U.S. Department of Commerce Non-Competitive Job Alert

Direct Hiring Authority

JOB ALERT: U.S. Department of Commerce is seeking to fill a Cyber Criminal Investigator position.

The U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement is seeking to fill a non-supervisory Cyber Criminal Investigator, 1811-11/12/13/14 position in Manassas, VA.

This is a temporary excepted service appointment, not-to-exceed (NTE) September 30, 2024 under the Bureau of Industry and Security's appointing authority authorized under Public Law 117-103, Consolidated Appropriations Act, 2022, to support the situation in Ukraine. This appointment may be extended as needed, up through September 30, 2024. You may be required to serve a trial period. After one year of completion of work in accordance with the established performance plan and demonstrating proper conduct, you may be converted to a career/career-conditional appointment in the competitive service.

Full Permanent Change of Station expenses are not authorized. However, in limited circumstances, a relocation incentive may be authorized for GS-1811-14 career/career-conditional appointments in the competitive service.

Organization

The Bureau of Industry and Security (BIS) advances U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system, and by promoting continued U.S. leadership in strategic technologies. BIS accomplishes its mission by maintaining and strengthening adaptable, efficient, effective export controls and treaty compliance systems, along with active leadership and involvement in international export control regimes. BIS's Office of Export Enforcement (OEE) is an elite law enforcement organization recognized for its expertise, professionalism, integrity, and accomplishments. OEE accomplishes its mission through preventative and investigative enforcement activities and then pursuing appropriate criminal and administrative sanctions against export violators.

Position Description

OEE special agents are sworn federal law enforcement officers with authority to make arrests, execute search warrants, serve subpoenas, and detain and seize goods about to be illegally exported. OEE initiates investigations based on information and intelligence obtained from a variety of sources. OEE conducts investigations to gather testimony and evidence of alleged or suspected violations of dual-use export control laws. OEE works closely with the Department of Justice to impose criminal sanctions for violations, including incarceration and fines, and with the Office of Chief Counsel for Industry and Security (OCC-IS) to impose civil fines and denials of export privileges. OEE routinely works with other Federal law enforcement agencies, including the FBI and the Department of Homeland Security, when conducting investigations or preventative actions. OEE conducts its enforcement operations worldwide.

This position is located in OEE's Cyber Division located in Manassas, VA and is responsible for conducting complex analysis and investigations through industry outreach and leveraging data analytics and data visualization tools.

To be successful, OEE needs special agents who possess a broad range of education, experiences, and skills. Our special agents come from a wide variety of career backgrounds beyond law enforcement or the military, including foreign affairs, intelligence analysis, science, business, and technology. For example, you may utilize foreign language skills to elicit information from a witness to an illegal export, technical skills to place covert recording and transmitting devices on an undercover special agent, accounting skills to decipher financial records to trace the illicit flow of money to prohibited entities overseas, or communication and collaboration skills to participate in joint agency investigations.

General Duties and Responsibilities:

The selected candidate will be responsible for the following duties:

- Receives, develops, and evaluates leads, original requests, complaints and allegations from informants, industry, the U.S. Government, and other sources.
- Plans, coordinates, conducts, and completes exceptionally complex cyber investigations into criminal and noncriminal matters.
- Applies knowledge of federal criminal statutes, rules of evidence, court procedures, and investigative techniques in the Cyber realm.
- Develops an investigative plan designed to obtain essential facts and proof and performs accurate and impartial fact-finding to execute that plan.
- Conducts interviews, interrogations, and examination/procurement of pertinent records both in the U.S. and abroad.
- Conducts investigative activities including surveillance, writing, and serving of subpoenas, taking sworn statements, preparing, and serving search and arrest warrants, developing and utilizing informants and conducting detentions/seizures of shipments/items.
- Coordinates findings with other law enforcement agencies, other regulatory agencies, OCC-IS, other DOC program areas, and the United States Attorney's Office, as appropriate, in preparation for prosecution of administrative proceedings and/or criminal prosecutions arising from investigations conducted.
- Summarizes and reports all investigative activities efficiently in a clear, logical, and impartial manner.
- Plans, coordinates, conducts, and completes exceptionally complex cyber investigations that result in criminal or administrative penalties or actions.
- Performs digital forensic analysis to identify investigative leads and/or identify evidence which tends to prove or disprove a criminal act occurred.
- Analyzes and prepares clear, concise, and comprehensive written reports on trends regarding highly complex and sensitive cyber intrusion matters.
- Develops and maintains liaison and communication with other Cyber investigative partners and private sector stakeholders.
- Provides technical advice or recommendations on Cyber investigative activities, coordinating investigation activities with federal, state, or local law enforcement as necessary.
- Advises and supports matters involving defensive measures to enhance computer network operations against exploitation.
- Applies intelligence and analytic processes, standards, and tradecraft to perform targeted analyses of emerging cyber adversary tactics and threats.
- Prepares and edits written cyber-intelligence/assessment products from multiple sources.

Qualifications for the Position:

- Adheres to the highest standards of conduct, especially in maintaining honesty and integrity.
- Undergo a rigorous background investigation and credit checks in order to obtain and maintain a Top-Secret Clearance.
- Pass a medical exam, which includes but is not limited to, meeting visual and hearing standards.
- Pass a drug test prior to appointment and be subjected to random drug testing periodically thereafter.
- Successfully complete approximately 12 weeks of employment as a special agent trainee while housed at the Federal Law Enforcement Training Center (FLETC) in Glynco, GA. Similar certification from the DEA, FBI, or Postal Inspector academy may be considered in lieu of CITP from FLETC.
- Maintain a high level of physical fitness necessary to complete FLETC training and throughout their career.
- Possess and maintain a valid state driver's license.
- Upon graduation from FLETC and throughout their career, be available for worldwide assignment on either a temporary or long-term basis.
- Work 50 hours a week, which may include irregular hours, and be on call 24/7, including holidays and weekends.
- Be willing to travel either domestically or internationally when necessary to complete mission objectives.
- Firearms Qualification: The incumbent must qualify with firearms authorized by OEE and participate in a recurring qualification course. The incumbent is expected to abide by current OEE policies. The incumbent will also arm at specific times as required by the supervisor.
- Lautenberg Amendment: This position authorizes the incumbent to carry a firearm. Any person who has been convicted of a misdemeanor crime of domestic violence cannot lawfully possess a firearm or ammunition (Title 18 U.S.C. 922(g).
- Be willing and able to participate in arrests, execution of search warrants and other potentially dangerous assignments.
- Those with current or prior federal LEO coverage will be considered only if they can demonstrate that they will have completed 20 years of covered service by mandatory retirement age of 57. This requirement may be waived for Veterans.
- Be willing to complete advanced and time intensive cybersecurity certifications through proctored examinations

Desired Qualifications:

- Data analytics, data science experience
- Excellent written and oral communication skills
- Computer network exploitation/defense experience
- Advanced Cyber Security Certifications
- Computer network administration background
- Cyber threat intelligence/assessment products background

To Apply

Email your resume, Cover Letter, professional references, non-competitive eligibility (NCE) documents to**:** **criminalinvestigators@bis.doc.gov . Open until filled. Personally**

Identifiable Information (PII) must be redacted or removed prior to sending any documents as a part of this application. Examples of PII are social security numbers (even if truncated to the last 4), date of birth and specific medical information. DD 214s and VA disability letters often have PII on them, please review your documents carefully before sending.

Please refer to the position descriptions on the BIS Website (doc.gov) prior to submitting your resume/documents for consideration to ensure you meet the qualifications for the position to which you are applying.

Many of the positions being advertised are not entry level and require a graduate degree or relevant experience in the specified field in order to qualify for employment.

If you only hold a bachelor's degree, you will likely need 3 to 5 years of relevant work or volunteer experience in order to qualify for a GS-11 position.

Graduate degree holders or bachelor's degree holders with 3 or more years of relevant work experience may be qualified for higher grade position based upon relevant volunteer or work experience.

Note: The Subject line should contain the following information "Cyber Criminal Investigation Application." Please ensure the content of your resume adequately addresses the qualification requirements of the position as listed in the solicitation announcement.

Selection will be made without discrimination for non-merit reasons such as race, color, religion, sex, national origin, age, handicapping condition, marital status, sexual orientation, or political affiliation.