U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
HOMELAND SECURITY INVESTIGATIONS

HSI Directive 22-01: Cyber Operations Officer Program

Issue Date: September 7, 2022
Superseded: N/A

1. Purpose/Background. This Directive establishes the policies governing the Cyber Operations Officers (COOs), General Schedule (GS)-1801, for all programmatic areas in Homeland Security Investigations (HSI) and the capabilities of the COO position.

The core cyber investigative mission of U.S. Immigration and Customs Enforcement (ICE) is carried out by HSI domestic field offices, with critical support and oversight provided by the Cyber Crimes Center (C3) at HSI Headquarters (HQ). As a result, COOs should possess and develop robust cyber skillsets to support HSI investigations. Adhering to this Directive will ensure that the best qualified COOs are recruited, trained, retained, and properly utilized based on their skillsets and the needs of C3 and HSI field offices.

2. Policy. It is the policy of HSI to recruit, hire, and retain the best-qualified candidates for its COO positions. Furthermore, it is the policy of HSI to ensure that COOs are utilized in line with HSI priorities as determined by HSI leadership.

3. Definitions. The following definitions apply for purposes of this Directive only:

3.1. Case Agent: Special Agent assigned to, or in charge of, a criminal investigation with responsibility over the management, strategic direction, and operational security of the case, including requesting assistance and coordinating with assigned COO(s), as necessary.

3.2. Field Supervisor: Any supervisor assigned to an HSI field office with direct management responsibilities of assigned COO(s).

3.3. Cyber Crimes Center: HSI HQ entity with direct oversight of the COO Program.

4. Responsibilities.

4.1. Executive Associate Director (EAD), HSI. The EAD of HSI has overall responsibility for the oversight and implementation of the provisions of this Directive.

4.2. Deputy Assistant Director (DAD), C3. The DAD of C3 is responsible for the administration of the COO Program.

4.3. Unit Chief (UC), Cyber Crimes Unit (CCU). The CCU UC is responsible for providing policy, guidance, training, and resources to ensure that the COO Program is sufficiently supporting HSI cyber investigations. This responsibility includes coordinating and developing training for all COOs and providing them with the initial training and equipment necessary to perform their duties. Since technology is constantly evolving, the CCU Unit Chief is responsible for keeping abreast of new changes, and for providing ongoing resource updates for the COO Program.

4.4. Section Chiefs (SCs), CCU. CCU is divided into three sections: the Network Intrusion Section, the Digital Crimes Section, and the Technical Solutions Section, each managed by an SC. The SCs are responsible for overseeing the Program Managers (PMs) and other assigned personnel, including the COOs assigned to C3, and for coordination with field supervisors with assigned COOs. The SCs report to the CCU Unit Chief.

4.5. Program Managers (PMs), CCU. CCU PMs are responsible for providing direct support to COOs, and for liaising with HSI HQ divisions, HSI field offices, ICE Directorates and Program Offices, and other agencies. This function may include forwarding requests for cyber investigative support and replacing or acquiring new equipment for COOs.

4.6. Special Agents in Charge (SACs). SACs are responsible for implementing the provisions of this Directive within their respective areas of responsibility. SACs are also responsible for designating a Group Supervisor as a Field Supervisor (defined in Section 4.7 below) to manage the day-to-day activities of the COO(s) assigned to their office.

4.7. Field Supervisors. Field Supervisors are Group Supervisors or Resident Agents in Charge who are responsible for the day-to-day assignment of work, time and attendance, local awards, discipline, and Performance Work Plans for their assigned COO(s). The Field Supervisor should maintain regular contact with the CCU PM to ensure that the COO(s) are being properly utilized to support field office requirements in line with COO capabilities. CCU will coordinate any requests for COO support through the Field Supervisor to ensure proper workload management and for visibility.

4.8. Special Agents. HSI Special Agents are responsible for complying with the provisions of this Directive and collaborating with COOs to leverage their cyber-specific skillset, as appropriate or required, to support investigations and operational initiatives.

4.9. Cyber Operations Officers. COOs are HSI GS-1801 employees who provide support to HSI investigations with a need for cyber-specific skillsets in the planning and execution of law enforcement activities. COOs assist criminal investigations through functions including, but not limited to, computer network operations activities, undercover computer network architecture and management, computer forensics analysis, computer network intrusion response, and/or computer programming activities. The functions of a COO are consistent with CCU's enumerated functions under Title 6, United States Code (U.S.C.), Section 473(d)(2). Further, COOs will engage in duties related to investigative

support, and prepare detailed written investigative reports, as appropriate. The COO(s) may, with coordination and approval of a supervisor, and consistent with 6 U.S.C. § 473 (d)(2)(C)(ii), provide training and technical support in cyber-related matters to local, state, federal, tribal, military, and foreign law enforcement partners upon request and subject to the availability of funds.

5. Procedures/Requirements.

5.1. Administration of the COO Program. The COO Program will be administered by CCU at C3.

1) No COO will be subject to geographic mobility as a condition of employment.

2) HSI is the ICE Line of Business Directorate for the COO, GS-1801, occupational series.

3) HSI will use a competitive process to hire candidates and/or make use of the various hiring authorities as authorized.

4) External candidates may be considered for COO positions at various grade levels based on a qualification evaluation.

5) Candidates will be hired for placement either at C3 or in an HSI field office.

   a) If selected for and assigned to C3, the COO(s) will report to a first-line SC or equivalent for assignment of work, Performance Work Plan ratings, time and attendance, and other C3 management functions, including, but not limited to, Telework or Remote Work agreements or considerations, workplace accommodations, and local administrative requirements or functions, consistent with ICE policy.

   b) If selected for and assigned to an HSI field office, the COO(s) will report to a Field Supervisor or equivalent for assignment of work, Performance Work Plan ratings, time and attendance, and other field office management functions, including, but not limited to, Telework or Remote Work agreements or considerations, workplace accommodations, and local administrative requirements or functions, consistent with ICE policy. The Field Supervisor will coordinate closely with C3 to ensure that COOs are being assigned and are performing work commensurate with their skillsets and the needs of the HSI field office. Based on operational and special skillset needs, C3 may request assistance from the COO(s) through the Field Supervisor.

5.2. Computer Forensics Program (CFP). If appropriately trained and certified in Computer Forensics (consistent with the Computer Forensics Handbook (HSI HB 20-03), dated June 12, 2020, or as updated), and with the approval of the Unit Chief of the C3 Computer Forensics Unit, the COO(s) may be placed in the CFP and equipped with

appropriate computer forensics equipment. A COO placed in the CFP will be exempt from the minimum hour requirements set forth for full time Computer Forensic Agents/ Analysts but is expected to contribute to or collaborate with the CFP in furtherance of HSI operational goals.

5.3. Continuing Education. COOs will participate in at least 40 hours of C3-approved and funded annual continuing education in areas related to cyber-based skills, including, but not limited to, cybersecurity, network intrusion, digital crime, computer forensics, programming, and other relevant technologies in furtherance of HSI investigative priorities.

5.4. Cyber Investigative Support. COOs will comply with the Cyber Crimes Investigations Handbook (HSI HB 11-03), dated August 9, 2011, or as updated. Unless otherwise prohibited by statute, policy, or Office of the Principal Legal Advisor (OPLA) opinion, COOs, under the guidance or coordination of an HSI supervisor or a criminal investigator, may participate in the following cyber investigative support activities (not inclusive, but demonstrative of identified skillsets):

1) **Network Intrusion Investigations**
   Encryption and Decryption
   Malware Analysis
   Timeline Composition for Intrusions and Data Theft
   Incident Response
   Network Investigations and Mitigation
   Cyber Threat Intelligence

2) **Digital Crime Investigations**
   Peer-to-Peer, VPNs, and Proxy Servers
   Open Source and Social Media Research
   Dark Web/Darknet Marketplaces
   Anonymization Technology
(b) (7)(E)

3) **Cryptocurrency Analytics**
   Illicit E-Commerce
   Blockchain
   Digital Wallet Attribution
   Computer Forensics with a Focus on Digital Finance
   Cryptocurrency Forensics and Analysis

4) **Computer Forensics**
   Basic (based on operational need)
   Advanced

5) **Operational Support**
Website Design
Website Administration
Project Management
Court Testimony
Evidence Handling

(b) (7)(E)

5.5. (b) (7)(E)

5.6. **Training.** Based on the availability of funding, C3 will offer newly hired COOs with introductory level curriculum, which includes cyber investigative or cybersecurity focused disciplines. Based on availability, OPLA will provide legal training that will supplement the existing curriculum.

Based on the availability of funding, C3 will provide COOs with equipment commensurate with their skillsets/certifications in support of and to further HSI

investigations. COOs accepted into the CFP will be provided equipment, based on the availability of funding, in support of the forensics program.

Based on the availability of funding, C3 will sponsor COOs for C3-approved advanced training and certifications.

6. **Recordkeeping.** This Directive is a permanent record and should be retained in accordance with the approved Department-wide Administrative and Operational Records Common to All Offices Records Schedule (DAA-0563-2019-0008-0004). This Directive should be cut off when superseded or cancelled, then transferred to the National Archives and Records Administration 15 years after cutoff. If the records are subject to a litigation hold, they may not be disposed of under a records schedule until further notification.

7. **Authorities/References.**

7.1. 6 U.S.C. § 473(d)(2) – Cyber Crimes Unit, Functions.

7.2. HSI HB 20-03, Computer Forensics Handbook, dated June 12, 2020, or as updated.

7.3. HSI HB 11-03, Cyber Crimes Investigations Handbook, dated August 9, 2011, or as updated.

7.4. (b) (7)(E) [redacted]

8. **Attachments.** None.

9. **No Private Right.** This Directive provides only internal HSI policy guidance, which may be modified, rescinded, or superseded at any time without notice. It is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter. Likewise, no limitations are placed by this guidance on the otherwise lawful enforcement or litigative prerogatives of HSI.

STEVE K FRANCIS

Digitally signed by STEVE K FRANCIS
Date: 2022.09.07 08:38:19 -04'00'

Steve K. Francis
Acting Executive Associate Director
Homeland Security Investigations