CyberSecurity Academy


DoD APPROVED 8570

CYBERSEC FIRST RESPONDER™

ANSI ACCREDITED
ISO/IEC 17024
Personnel Certification Program
#1208

## CFR is Approved to U.S. DoD 8570

CFR is an approved Baseline Certification for the CSSP Analyst and CSSP Incident Responder categories, and it verifies the skills necessary to perform these job functions. The addition of CFR to the DoD 8570 highlights Logical Operations' ability to meet the most rigorous cybersecurity certification standards in the industry today.

## CFR Certification

The CyberSec First Responder exam validates that students have the skills needed to analyze cyber threats, design secure computing and network environments, proactively defend networks, and respond to and investigate cybersecurity incidents. Students can sit for the high-stakes CFR-210 exam virtually or in-person through PearsonVUE.

### CORPORATE BENEFIT

CFR takes a holistic approach to preparing employees to analyze threats, secure networks, handle incidents, and utilize other critical security skills to protect your organization with a single course.

### STUDENT PROFILE

Designed for information assurance professionals whose job functions include development, operations, management, and enforcement of secure systems and networks.

### COURSE OBJECTIVES

This course focuses on developing a systematic process for securing an organization's network by implementing an incidence handling and response plan through threat detection and analysis.

### LABS

At CyberSecurity Academy, we feel there is no substitute for practice. Hands-on practical activities are provided in a cloud based format, accessible from just about anywhere.

## LESSON OBJECTIVES

1. Assess information security risk in computing and network environments.
2. Analyze the cybersecurity threat landscape.
3. Analyze reconnaissance threats to computing and network environments.
4. Analyze attacks on computing and network environments.
5. Analyze post-attack techniques on computing and network environments.
6. Evaluate the organization's security posture within a risk management framework.
7. Collect cybersecurity intelligence.
8. Analyze data collected from security and event logs.
9. Perform active analysis on assets and networks.
10. Respond to cybersecurity incidents.
11. Investigate cybersecurity incidents.

## WHO SHOULD ATTEND?

This course is designed for information assurance professionals who perform job functions related to the development, operation, management, and enforcement of security capabilities for systems and networks.

## PREREQUISITES

- Recommended at least 2 years of experience in computer network security technology or a related field.
- Recognize information security vulnerabilities and threats in the context of risk management.
- Operate at a foundational level some of the common operating systems for computing environments.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in computing environments. Safeguards include, but are not limited to, basic authentication and authorization, resource permissions, and anti-malware mechanisms.
- Operate at a foundational level some of common concepts for network environments, such as routing and switching.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in network environments. Safeguards include, but are not limited to, firewalls, intrusion prevention systems, and VPNs.

## DAYS OF TRAINING

5 days/approximately 35 contact hours/
1 semester/5 days boot camp

## CERTIFICATION / EXAM

Certified CyberSec First Responder/
2 hours (100 questions)

# MEET YOUR CFR INSTRUCTOR – STEVE HAILEY

As of 2018, Steve Hailey will be an Information Technology veteran of thirty-five years, with twenty-eight years of experience developing and delivering technical training. Steve has thirty-two years of data recovery experience, and has been providing cybersecurity and digital forensics services professionally for twenty-one years. years. He is a highly skilled expert witness and dynamic instructor, bringing to bear his combined skills in cybersecurity and digital forensics. He is currently serving on the National CyberWatch Center's Curriculum Standards Panel, contributing to the nation's first curriculum model standard for cybersecurity education.

He is the founder and former President of the Washington State High Technology Crime Investigation Association, and was formerly Vice President of the Digital Forensics Certification Board. Steve has performed work and conducted training in the fields of computer networking, cybersecurity, and digital forensics for Fortune 500 companies, law firms, the federal government, the DoD, law enforcement agencies, and several colleges and universities. He is actively involved with developing and delivering training in digital forensics and information security to members of city, state, and federal law enforcement agencies, and has trained military personnel tasked with performing smart phone and computer forensics in the Mideast. Steve has also served as an instructor and Subject Matter Expert for Texas A & M University, developing information security curriculum for them.

Steve is a Cyberterrorism Subject Matter Expert for DHS and FEMA sponsored programs, and has trained DoD and Federal law enforcement personnel to protect some of the most aggressively targeted information systems in the world within our nation's critical infrastructure. Students attending the Cyberterrorism courses include members of FEMA, NSA, DARPA, U.S. Air Force, U.S. Army, U.S. Navy, U.S. Marine Corps, Unified Military Commands, FBI and the USSS.

Steve developed the Continuing Legal Education course "Digital Forensics for Attorneys" which has been delivered to attorneys and legal professionals locally and internationally, to include the Washington State Attorney General's Office and the United Arab Emirates Ministry of Justice. As well, he developed and delivered training in conducting comprehensive digital forensic examinations to members of law enforcement for the Abu Dhabi, Ajman, Dubai, and Sharjah police departments in the United Arab Emirates.

He has authored certification practice tests for several vendors and is also a Subject Matter Expert for CompTIA's Security+. Steve has processed digital forensic cases ranging from inappropriate resource use and network intrusions to cases involving identity theft, credit card fraud, child pornography and money laundering. He is creator of the CyberSecurity Forensic Analyst (CSFA)™ certification, as well as the author of several digital forensics/forensic computing course books.

Steve is co-author of the paper "Defining a Process Model for Forensic Analysis of Digital Devices and Storage Media" which was published by the IEEE in 2007. In 2008, Steve co-authored a paper entitled "A Case Study; Overcoming Anti-Forensic Methods Used on External Storage Drives" which was presented at the Annual Scientific Meeting for the American Academy of Forensic Science. The methodology developed and presented for the paper is now in use by forensic analysts worldwide.

He is a Certified Information Systems Security Professional (CISSP), an AccessData Certified Examiner, a Digital Forensics Certified Practitioner, and he possesses a certificate in computer forensics from Oregon State University. In addition to these credentials, Steve has 31 additional technical certifications. His professional affiliations include The Agora, InfraGard, and the High Tech Crime Consortium. Steve has been featured on television, radio, and has authored several articles related to digital forensics and information security.

# MEET YOUR CFR INSTRUCTOR – MIKE ANDREW

Mike has been an Information Technology professional for fifteen years, and has been conducting training and forensic analysis since 2003 for attorneys, various law enforcement agencies, and several colleges throughout the Pacific Northwest. He is certified by the National Security Agency in INFOSEC Assessment Methodology and is a CyberSecurity Institute Certified Instructor, Certified Ethical Hacker, AccessData Certified Examiner, Digital Forensics Certified Practitioner, and Certified Data Recovery Expert. He also possesses college-level certificates in Network Security and Micro-Computer Support, and has attended and completed training from the E-Discovery Training Academy at Georgetown University Law Center.

Mike is actively involved with developing and delivering training in digital forensics to members of city, state, and federal law enforcement agencies, and has trained military personnel performing forensic analysis in the Mideast. He has performed work as a forensic analyst on cases at all levels - local, state, and federal.

Mike is currently a member of the Computer Information Systems Dept. Advisory Committee and Digital Forensics Committee at Edmonds Community College in Washington State. He is an officer and founding member of the Washington State chapter of the High Technology Crime Investigation Association and is also a member of the High Tech Crime Consortium.

Mike is a Cyberterrorism Subject Matter Expert for DHS and FEMA sponsored programs, and has trained DoD and Federal law enforcement personnel to protect some of the most aggressively targeted information systems in the world within our nation's critical infrastructure. Students attending the Cyberterrorism courses include members of FEMA, NSA, DARPA, U.S. Air Force, U.S. Army, U.S. Navy, U.S. Marine Corps, Unified Military Commands, FBI and the USSS.

Working with Steve Hailey, Mike developed the CLE course "Digital Forensics for Attorneys" which has been delivered to attorneys and legal professionals locally and internationally, to include the Washington State Attorney General's Office and the United Arab Emirates Ministry of Justice. In partnership with Steve Hailey, Mike recently developed and delivered training in conducting comprehensive digital forensic examinations to members of law enforcement for the Abu Dhabi, Ajman, Dubai, and Sharjah police departments in the United Arab Emirates.

Mike is principal author of the paper "Defining a Process Model for Forensic Analysis of Digital Devices and Storage Media" which was published by the IEEE in 2007. In 2008, Mike was also principal author of the paper that he and Steve Hailey wrote entitled "A Case Study; Overcoming Anti-Forensic Methods Used on External Storage Drives" which he presented at the Annual Scientific Meeting for the American Academy of Forensic Sciences. Mike is also co-author of the book "Computer Forensics Core Competencies - Practical Skills for the Forensic Examiner." In addition to all of his credentials, Mike recently earned the prestigious Digital Forensic Certified Practitioner certification through the National Center for Forensic Science.