**DESCRIPTION OF SERVICES:**

The Cyber Digital Career Pathways project, sponsored by the Home Office, started in 2016 focusing on the professionalisation and upskilling of Law Enforcement Agency (LEA) cyber and digital investigation operatives.

A skills and standards framework (SSF) has been developed, providing a consistent standard for operatives working on cybercrime investigations or involved in investigations where digital opportunities exist. The Intellectual Property Rights (IPR) is owned by the CoP who will maintain and update the framework on a regular basis. A process for assessing competency, involving submission of a written portfolio and face-to-face interviews, has been designed and successfully tested. The provider will be contractually required to comply with the existing framework and accreditation processes which have been ratified to be used by ICDIP.

This contract will require the provider to work in conjunction with stakeholders including the CoP. The requirement to conduct face-to-face interviews and GDPR (Official Sensitive data) means the provider will need to have a UK footprint.

The provider must deliver the highest accreditation standards and afford professional status enabling the Institute’s membership to be recognised for its expertise and professional standing in law enforcement. The ICDIP must provide all LEAs, as well as the judiciary with confidence that its members hold professional competency and status for the specialist work that they perform in this field.

The development of an ‘investigation’ professional body is new in the cyber digital environment. The skills requirements for investigation are distinct from those that exist in its equivalent cyber security sector. It is fully intended however, that the ICDIP will work in parallel with cyber security professional accrediting bodies.

The following is indicative of services the provider will be expected to deliver (to be expanded upon at the market day):

* Effective and efficient delivery of the assessment and accreditation process
* Undertake planning and delivery of the assessment process whilst providing good value for money for candidates and organisations
* Robust quality assurance and evaluation processes to ensure continuous improvement of the assessment and accreditation process
* Maintain the register of accredited practitioners and ensure members comply with continuing professional development (CPD)
* Provide training and development to ensure the assessors and interviewers have a full understanding of the skills and standards framework, the assessment process and the required standard
* Quality assure the assessors and interviewers to ensure they deliver consistent assessments and deliver high quality feedback
* Comply with the skills and standards framework and work with the CoP to ensure this is maintained and updated on a regular basis
* Promote and expand the scheme to LEAs to increase uptake whilst ensuring the integrity of the scheme is maintained
* Provide upskilling opportunities and events in cyber and digital investigation, to all members as part of their membership fee
* Provide support to all candidates to ensure they fully understand the accreditation process and membership criteria
* Provide accurate management information as required by the CoP to enable it to manage the contract

The competitive process to appoint a provider of services to the ICDIP will result in a contract being awarded, for a proposed period of at least three years, with the option to extend for up to two further one-year periods.

The value of the contract will become clear during the procurement process. There will be no payment by the CoP for this work; the funding for the provider will derive from the agreed membership structure charges along with sponsorship and other funding sources. The fees charged will be expected to cover the running costs of the provider, the ICDIP and the CoP in its role of maintaining the SSF. Further information will be provided at the market day.