



# Position brief for the position of Chief Information Security Officer The U.S. House of Representatives



# Contents

Opportunity Overview	3
About the U.S. House of Representatives	4
The Position	5
The Candidate	7
How to Apply	8

## Contact Information

---

**Diane Gilley** | Partner, Technology Practice

**Jon Barney** | Head, US Aerospace,  
Defense & National Security Practice

CV Submissions: [HouseCISO@odgersberndtson.com](mailto:HouseCISO@odgersberndtson.com)

**Odgers Berndtson**

1100 Connecticut Avenue, NW,  
Suite 800  
Washington, D.C. 20036



# Opportunity Overview

## The Position

The Office of the Chief Administrative Officer (CAO) provides operations support services and business solutions to the community of 10,000 House Members, Officers, and staff. The CAO organization comprises more than 650 technical and administrative staff working in a variety of areas, including information technology, finance, budget management, human resources, payroll, childcare, food and vending, procurement, logistics and administrative counsel.

The CISO will be responsible for leading and operating the House cybersecurity program, maintaining, and updating a comprehensive cybersecurity strategy that ensures the confidentiality, integrity, and availability of the House's information systems and resources. The CISO role requires a visionary, positive leadership focused individual with sound knowledge of cybersecurity fundamentals for risk management, incident management/response, and offensive engineering.

The ideal candidate is a thought leader, a consensus builder and builder of bridges between the cybersecurity office, its policies and strategy with the members, committees and leadership offices at the House, as well as with the other legislative branch agencies and oversight committees. The CISO must be able to translate complex technical concepts to non-technical audiences and to succinctly categorize and rank risk at higher and higher levels of leadership at the House. Finally, the CISO must be customer oriented, communicating the value of security to the organization to protect its reputational and data integrity.



# About U.S. House of Representatives, CAO

The U.S. House of Representatives is one of two chambers in the United States Congress. It is composed of 441 Members, who serve two-year terms.

Established in 1995, the Office of the Chief Administrative Officer (CAO) serves as an essential resource for the U.S. House of Representatives. We function as a non-partisan, non-legislative office that provides support services and business solutions to a community of 10,000 House Members, Officers, and staff. Our team of more than 700 employees is Member focused and service driven with a steadfast commitment to the values of Service, Innovation, Teamwork, Integrity, and Respect.

As a non-partisan organization, we provide everyone with the same level of exemplary service and have a cohesive and highly collaborative culture, regardless of political affiliation. For more information please visit: <https://cao.house.gov/about> and <https://www.house.gov/>

## DEI Statement

All applicants will be considered without regard to race, color, national origin, religion, sex (including marital or parental status), disability, or age.

Continued employment is contingent upon satisfactorily completing a criminal history records check (or other applicable security clearance) and pre-employment drug-test (pre-identified position only).

Title 1 of the Ethics in Government Act of 1978, as amended (5 U.S.C app§ 101 et seq.) requires certain House employees to file Financial Disclosure Statements.

For information please visit [http://clerk.house.gov/public\\_disc/index.aspx](http://clerk.house.gov/public_disc/index.aspx)



# The Position

## Duties & Responsibilities

---

- The CISO will be responsible for leading and operating the House cybersecurity program, maintaining and updating a comprehensive cybersecurity strategy that ensures the confidentiality, integrity, and availability of the House's information systems and resources. The CISO will lead a team of approximately 100 (30 full-time and 70 contractors) and a budget of approximately \$29M.
- The CISO role requires a visionary, positive leadership focused individual with sound knowledge of cybersecurity fundamentals for risk management, incident management/response, and offensive engineering.
- The ideal candidate is a thought leader, a consensus builder and bridge builder between the cybersecurity office, its policies and strategy with the members, committees and leadership offices at the House, as well as with the other legislative branch agencies and oversight committees.
- The CISO must be able to translate complex technical concepts to non-technical audiences and to succinctly categorize and rank risk at higher and higher levels of leadership at the House.
- Finally, the CISO must be customer oriented, hands-on, and action oriented, communicating the value of security to the organization to protect its reputational and data integrity.

## Measurement Criteria

---

The U.S. House of Representatives, CISO will be measured on the following criteria:

- Maintains responsibility for the overall/comprehensive executive level management in the areas of Information Security.
- Acts as a senior advisor to the CAO, the CIO, and various House and legislative branch constituents on issues related to Information Security.
- Maintains responsibility for the development, socialization, approval, and implementation of security policies.
- Appropriately assigns and monitors the progress of special limited-term projects and initiatives from assignment through completion.
- Briefs House leadership and officials on information security matters and issues.
- Provides appropriate assistance with computer forensics investigations to other House entities.
- Implements, manages, and operates systems to control access to House systems and data.
- Coordinates Members, Committees, and House Support Office security audits to ensure continued security of the network.



## Qualifications

---

- Demonstrated experience and success in senior leadership roles in risk management, information security, and IT or OT security.
- Bachelor's degree in Information Systems or in a discipline related to the position, or an equivalent level of professional work experience required; advanced degree preferred.
- 12+ years of experience in professional, executive level information security roles, including administering Information Technology security policies, procedures, configuration management and quality assurance preferred.
- Successful senior level experience in corporate, legislative and/or government environments required.
- Experience successfully executing programs that meet the objectives of excellence in a dynamic environment.
- Experience in progressive managerial/supervisory positions including effective use of employee performance plans and evaluations, coaching, and mentoring techniques, and addressing employee conflicts and disciplinary actions required.



# The Candidate

## Duties:

- Understands and interacts with related disciplines, either directly or through committees, to ensure the consistent application of policies and standards across all technology projects, systems, and services, including privacy, risk management, compliance and business continuity management
- Works with the vendor management office to ensure that information security requirements are included in contracts by liaising with vendor management and procurement organizations
- Assists with the identification of non-IT managed IT services in use ("citizen IT") and facilitates a corporate IT onboarding program to bring these services into the scope of the IT function, and apply standard controls and rigor to these services; where this is not possible, ensures that risk is reduced to the appropriate levels and ownership of this information security risk is clear
- Develops and maintains a document framework of continuously up-to-date information security policies, standards and guidelines. Oversees the approval and publication of these information security policies and practices
- Liaises with external agencies, such as law enforcement and other advisory bodies, as necessary, to ensure that the organization maintains a strong security posture and is kept well-abreast of the relevant threats identified by these agencies
- Creates a risk-based process for the assessment and mitigation of any information security risk in the ecosystem consisting of supply chain partners, vendors, consumers and any other third parties
- Coordinates the development of implementation of incident response plans and procedures to ensure that business-critical services are recovered in the event of a security event; provides direction, support and in-house consulting in these areas
- On a continuous basis, evaluates overall Information Technology security direction of the House, ensuring that all activities are secure, effective, and efficient.
- Develops budget plans for the Information Security office personnel and non-personnel resources
- Ensures 24x7 hour coverage for Information Security office functions.
- Provides guidance to staff and supervisors on desired results and planning considerations, monitors progress of assigned projects, and provides additional resources as appropriate.
- Performs other official duties and special projects as assigned.
- Has strong executive presence and has ability to brief and interact with multiple high level internal and external stakeholders.



## Location & Remuneration

This position will be based in the U.S. House of Representatives Office in Washington, D.C.

# How to Apply

In order to apply, please submit a comprehensive CV along with a cover letter that indicates your interest in the role and encapsulates the aspects of your experience relevant to the required criteria. Please include the names and addresses of three references. References will not be approached until the final stages and not without prior permission from candidates.

Please submit CVs to:  
[HouseCISO@odgersberndtson.com](mailto:HouseCISO@odgersberndtson.com)

### Contact Details

For a conversation in confidence, please contact:

**Diane Gilley** | Partner, Technology Practice  
[Diane.Gilley@odgersberndtson.com](mailto:Diane.Gilley@odgersberndtson.com)

**Jon Barney** | Head, US Aerospace,  
Defense & National Security Practice  
[Jon.Barney@odgersberndtson.com](mailto:Jon.Barney@odgersberndtson.com)





# About Odgers Berndtson



Odgers Berndtson Executive Search is a leading global executive search firm, assisting private and public sector organizations find the highest caliber, people, for senior management appointments across North America and internationally.

---

Our reputation at the top of the executive search profession is over 50 years old. With offices in over 60 cities worldwide, our experienced executive search specialists operate with absolute discretion, integrity, and care, and are expert in finding exceptional individuals for challenging roles.

## WE ARE GLOBAL

We have the support of an excellent international network of offices on the ground.





**ODGERS BERNDTSON**

Odgers Berndtson  
1100 Connecticut Avenue, NW,  
Suite 800  
Washington, D.C. 20036

<https://www.odgersberndtson.com/en-us>