A Call to Action: Equipping Law Enforcement With the Tools to Investigate Cybercrime

Cybercrime Training for Law Enforcement

A National Threat

Cybercrime is one of the greatest threats facing our country and has enormous implications for our national security, economic prosperity, and public safety. The challenge facing state, local, tribal, and territorial (SLTT) law enforcement partners includes investigating a broad variety of cybercrimes and cyberthreats by criminals, hackers, terrorists, and state actors. **To meet this challenge, it is vital that SLTT law enforcement leaders ensure that appropriate agency personnel receive cybercrime training.** The following examples of no-cost federally funded cybercrime trainings are available for agency personnel to build a basic understanding of cybercrime and to explore advanced considerations.

No-Cost Federally Sponsored Cybercrime Training

FBI Cyber

Cyber Certification Program: The Cyber Investigator Certification Program (CICP) is a multilevel online training program designed to teach advanced technical skills to law enforcement personnel at all levels. The first course, "The First Responders Course," is currently available through the Law Enforcement Enterprise Portal at https://www.cjis.gov or via www.riss.net. Other advanced courses will follow in the future.

The FBI Cyber Shield Alliance (https://www.cjis.gov/CJISEAI/EAIController) provides extensive resources for SLTT partners, including eGuardian (https://www.cjis.gov/CJISEAI/EAIController) access, intelligence sharing, federally sponsored training, and fellowships at the National Cyber Investigative Joint Task Force (http://www.fbi.gov/about-us/investigate/cyber/ncijtf). The FBI also supports the InfraGard (https://www.infragard.org) partnership with the private sector.

National Initiative for Cybersecurity Careers and Studies

The National Initiative for Cybersecurity Careers and Studies (NICCS)—a national resource for cybersecurity awareness, education, training, and career opportunities—makes research and training information available through a robust, searchable catalog that allows users to find cyber training programs based on location, preferred delivery method, specialty area, or proficiency level. NICCS supports the U.S. Department of Homeland Security's (DHS) objective to grow the cyber workforce by providing information about science, technology, engineering, and math; cyber-related degree programs; internship and scholarship opportunities; and cyber competitions and events. The NICCS Training Catalog is also located at https://niccs.us-cert.gov/training/tc/search.

National Computer Forensics Institute

The U.S. Secret Service, in cooperation with the Alabama District Attorneys Association, operates the National Computer Forensics Institute (NCFI) to provide federally sponsored training (including equipment) for SLTT partners, including law enforcement, prosecutors, and judges. For additional information on the NCFI, visit https://www.ncfi.usss.gov.

This project was supported by Grant No. 2014-DB-BX-K004 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the Global Justice Information Sharing Initiative and the U.S. Department of Homeland Security. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice and the U.S. Department of Homeland Security.

No-Cost Federally Sponsored Cybercrime Training (continued)

Federal Law Enforcement Training Centers (FLETC) Cyber Division

The FLETC Cyber Division, located in Glynco, Georgia, has 14 cyber-related training programs for law enforcement personnel. The programs provide entry-level to advanced cybercrime training, as well as training on electronic surveillance and tracking with use of GPS, IP Camera, and Wi-Fi technologies. One of these programs, the Basic Incident Response to Digital Evidence (BIRDE) program, can be delivered to SLTT law enforcement across the United States. The full FLETC training course catalog is located at https://www.fletc.gov/training-catalog.

FEMA's National Training and Education Division

FEMA's National Training and Education Division (NTED) services include cybercrime- and cybersecurity-focused courses provided by the Texas Engineering Extension Service, the University of Texas–San Antonio, Norwich University Applied Research Institutes, the Illinois Emergency Management Agency, and the Criminal Justice Institute that address a range of issues, including network assurance, digital forensics, cyber law, white collar crime, and cyber incident analysis and response. To access the NTED Web site, visit https://www.firstrespondertraining.gov.

SEARCH Online Learning Portal Cyber Training

SEARCH is a nonprofit organization that provides technical, policy, and operational assistance, as well as training, to justice and public safety agencies throughout the country. SEARCH provides several computer-related online training courses for law enforcement personnel investigating crimes with a possible cyber link, such as *Crime Involving Handheld Computing Devices* and *Social Networking Sites: Investigative Tools and Techniques*. To access SEARCH online training, visit https://elearning.search.org.

National White Collar Crime Center (NW3C)

NW3C provides a nationwide support system for law enforcement and regulatory agencies involved in the prevention, investigation, and prosecution of economic and high-tech crime. NW3C delivers training in computer forensics, cyber and financial crime investigations, and intelligence analysis. NW3C currently provides several no-cost federally funded courses in the fields of cyber investigations, forensics and cybercrime, network intrusions, mobile forensics, and wireless network investigations, such as *Cyber Investigation 100—Identifying and Seizing Electronic Evidence* and *Legal Concerns for Digital Evidence Responders 101: First Responders and Digital Evidence*. To access NW3C online training, visit http://www.nw3c.org/training/online-training.

Additional Resources and Training

Law Enforcement Cyber Center

The Law Enforcement Cyber Center (LECC) was created to enhance the awareness, expand the education, and build the capacity of justice and public safety agencies to prevent, investigate, prosecute, and respond to cyberthreats and cybercrimes. http://www.iacpcybercenter.org.

U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Cyber Crimes Center

The **ICE HSI Cyber Crimes Center** offers a variety of technical training courses related to cyber investigations and digital forensics on a request basis. http://www.ice.gov/cyber-crimes.

U.S. Department of Justice Computer Crime and Intellectual Property Section (CCIPS)

The CCIPS manuals *Searching and Seizing Computers* and *Electronic Evidence and Prosecuting Computer Crimes* are available at http://www.justice.gov/criminal/cybercrime/documents.html.

Internet Crime Complaint Center (IC3)

SLTT partners can also advise the public to file complaints online with the Internet Crime Complaint Center (http://www.ic3.gov/default.aspx).

For More Information

For more information about the training programs highlighted in this document and additional training opportunities, visit the Law Enforcement Cyber Center Training page, located at http://www.iacpcybercenter.org/topics/training-2.

"Cyberthreats are among the gravest national security dangers to the United States."

—White House Press Release

Issued 03/16