HOUSE OF COMMONS

JOB DESCRIPTION

Supporting a thriving parliamentary democracy

Job title:	**Parliamentary Accreditor**
Campaign Type:	**Concurrent**
Payband:	**A1**
Pay range:	**£63,716 – £75,953 per annum** *(Appointment will normally be made at the minimum of the pay range)*
Team:	**Research and Information**
Section:	**Information Rights, Information Security (IRIS)**
Reports to:	**Head of IRIS Service**
Number of posts:	**1**
Hours:	**Full time, 36 hours per week**
Contract type/ duration:	**Permanent**
Issue date:	**10/10/2019**
Closing date:	**10/11/2019 at 23:55**

The House of Commons

The House of Commons and the iconic Palace of Westminster are key elements of the UK Parliaments. Around 2,500 staff work behind the scenes at the House of Commons, supporting the democratic process in many different ways. We are politically impartial and take great pride in the vision and values which guide our work.

It takes a huge range of skills and experience to keep the House of Commons running, and we all contribute to supporting a thriving parliamentary democracy.

Team information

The Information Rights and Information Security (IRIS) Service leads for the House on security of information, both paper and electronic, and manages the House's obligations under the information laws (The General Data Protection Regulation (GDPR/DPA 2018), Freedom of Information 2000 (FOI) and Environmental Information Regulations 2005 (EIRs)). Privacy, confidentiality, integrity and accessibility are the fundamental principles of the work of the IRIS service.

Job introduction

The Parliamentary Accreditor is a bicameral role, working across both Houses of Parliament and the Digital Service. The process of accreditation aims to ensure security is built into every solution we procure or develop. The Parliamentary Accreditor will provide independent assurance that technical solutions, storing or processing of Parliamentary data are meeting appropriate security standards. The post-holder will manage a programme of accreditation for Parliament, including the actions necessary to maintain these standards and mitigate risks identified. Applicable knowledge of national security policies, HMG security framework and

procurement processes as well as a sound understanding of Information Assurance and risk management are essential to this role.

The Parliamentary Accreditor is expected to maintain an agreed accreditation strategy that determines the accreditation process for Parliamentary ICT systems.

Key stakeholder relationships
Information Authority (IA) and Assurance Working Group (AWG)
House of Lords Information Compliance
Parliamentary Digital Service (PDS) and in particular, the Cyber Security team
Parliamentary Programmes such as Restoration and Renewal, Northern Estates, and other programmes related to information security
Government Departments (Security related)

Management responsibility

No current line management responsibility. As a specialist, you will oversee the work allocation and performance of project/support staff on a day to day basis as required.

Location
This post will be located on the Parliamentary Estate, Westminster, London. As part of the House of Commons Smart Working Pilot, flexible/remote working arrangements can be considered.

Security
Successful candidates will be required to complete pre-employment checks. All successful candidates are required to pass these checks before an offer can be confirmed.

The appointed candidate is required to be security cleared to Security Check (SC) level to undertake the role. Candidates who do not already have this level of clearance can have this undertaken post-appointment. In all cases the appointment remains conditional on this level of security clearance.

Applicants should be aware that if they have resided outside of the UK for a total of more than two of the last five years they are not eligible for vetting.

Please visit: https://www.parliament.uk/documents/PSD-Security-Vetting-booklet.pdf for further information.

Hours
Consideration will be given to candidates who wish to work part-time or as part of a job share. If you are selected for interview please inform the panel of the days/hours you are available to work, alternatively you can inform the recruitment team at any stage of the process.

Net conditioned full-time working hours for staff of the House are usually 36 per week. This excludes daily meal breaks of one hour.

The exact daily times of attendance will be agreed with line management.

For further information:
Candidates should refer to the House of Commons careers website https://www.parliament.uk/about/working/jobs/ or contact **Recruitment@parliament.uk** or 020 7219 6011.

Application and selection process
We will conduct a sift based on the criteria set out in the skills and experience section and successful candidates will be invited to attend a competency-based interview.

Key responsibilities

Knowledge
- Specialist knowledge of national security policies, international and British standards relevant to information security, HMG security framework and procurement processes as well as an expert understanding of information assurance and risk management
- Keeps up to date with new and emerging information and trends relating to information security
- Knowledge of the application of Information Security in construction projects and supply chain assurance is desirable

Accreditation and assurance
- Maintains and promotes the accreditation/assurance processes in Parliament
- Develops security accreditation strategies and provides guidance and support on security accreditation and re-accreditation activities
- Reviews the effectiveness of accredited solutions for re-accreditation where necessary
- Reviews and provides technical assessment of the security-related documentation required in the accreditation process
- Reviews cyber security overarching (high-level) architectures ensuring compliance to security policies and coherence among projects and systems
- Challenges others on the sensitivity of data and gains assurance that appropriate controls are in place
- Considers the needs of the Parliament and makes recommendations that balance business requirements against information risk
- Articulates risks in technical solutions clearly and concisely to non-technical audiences
- Creates Accreditation Statements to provide the Assurance Working Group and Information Authority with assurance that good security practices are in place and that information is not being exposed to any unnecessary or unwarranted risk

Independent decision-making
- To be responsible for accreditation decisions and maintaining a record of decisions along with the appropriate justification
- To provide independent assurance and manage a programme of accreditation for Parliament, including the actions necessary to maintain these
- Performs thorough assessment and analysis on new and existing changes to the service and its end-to-end components, ensuring fit for purpose solutions are implemented

Relationship building
- The Accreditor will work alongside the HOC IRIS Team, HOL Information Compliance Team and PDS Cyber Team to provide briefings for the IA on significant information security issues and progress reports
- The Accreditor will work on bicameral projects and will be expected to build working relationships across both Houses of Parliament and the Parliamentary Digital Service
- The Accreditor will be expected to build working relationships with similar roles across government and the wider public sector to aid benchmarking and keep up to date with developments.

Qualifications:
The following qualifications are required for this role:

Essential
NCSC Certified Cyber Professional Scheme at Senior Accreditor or Senior SIRA level, or able to provide evidence of working to this standard under each competency listed under the Skills and Experience section

Knowledge of ISO27001, CISSP, CISM, CISA, GIAC certification or equivalent or IAPP CIPP/E or CIPM qualified)

Desirable
A degree or equivalent recognised professional qualification in information security.

SKILLS AND EXPERIENCE	APPLICATION FORM	TEST/ EXERCISE	INTERVIEW
Essential **CRITERIA 1 –Experience** Proven experience as a Senior Accreditor working for a government department, public authority or similar organisation. Able to demonstrate accreditation or assurance experience on a wide range of information systems including standard IT infrastructures such as, cloud (AWS, Microsoft 365 and Azure) and BIM PAS 1192-5:2015.	☑	☐	☑
CRITERIA 2 – Knowledge A working knowledge of ISO27001/27002 control implementation and NCSC/CPNI guidance and assurance schemes. A good understanding of security related technologies including networks, remote access solutions and public key infrastructure.	☑	☐	☑
CRITERIA 3 – Risk Analysis Ability to analyse information and data, with excellent attention to detail to identify the main risks in complex situations, evaluate options and make sound accreditation decisions	☑	☐	☑
CRITERIA 4 – Decision Making Ability to use evidence and knowledge, balancing business need with risk, to make sound decisions based on business requirements	☑	☐	☑
CRITERIA 5 – Communication Skills	☑	☐	☑

Excellent oral and written communication skills with the ability to influence key stakeholders and present complex information clearly and effectively, with the ability to write policies and draft assessment reports for a wide range of audiences as required			
CRITERIA 6 - Collaborative Working Ability to work collaboratively and inclusively with others, identifying where responsibility lies and using feedback from others in the decision-making process while upholding the principles of diversity and inclusion	☑	☐	☑
CRITERIA 7 - Influencing and negotiating Demonstrable experience of influencing a diverse range of stakeholders at all levels, developing effective negotiation, influencing strategies and challenging assumptions where necessary	☑	☐	☑
Desirable **CRITERIA 8** Knowledge of Microsoft Active Directory, Microsoft Cloud and security standards for industrial control systems would be an advantage.	☐	☐	☑