Framework considering compliance and levels of maturity in implementing the May 2019 Executive Order on America's Cybersecurity Workforce (E.O. 13870), and the Training Modernization Initiative. The following elements and activities have been identified to meet the needs of the CMS workforce learners and help make training efforts successful.

LMS Support

The contractor shall strategically support the deployment and maintenance of a unified training management solution that includes:

- Supporting and maintaining, as necessary, a Moodle Workplace Learning Management System (LMS) that will seamlessly manage participant registration, creation, distribution, and reporting of all training activities across ISPG and OIT to ensure compliance and audit-readiness.
- A LMS that has the ability to integrate with external designated content management systems rather than siloing all learning content internally to the system. This system will also provide integration with other virtual technologies – e.g., Pluralsight or Zoom – through specifications such as IMS Global's Learning Tools Interoperability (LTI) specification. This is common in current LMS solutions.
- Incorporating the latest tracking to assess the learner's prior learning and data specifications – i.e., xAPI – for providing cloud-based tracking of learner performance through a learning record store (LRS) and either built-in or SaaS analytical solutions for analyzing LRS data and reporting using dashboards.

The contractor shall assist the course developers by helping load, configure, edit, remove, maintain, and update courses in the LMS, to include addressing LMS configuration and system settings.

CyberVet Training

The Contractor will review the current CyberVet training program, all emerging draft materials, designated learning outcomes, goals, and objectives, and performance measures and metrics. Following the overall review, the Contractor shall provide a framework and strategy for aligning efforts and materials so that there is cohesion within and alignment among the various ISPG training programs. Outcomes should also align to and reference the current version of the NIST NICE framework, considering compliance and levels of maturity in implementing the May 2019 Executive Order on America's Cybersecurity Workforce, and the Training Modernization Initiative. The Contractor shall develop and implement the curriculum using the cognitive apprenticeship learning model and problem-based approach. Training should occur no less than 80% onsite at CMS HQ or other designated location or a blended approach (onsite and virtual) using appropriately designed technology platforms and learning tracking mechanisms.

Additional Information

It is anticipated that CMS will award a SDVOSB contract that will have a one-year base period, three (3) one-year option year periods, one (1) ten-month option period, and one (1) two-month transition-out period. The PSC code applicable to this procurement is U012 – Education/Training - Information Technology/Telecommunications Training.

This announcement is not a Request for Proposal (RFP). CMS expects to release a formal RFP around June 8, 2022 and to make a single contract award by September 2022. All responsible sources may submit a capability statement, which CMS will consider.

All statements of interest and capability must be submitted in writing (via e-mail) to the Contracting Officer and Contract Specialist **no later than 11:00am E.S.T. on Tuesday, June 7, 2022**. Telephone and fax inquiries will not be accepted. The Government is not obligated or committed to award any contract as a result of this notice.

Primary Point of Contact
Dawn R. Wilkins
Contracting Officer
Dawn.Wilkins@cms.hhs.gov
7500 Security Blvd., Mailstop B3-30-03
Baltimore, Maryland 21244

Secondary Point of Contact
Tiara Freeman
Contract Specialist
Tiara.Freeman@cms.hhs.gov
7500 Security Blvd. , Mailstop B3-30-03
Baltimore, MD 21244