

SOURCES SOUGHT NOTICE
OAM23065S- InfoSec Staff Augmentation
5/9/23

This is NOT a solicitation for a proposal, proposal abstract, or quote. The purpose of this notice is to obtain information regarding qualified business sources. The responses to the information requested will assist the Government in determining the appropriate acquisition method.

The mission of House Cybersecurity is to lead and direct the effort to provide a secure cyber environment for the enterprise, to ensure the integrity of the legislative process, maintain the ongoing operations of the House and protect legislative information residing on systems operating by and on behalf of the House. To accomplish this, Cybersecurity has four distinct sub-elements:

- Information Security provides incident response, investigates unauthorized or malicious activity, actively mitigates security risks, and uses threat intelligence, monitoring, and analyses to detect threats.
- Information Assurance leads governance (policy) activities, promotes security awareness, and implements system risk management activities.
- Identity Governance and Administration oversees the House identity, account management and certificate programs.
- Cybersecurity Architecture and Engineering develops innovative, adaptive, and trusted solutions to meet CAO's cybersecurity goals of ensuring secure cyber operations.

INFOSEC provides a wide range of information security support services to U.S. House of Representatives (House) Members, Committees, Leadership Offices, and staff. Chief among them is ensuring the continued operation of the systems that protect the House network against unauthorized access, modification of data, and malicious activity. These systems require continuous management and monitoring to ensure they are functioning as expected and to analyze and respond to alerts as they occur.

The Office of Cybersecurity's Information Security directorate (INFOSEC) anticipates seeking contractor support to assist in developing and maintaining efficient operational cybersecurity processes. The program focuses on the personnel, administrative, and technical measures applied to protect House assets, systems, and data from loss, destruction, misuse, alteration, or unauthorized disclosure or access. Cybersecurity adheres to applicable Federal and House security policies, standards, and regulations, while using industry best practices to drive program efforts. The Contractor must be able to provide qualified personnel to perform the work in the following areas:

- Cybersecurity Architecture
- Cloud Security
- Mobile Security
- Privilege Access Management
- Security Engineering
- Cybersecurity Threat Intelligence
- Penetration Testing
- Active Directory
- Cybersecurity Operations Support
- Endpoint Security Support

Questions may be submitted at any time. However, due to the nature of a Sources Sought the Government will do its best to answer questions in a fair/efficient manner and may not be able to answer all questions.

If interested, please submit a capability statement demonstrating your capacity to complete the requirement outlined above to Sharice.Frazier@mail.house.gov and Ryan.Moran@mail.house.gov no later than (NLT) Wednesday, May 24, 2023, at 2 PM EST.

The Capability Statement shall meet the following criteria:

- a. On page one (1) of the Capability Statement, begin by providing your company information as follows: Company name, address, phone number, CAGE code, DUNS number, GSA Contract Number (if applicable) and point of contact (name, phone and e-mail).
- b. Capability Statement must be in Microsoft Word, Microsoft Excel, or Adobe PDF format, single spaced, 11-point font (excluding charts and graphics) and the entire document shall not exceed 3 pages in length to include all attachments, charts, etc.
- c. Capability Statement must include but is not limited to (a) companies core capabilities (b) corporate experience, management capability, and the ability to recruit and retain talent for the positions requested; and examples of prior completed Government contracts (if any), references, and other related information.

Disclaimer and Important Notes

This Sources Sought does not obligate the Government to award a contract or otherwise pay for the information provided in response. The Government reserves the right to use information provided by respondents for any purpose deemed necessary and legally appropriate. Any organization responding to this notice should ensure that its response is complete and sufficiently detailed to allow the Government to determine the organization's qualifications to perform the work. Respondents are advised that the Government is under no obligation to acknowledge receipt of the information received or provide feedback to respondents with respect to any information submitted. However, responses to this notice will not be considered adequate responses to a solicitation. **Please note that the United States House of Representatives is not subject to Federal Acquisitions Regulations (FAR) or any of its supplements.**

Confidentiality

No proprietary, classified, confidential, or sensitive information should be included in your response. The Government reserves the right to use any non-proprietary technical information in any resultant solicitation(s).