Department for Transport

Role profile

Head of Cyber Compliance Team

Civil Service Grade: Grade 7	Salary Minimum: £54,105	Contract Type: Permanent
Job Type(s): Policy Risk Management Security	Civil Service Profession: Policy	DfT Directorate: Transport Security Co-ordination & Operational Response
Location(s): London	Reporting to Job Title: Head of Cyber, National Security Division	

Job description

Job summary

Transport Security, Resilience and Response (TSRR) leads on national security matters, ranging from counter terrorism and cyber security to planning for and responding to natural hazards or civil contingencies. We deliver expertise to support security and resilience policy teams whilst also providing the department's 24/7 response for all security or civil contingency incidents. The team works with security and intelligence partners from across government to mitigate risk to the UK's transport sector.

TSRR is a major player in delivering both the Government's counter-terrorism strategy (CONTEST), and the department's aim for a transport system that works for everyone and balances the needs of society, the environment, and the economy. A key factor in that aim is to deliver a safe, secure, and resilient transport network, for people and goods, for today and tomorrow.

Within TSRR, the National Security Division sits at the centre of the department's work to mitigate current and emerging National Security threats. We work collaboratively with modes, Government partners and industry to develop policy and regulations to proportionately mitigate current and emerging National Security threats, including:

- Using policy and regulatory levers to improve cyber security awareness and standards so the transport sector remains safe, secure, and resilient to cyber threats.
- Shaping Government strategies and policies to reflect the Department's equities and support wider HMG National Security objectives.
- Understanding and mitigating the risk to our Critical National Infrastructure and supply chains, particularly from Hostile State Activity; and

- Building a strong National Security community within the Department, which is supportive, diverse, and inclusive.

We also play a crucial role in the Department's emergency response mechanisms. You may be required to participate in the Department's response to a security or civil contingencies incident. This may include out of hours working on occasion, but we make every effort to allow for your personal circumstances.

Transport Security, Resilience and Response invests significantly in training and developing staff to prepare them not just for an interesting and challenging job, but also for a rewarding career in national security. Our expectation is that our staff will remain in post for at least two years.

Duties and responsibilities

This is a fantastic opportunity to shape the Department's work on cyber security, develop our approach to cyber regulation and lead our cyber compliance team to drive up standards across the transport sector to deliver the department's responsibilities under the Network and Information Systems (NIS) Regulations 2018.

You will be a motivational leader with the capability to lead a team, co-ordinate multiple work streams and deliver through others. You will be encouraging during challenging periods and embrace change and continual improvements.

You will have outstanding interpersonal and influencing skills, be articulate and demonstrate confidence in dealing with industry partners, as well as being comfortable handling challenging conversations to gain consensus.

You will have a strong security and technical background along with the relevant cyber qualifications and have a track record in leading and managing cyber or risk management teams. You will have strong interpersonal skills and experience of building and managing teams to deliver high profile programmes of work.

An additional allowance may be payable depending on candidate qualification. This allowance is non-pensionable and may be reviewed in any contractual agreements

As Head of Cyber Compliance Team, your key responsibilities will include:

- Lead a team of cyber compliance inspectors to ensure that transport operators in the UK implement appropriate and proportionate cyber security measures.
- Undertake a portfolio of inspections and visits to transport operators in the UK and to ensure relevant cyber security measures are implemented
- Ensure that the programme of inspections is properly resourced with trained inspectors
- Build and maintain key relationships with a range of stakeholders including transport operators, policy officials and fellow cyber regulators.
- Ensure accurate and concise information about cyber self-assessments and compliance activity is provided and recorded in a timely manner
- Maintain and awareness of current threats to the transport sector and what this may mean for the DfT as a cyber regulator.
- Develop and implement our cyber compliance operating model and is underpinning processes and practices
- Assist in the response to and handling of transport security incidents
- Work closely with the Head of Cyber to support wider work on compliance policy

Behaviours

Changing and Improving

Make changes which add value and clearly articulate how changes will benefit the business. Understand and identify the role of technology in public service delivery and policy implementation. Consider the full impact of implementing changes on culture, structure, morale and the impacts on the diverse range of end users, including accessibility needs. Identify early signs that things are going wrong and respond promptly. Provide constructive challenge to senior management on change proposals.

Making Effective Decisions

Clarify your own understanding and stakeholder needs and expectations, before making decisions. Ensure decision making happens at the right level, not allowing unnecessary bureaucracy to hinder deliver. Encourage both innovative suggestions and challenge from others, to inform decision making. Analyse and accurately interpret data from various sources to support decisions. Find the best option by identifying positives, negatives, risks and implications. Present reasonable conclusions from a wide range of complex and sometimes incomplete evidence. Make decisions confidently even when details are unclear or if they prove to be unpopular.

Communicating and Influencing

Communicate with others in a clear, honest and enthusiastic way in order to build trust. Explain complex issues in a way that is easy to understand. Deliver difficult messages with clarity and sensitivity, being persuasive when required. Remain open-minded and impartial in discussions, whilst respecting the diverse interests and opinions of others. Monitor the effectiveness of own and team communications and take action to improve where necessary

Managing a Quality Service

Demonstrate positive customer service by understanding the complexity and diversity of customer needs and expectations. Deliver a high quality, efficient and cost-effective service by considering a broad range of methods for delivery. Ensure adherence to legal, regulatory and security requirements in service delivery. Proactively manage risks and identify solutions. Create regular opportunities for colleagues, stakeholders, delivery partners and customers to help improve the quality of service.

Delivering at Pace

Ensure everyone clearly understands and owns their roles, responsibilities and business priorities. Give honest, motivating and enthusiastic messages about priorities, objectives and expectations to get the best out of people. Comply with legal, regulatory and security requirements in service delivery. Ensure delivery of timely quality outcomes, through providing the right resources to do the job, reviewing and adjusting performance expectations and rewarding success. Maintain own levels of performance in challenging circumstances and encourage others to do the same.

More information about Behaviours

Experience

Successful candidates must demonstrate experience of the following:

- Worked in a cyber security or risk management role
- Successfully led a team/group of people to deliver a business outcome
- Delivered a cross-cutting programme to challenging project timescales

More information about Experience

Strengths

You will be assessed against Civil Service Strengths at interview. For further details, please see the Civil Service Strengths Dictionary.

- Problem Solver

More information about Strengths

Other helpful information you need to know

Level of security clearance:	Working Pattern:	Contact Information:
Developed Vetting (DV)	Full-time; Part-time; Job share; Flexible working	Rachel Sowerby Rachel.Sowerby@dft.gov.uk

The post is reserved for UK Nationals.

The successful candidate would need to be willing to undergo DV clearance immediately if they do not hold it already.

This position is based in London, due to the need for the post holder to regularly access secure information in person in GMH and their responsibilities as a senior leader in response to a cyber security incident. TSRR strong supports flexible working and we would accommodate some remote working (including during Covid-19 travel restrictions) but the successful candidate would ultimately need to work in GMH at a minimum several days a week.