



HM Prison & Probation Service

HQ Job Description (JD)

Band 5

Directorate: Security

Job Description: DMIU Digital Forensics Investigator

Document Ref.	HQ-JES-3044_DMIU Digital Forensics Investigator_v1.0
Document Type	Management
Version	1.0
Classification	Unclassified
Date of Issue	29/09/2022
Status	Baselined
Produced by	Head of Group
Authorised by	Reward Team
JD Evidence	

HQ Job Description

Job Title	DMIU Digital Forensics Investigator (DFI)
Directorate	Directorate of Security
Band	5
Overview of the job	<p>The post holder(s) will work in the in the Digital Media Investigation Unit, part of the National Intelligence Unit at our Digital Forensics Facility (Doncaster) reporting directly to the Band 6 Digital Forensic Hub Manager</p> <p>The post holder will be responsible for supporting criminal investigations through Digital Forensic extraction and analysis across HMPPS, in conjunction with key Intelligence teams that include, but are not limited to, Prison Establishments, Counter Terrorism, Counter Corruption, Financial Intelligence, Sensitive Intelligence, Strategic Intelligence or Crime including Organised Crime nationally in HM Prison and Probation Service (HMPPS).</p> <p>DFIs will play a critical role in developing the intelligence picture on a range of threats impacting upon HMPPS, enhancing existing intelligence products as well as developing their own analysis.</p> <p>The post holder will be responsible for providing strategic and tactical intelligence analysis and products which will look across prison and probation contexts at 'high priority' offenders, offending groups and operational security vulnerabilities across HMPPS.</p> <p>They will be working within the DMIU Forensics Facility (Doncaster), which acts as the Centre of Excellence for Digital Forensic Services across HMPPS .Occasional travel is likely and will include prison establishments and specialist intelligence units and hubs, as well as law enforcement partners' offices.</p> <p>A background in analytical work (any discipline) would be an advantage but is not essential; training in Digital Forensics will be provided.</p> <p>Furthermore, this role will require the post holder to partake in specialist training and accreditation which will be provided and would be responsible for supporting the DMIU Forensics Facility in the delivery of digital forensic services. As such, the post holder will have: an active interest in technology and communications as required to support the delivery of the current policy (PSI 30/2011 – to be updated) in line with Forensic practices detailed within the ISO 17025 requirements.</p>
Summary	<p>This is an exciting opportunity to take up a key role within DMIU, which was created to support the key deliverables of the Directorate of Security (DoS), strengthening control systems and the processes for which the Director of Security is responsible. It was created to bring a range of tactical provision for exploiting illicit digital devices and illicit communications into one place, so that joined up and comprehensive services may be provided to a diverse range of local, regional and national customers dealing with digital threats affecting HMPPS.</p> <p>It is accepted that the existence of mobile devices in custody can be a facilitating factor in the continuance of crime by offenders involved in Serious Organised Crime, other criminal activity such as corruption and counter terrorism, and can undermine the safety and security of prison regimes, the rehabilitation of offenders and the safety and security of the public. Law Enforcement partners have experienced the</p>

	<p>need to ensure all criminally-focused investigations are able to fully exploit available digital sources of intelligence, a capability which DMIU has built in parallel.</p> <p>The post holder will also require strong communication skills to engage with a wide range of consumers of DMIU Services at all levels within HMPPS, with Law Enforcement partners.</p> <p>The post has no operational requirement, however, an understanding of prisons, probation and/or Law Enforcement operating environments would be an advantage. The post holder must act with the highest levels of personal and professional integrity and champion these qualities in others. They must be vetted to Security Check (SC) or Developed Vetting (DV) depending on the role.</p>
Responsibilities, Activities & Duties	<p>The following responsibilities, activities and duties are expected to be carried out by the post holder:-</p> <ul style="list-style-type: none"> • Extract and analyse seized digital media device content – To extract data from mobile phones, SIM Cards and associated media devices in order to analyse the content of these downloads to provide assessments that support investigations in prisons, and wider law enforcement in line with the latest guidance – providing witness statements for, or attendance at court for criminal cases as required. • Support the development of National and Regional Intelligence Products, producing evidence packages to support ad hoc ‘problem profiles’ based on emerging trends. • Produce Digital intelligence assessments to support the case management of high risk or emerging ‘threat group’ individuals. • Discuss and develop ‘Digital Strategies’ alongside key stakeholders (RIU, RDMI, Prisons) to assist with intelligence analysis products. • Obtain and evaluate digital evidence for intelligence analysis; apply analytical techniques to interpret extraction reports for intelligence analysis. • Disseminate digital intelligence products; and review the effectiveness of the analysis process. • Support prison and probation colleagues, as well as Law Enforcement partners, in understanding the Professionalisation of digital intelligence. • Ensure high quality forensic practices are maintained (in line with BS ISO 17025), while processing devices including appropriate storage / destruction of devices and data. • Ensure that the use of DMIU tactics remain effective and efficient by attending and engaging in tasking meetings regularly, acting as Subject Matter expert on Digital Forensics - providing advice and guidance to other staff where necessary. • Assist with cases where HMPPS are supporting a criminal investigation where specialist investigators are involved; covering all crime types affecting prisons and probation. DFIs will discuss these on a case-by-case basis with HMPPS leads, and provide the appropriate support and guidance in helping them to achieve operational objectives where by the use of digital forensics data may be required. • Ensure that Continuity of Evidence Procedures are maintained and followed in line with current local and national Policy to ensure adherence to legislation – aiding the possibility of successful prosecutions • Support the DMIU management team in maintaining the specialist technology provided. <p>The duties/responsibilities listed above describe the post as it is at present and is not intended to be exhaustive. The job holder is expected to accept reasonable alterations and additional tasks of a similar level that may be necessary. Significant adjustments may require re-examination under the Job Evaluation Scheme and shall be discussed in the first instance with the job holder.</p>

	An ability to fulfil all spoken aspects of the role with confidence through the medium of English or (where specified in Wales) Welsh.
--	--

Behaviours	<ul style="list-style-type: none"> • Seeing the Big Picture • Communicating and Influencing • Delivering at Pace • Working Together • Managing a Quality Service
Strengths	It is advised strengths are chosen locally, recommended 4-8.
Experience	<p>The post holder must have a sound understanding of the operational line and the way prisons and probations operate. They should have an advanced understanding of covert tactics, intelligence gathering and development, and investigations (criminally focused).</p> <p>Thorough knowledge and understanding of:</p> <ul style="list-style-type: none"> • NPCC Forensic Guidelines • ISO 17025 accreditation requirements • FSR Guidelines <p>The post holder must have an understanding and familiarity with the principles, legislation, rules, policies and tools of intelligence management.</p> <p>Have a good understanding and working knowledge of communications devices, social media user preferences and willingness to continually develop as technology advances.</p> <p>Have or able to obtain security clearance of at least SC level (DV may be required)</p>
Technical Requirements	<p>Conduct necessary upskilling and training in order to meet the requirements of ICDIP accreditation.</p> <p>The role requires accreditation as a trained Forensic Technician in relation to the retrieval and analysis of data from digital technology ensuring applicants compliance with policy</p> <p>Complete necessary certified training in order to conduct device extractions and other advances techniques such as physical repair and specialist interpretation of datasets.</p>
Ability	
Minimum Eligibility	<ul style="list-style-type: none"> • All candidates are subject to security and identity checks prior to taking up post • All external candidates are subject to 6 months probation. Internal candidates are subject to probation if they have not already served a probationary period within NOMS • All staff are required to declare whether they are a member of a group or organisation which the Prison Service consider to be racist

Hours of Work (Unsocial Hours) Allowances	<i>Leave Blank</i>
---	--------------------

Success Profile

Behaviours	Strengths It is advised strengths are chosen locally, recommended 4-8	Ability	Experience	Technical
------------	--	---------	------------	-----------

Seeing the Big Picture			The post holder must have a sound understanding of the operational line and the way prisons and probations operate. They should have an advanced understanding of covert tactics, intelligence gathering and development, and investigations (criminally focused).	Conduct necessary upskilling and training in order to meet the requirements of ICDIP accreditation.
Communicating and Influencing			Thorough knowledge and understanding of: <ul style="list-style-type: none"> • NPCC Forensic Guidelines • ISO 17025 accreditation requirements • FSR Guidelines 	The role requires accreditation as a trained Forensic Technician in relation to the retrieval and analysis of data from digital technology ensuring applicants compliance with policy.
Delivering at Pace			The post holder must have an understanding and familiarity with the principles, legislation, rules, policies and tools of intelligence management.	Complete necessary certified training in order to conduct device extractions and other advances techniques such as physical repair and specialist interpretation of datasets.
Working Together			Have a good understanding and working knowledge of communications devices, social media user preferences and willingness to continually develop as technology advances.	
Managing a Quality Service			Have or able to obtain security clearance of at least SC level (DV may be required)	

Choose an item.				
Choose an item.				
Choose an item.				