

Intelligence, Counterintelligence and Counterterror Training Modules

Offered by CT/CI Training Partners LLC

Intelligence and CI Courses

(The length of all courses listed below is designated in hours unless otherwise noted.)

The Practice of Counterintelligence

4 hours

This module will focus on the fundamental principles, theories and tradecraft of Counterintelligence, as practiced by both allied and hostile Foreign Intelligence Services [FIS]. We will examine espionage and the pursuit of spies by answering the following: Who are the spies? How and for whom do they spy? How has their profile and motives evolved from the Cold War to the present? How do we catch spies?

Events that Shaped US Intelligence and CI: 1776-Present

5-days

This 5-day class considers the spies, the intelligence operations and the laws from the Revolution to the modern era that have impacted the intelligence and CI professions in America. It is a comprehensive look at the interrelated intelligence, counterintelligence, law enforcement, politics, historic events and the personalities that impacted not only the U.S. intelligence profession but American history as well.

(The following are ten, ½ day, classes that form the basis of the 5-day course on the history of intelligence in America above)

Intelligence, CI and the Revolutionary War

4

An overview of America's intelligence collection and counterintelligence operations in our war for independence from Great Britain. It covers the challenges, risks, successes, and failures of our novice intelligence leadership, operations officers, and spies. It also considers the early development of intelligence tradecraft using real case examples of spies, counterintelligence and covert communications techniques.

Intelligence, CI and the Civil War

4

We were forced to reinventing intelligence collection and counterintelligence capabilities in 1861 because, like our standing army, our intelligence capabilities created during the Revolutionary War were allowed to wither. This module considers the spies, tradecraft, risks, successes, and failures of the intelligence agencies and officers on both sides in the Civil War.

Intelligence, CI and Sabotage in WWI

4

This module is an overview of German intelligence and sabotage operations in American during WWI and the U.S. counterintelligence response by the Secret Service, the Department of Justice, NYPD, Military Intelligence Division and the Office of Naval Intelligence.

SOVIET-CPUSA Espionage in America: 1917-1945 4

An overview of thirty years of effective Soviet intelligence collection operations and the damage done to America. This module considers the early development of the Soviet intelligence effort in America and our lack of an effective response. Topics: the Communist Revolution in Russia and the “Red Scare” that followed; the Palmer Red Raids; CPUSA as a vehicle for identifying and recruiting spies; the impact of the Depression and Spanish Civil War on espionage; WWII and Soviets switch sides; WWII ends – the Cold War begins.

German Espionage in US: 1925-1945 4

An in-depth examination of German intelligence collection operations during the inter-war years through the end of WWII and the American counterintelligence operations against them. Topics: German targeting of the U.S. aircraft industry; the Griehl-Rumrich espionage ring; the theft of the Norden Bombsight; the William Sebold case; the creation of the FBI’s Special Intelligence Service (SIS) and its operations against Nazi spies in South America; Nazi spies land in American.

Japanese Espionage in America: 1930-1945: Focusing on the interwar years from the 1920s through the attack on Pearl Harbor in 1941 and continuing to the end of WWII, we will examine the agencies, officers and intelligence collection operations which targeted the US by the Empire of Japan.

The Rosenbergs, VENONA and McCarthyism 4

This module is an overview of the transition from the hot war of WWII to the Cold War. It considers the climate of fear in America that led to “witch hunts” for Communist in government; the loss of the military advantage of the atomic bomb from Soviet espionage; the trial and execution of the Rosenbergs, the greatest CI success of the Twentieth Century – the VENONA Program; and the lasting impact of McCarthyism.

The Rise, Fall and Rise of US Intelligence 4

This module is an overview of the evolution of the US Intelligence Community from the enactment of the National Security Act of 1947 to the present. It will explore the history, the organization, the successes and failures of the USIC from the massive reorganization of the National Security Act of 1947 to the present day. Students will examine the role played by intelligence in the history of America and the appreciation of its value by each presidential administration during the last sixty-five years. It is anticipated that this module will assist students to better appreciate the past mistakes that have caused the controls under which the modern intelligence community is required to operate and perhaps avoid some of those mistakes in the future.

The Anarchist Terror Threat: 1880s - Present 4

This module highlights world-wide Anarchist terrorism from the late 19th Century to the present. Students learn the connections between the Anarchist movement and the Industrial Revolution, the organization of the trade union movement and other significant events in the late 19th and early 20th Centuries so they can better understand the demonstrations and terror attacks we are currently experiencing from the 2d Wave of Anarchism today.

Codes, Ciphers and Secret Ink

4

The use of codes, cryptanalysis, secret ink and Signals Intelligence from the American Revolution to present, the spies who use them and the lessons learned in detecting and neutralizing them. Topics: Washington's Setauket Spies in Long Island use codes and the "*sympathetic stain*"; the role of the telegraph, signal codes, ciphers and code breakers in the Civil War; the Zimmerman telegram; Magic and Enigma and their role in WWII; the VENONA program.

The Media, Intelligence, CI and Counterterror Ops

4

This module explores the relationship between the Media and government institutions, at all levels, which deal with intelligence, CI and terrorism. Is the Media the "terrorist's best friend?" What is the responsibility of the Media to national security and the threats posed by terrorists? Does the Media know they are being manipulated by terror groups? These and other questions will be addressed as we explore the complex relationship between the Media, the government, intelligence and terror.

Intelligence, CI, CT and the Law

4

In this module we examine the U.S. Constitution, the Federal statutes, the Executive Orders and the agency regulations that have controlled and directed intelligence, counterintelligence and counterterrorism operations in American from the Revolution to the modern era. From early Neutrality and Sedition laws, to Supreme Court rulings following the Civil War to Watergate, to the Economic Espionage Law of 1996, to the Patriot Act, laws will be examined and connected to the operational controls intelligence and CI professionals must consider when operating today.

Foreign Intel Service Targeting of USIC

4

While most spies are "volunteers", Foreign Intelligence Services also target using elicitation techniques and/or recruitment operations, U.S. nationals with access to classified or proprietary information, technology, facilities and persons. This presentation examines the often complex process by which FIS's identifies and lures, sometimes unwitting, individuals into clandestine agent relationships and obtains intelligence from them.

The Espionage Threat to America

4/8 hours

This module is an overview of the evolution, organizational structure, capabilities and objectives of the Russian (the SVR, FSB, GRU and FSO), the PRC (the MSS, MID and 2PLA) and the Cuban (the Dirección General de Inteligencia or DGI) Intelligence and Security Services. Participants will examine the scope, scale and focus of their targeting of the U.S. over the past decade as well as their operational tradecraft in a series of case studies on each of these hostile services.

The Russian Intelligence Service

4/8 hours

Focus on the operational doctrine of the Russian intelligence services that targets Western services- "Operativnaya Ingra" (Aggressive" Operational Games"). Participants will study both Russian and Western CI doctrine and practices by examining the opposing intelligence and CI operations. We will examine a series of inter-related Soviet intelligence operations involving the recruitment and handling of "*penetrations*" (*Moles*), *double agents and turned agents* by both sides.

Russian Intelligence Service's Illegal Espionage Operations 4

This module will focus on the Russian Intelligence Services' long use of illegals in foreign espionage operations. The concept of the illegal intelligence officer will be defined, put in historical context and described in detail using a wide variety of case examples. Topics: the profile of an illegal, their mission, training, targeting and COVCOM; the role of "the Centre" (Moscow) in illegal operations; the role of the "Rezidentura"; evolution of illegal tradecraft, agent handling, communications with the Centre and support from Line N officers; the vulnerabilities of the illegal, including tradecraft/operational failures.

Farewell: Penetration of KGB ST Operations 4

This module will focus on one of the most important penetrations of the KGB by Western Intelligence Services. The operation resulted in mass expulsions of KGB S & T officers for Western countries, the identification of numerous KGB penetrations in a variety of and the exposure of the massive scale and scope of KGB acquisition of classified Western technologies and scientific information. The FAREWELL's information became a "wake-up call" for Western counterintelligence.

KGB/SVR's Denial/Deception Operations 4

An advanced CI presentation covering the theory and the practice of Denial and Deception operations. Students will examine a series of complex KGB/SVR deception operations by a "special ad hoc unit" inside the KGB/SVR handling and attempting to protect the identities of CIA spy Rick Ames and FBI spy Robert Hanssen. In addition students will study the phased KGB operations to lure to Moscow and arrest several CIA/FBI sources inside their organization, their fate once back in Russia and the subsequent deceptions by the KGB to explain their disappearances.

Hunt for 3rd Mole in the USIC: The Robert Hansson Case 4

This presentation details the Brian Kelley - Felix Bloch – Robert Hanssen investigation. After the arrest of Aldrich AMES, the KGB spy inside CIA in Feb 1994, it became apparent that there another another "penetration" of the USIC. This module will tell the story of the initially misguided counterintelligence operation by the FBI which eventually identified Robert Hanssen, an FBI agent, and one of the most damaging KGB penetrations of the USIC, as the real mole.

Cuban Intelligence Operations that Target US 4

This module highlights espionage operations by the Cuban intelligence service (CIS) to penetrate the US agencies and military organizations. It will focus CIS recruitment techniques, intelligence tradecraft, and operational missions. The American counterintelligence response to the Cuban intelligence threat will also be considered.

Chinese Intelligence Operations and Tactics: PRC intelligence strategies, theories, tactics, agencies and operations from Sun Tzu (544 - 496 BC) to the Modern Era and Uighur terrorism in the western provinces of China.

British SIGINT: Bletchley Park to Cheltenham 4 From Enigma, ULTRA and the Battle for the Atlantic in WWII; to GCHQ's operations as a part of the counterterrorism campaign in Northern Ireland from 1968 to 1995; to the present technical

collection operations against Islamist Extremists, this module tells the story of British SIGINT operations, goals and strategies.

CIAT 2035 American Traitors "Insider Spies" 4 Dan/Rusty

There is no more serious threat to the USIC than the "Insider Spy". From Larry Wu-Tai Chin at the CIA, to Edward Snowden and NSA, this presentation overviews a broad range of American traitors who were trusted "Insiders". We will detail their profiles, their various motivations, the damage they caused and how they were eventually caught.

CIAT 2039 Capturing Jonathan Pollard 4 Dan/Ron Olive

This module provide significant detail on a major espionage case run by our ally, Israel, and the treason of a trusted insider, Navy counterterror analysts, Jonathan J. Pollard, who is due to be released from prison after serving 30 years in November, 2015. This story will give students an understanding of the damage done to our national security when security rules, regulations, policies and management of an employee's actions are misunderstood, misinterpreted, manipulated, or ignored.

Economic Espionage: America at Risk 4

An overview of the economic espionage threat to the US government and our private sector companies from our allies and adversaries. From Ancient China to the Industrial Revolution, to WWI and WWII, to the modern era we will examine how FIS, foreign companies, our allies and US companies target intellectual property and proprietary information. We will also look at the law and countermeasures to this threat

Role of Women in US Intelligence Operations 4

This module highlight the motivations, risk taking, sacrifices, contributions, and accomplishments of women in numerous strategic and tactical U.S. intelligence operations from the Revolutionary War to the modern era.

African Americans in US Intelligence Operations 4

A historical overview of the contributions to freeing a people and serving the intelligence profession out nation. The module will consider the complex issues of race, gender stereotyping and the motivations of African Americans from the Revolutionary War to contemporary times. It highlights the motivations, risk taking, sacrifices, contributions, accomplishments and betrayals of Africans in American history who have been invloved in both strategic and tactical intelligence operations.

Elicitation: 2

This presentation first illustrates how professional Foreign Intelligence Services [FIS] officers and their agents, as well as other-motivated individuals, elicit information from unwitting persons with access to classified or proprietary information. A variety of elicitation techniques and countermeasures will be discussed. This will assist participants in recognizing them and assist them in briefing individuals as to the potential treat from elicitation during interfaces at conference, conventions, trade shows, visit of delegation and other business/social occasions.

Agent Recruitment:**4**

Agent recruitment by a Foreign Intelligence Service (FIS) is a complicated flow of interrelated events leading to the establishment of a clandestine relationship. Most FIS agents “Volunteer”. Others are “Recruited by Design” or are Recruitments of opportunity”. This presentation will examine the process of targeting/selection/meeting/development/recruitment and handling of agents.

The Attempted Recruitment of a Military Attaché in Moscow, A Case Study: 4 hours

This case study considers an actual KGB recruitment operation of a US Military Attaché. Students will consider case facts, suggest possible recruitment strategies, learn what the Security Service actually accomplished, the reaction of the target to the tactics and the outcome of the events on the career of the officer. Lastly, students will compare and contrast this case with an MI-5 recruitment operation that almost brought down the British government of Prime Minister Harold Macmillan – The Profumo Affair of 1963.

The Evolution of OPSEC:**4**

Operational Security (commonly referred to as OPSEC) is more than a program – it is a state of mind. OPSEC is being implemented throughout the national and homeland security communities as a planning methodology vital to the success of securing homeland assets. It focuses on the protection of critical, but unclassified information that becomes advantageous in the hands of the adversary. This module will present the operating principles of OPSEC (including an overview of the five-step analytical OPSEC process), case studies, the history and success stories of OPSEC since the Vietnam War. It will explain how OPSEC can and should be integrated into all operations to provide effective protection of critical and proprietary information. The history, the process case studies and operations success stories of Operational Security since the Vietnam War

Cyber Crime Course:**4**

The history of cyber crime and the evolution of tactics, techniques, and procedures used by the adversary. How tradecraft has changed due to revolution of technology how computers, networks and technology have proliferated all aspects of daily life. Instructor will provide first-hand examples of cyber crime investigations based on 28 years of cyber crime investigative experience. The importance of digital forensics today to answer the traditional, who, what, when, where, why, and how questions that are critical to identifying the fingers on the keyboards and protecting public safety as well as protecting our national and economic security.

Cybersecurity:**4**

Real-world guidelines to protect you from cyber exploitation and protect your and you and the NSA from compromise. Real-world examples of how poor practices and lack of knowledge have led to individual and organizational victimizations. Explain the common exploits by the different perpetrators and the best common-sense procedures to follow to protect yourself and the NSA.

An Overview of Espionage Cases and Terror Threats in the Washington-Baltimore Metro Area: **3**

From the Cold War to the modern threat from home grown violent extremists. In this module we will cover FIS operations, espionage arrests and HVEs who have a connection to the local area. This will expand the student's awareness that espionage and terrorism happen here and awareness is a critical component of personal and Agency security.

Double Agent Operations: **4**

The theory and evolution of this effective and complex counterintelligence tactic from Sun Tsu in China in the Sixth Century BC, to the Double Cross System in WWII, to the use of double agents in Northern Ireland during the "Troubles" and finally their use in Afghanistan.

Security Awareness, CI and the Insider Threat: **4**

The threat to classified data, the types of collectors, their tradecraft, the CI tools to counter that threat. Role of education for professionals and awareness updating for employees on the current range of threats, particularly the threat from the trusted insider.

The Insider Threat, Leakers and Whistleblowers: **4**

Eric Snowden is just the most recent example of this phenomenon. This class will explore the stories of Army Specialist Bradley Manning who gave classified data to WikiLeaks; Former State Department arms expert Stephen Kim, retired Marine Gen. James 'Hoss' Cartwright is the 'target' of a probe into leaked Stuxnet cyber-attack on Iran; and Daniel Ellsberg who leaked the Pentagon Papers during the Vietnam War. We will also consider the controversial tactic of the government targeting of the Media and reporters to identify leakers and consider countermeasures and CI investigative tradecraft.

Counterterrorism Courses:

Travel Safety in High Risk Countries **4 hours**

Students will learn the size, scope and character of threats to their personal safety while in a travel or PCS status. They will also be provided with the required knowledge and skill sets to avoid/minimize risks and incidents. This module will lower personal risk profile of students, increase their ability to recognize imminent threats, learn how to avoid, minimize or manage potential threats and will provide practical, common-sense advice and safety tips covering all modes of travel and accommodations.

Generation III Counter Terror Response **3-days**

This module considers the use of counterintelligence tradecraft in counterterror operations. Students will examine the critical importance of intelligence in CI and CT operations from the

examples of Mossad's operations against the Black September terror group after the attack on Israeli athletes at the 1972 Olympics. Student will learn about several complex forms of CI tradecraft including: the use of agent networks; defectors, double Agency; and countering illegals and terrorist sleeper cells.

(The following are 3, half-day, classes that form the basis for the 3-day class on Generation III Counter Terror Response above)

CI and Terror 1: Theory and Evolution of Terror **4**

This module is an overview of terrorism from the French Revolution to the present. It provided an in-depth look at the evolution of the terror threat prior to a student's future study of the counterintelligence tradecraft that are used in counterterror operations (CI and Terror 2 and 3). In this module Students will explore developments in the last 200 years of worldwide terror attacks including: Sun Tzu on intelligence, CI and terror; the French Revolution – “The Terror”; idols, leaders and mentors of modern day terrorists: IRA terrorist Michael Collins; the major causes of Near Eastern terrorism and the origin of the Israeli – Palestinian conflict; the terror paradigm shifts again: the attack on the Munich Olympic games in 1972; the 4 world events that changed international terror forever; the raid on Abbottabad and the death of bin Laden; Terror today and tomorrow – the Islamic State and HVEs.

CI and Terror 2: Basic CI Tradecraft used in CT Ops **4**

An overview of the basis counterintelligence tactics and tradecraft used in modern counterterror operations. Topics considered: CI theory and mission; Mossad operations following the attack on the Munich Olympics; CI advantages and the CI Team; the role of the CI case officer; agent/informant networks; interview and interrogation in CI; elicitation and recruitment; surveillance; and analysis in CI operations.

CI and Terror 3: Advanced CI Tactics used in CT Ops **4**

An overview of the advanced counterintelligence tactics and tradecraft used in modern counterterror operations. Students will explore advanced counterintelligence tradecraft and numerous recent terrorist attacks to better understand the critical role of CI in modern counterterror operations. Topics include: training/professional education of CI/CT officers; value of public awareness programs; use of informant networks; penetration of Internet chat rooms; Covert Operations – directed assassinations and cyber-attacks; use of SIGINT and IMINT in CT; Double Agent operations against terror groups; British counterintelligence tactics used in the “Troubles” in Northern Ireland.

Terrorist Attacks and Survival Skills **8**

This module considers the Tactics, Techniques and Procedures (TTP) of terrorist groups around the globe. It also identifies for the student proactive target hardening and countermeasures to terror attacks, including escape, evasion and other survival skills. Also, a wide spectrum of attack methodologies will be covered, from the collection of initial intelligence on potential targets, to actual target and site selection, to the surveillance(s) of the target, through the attack and escape route used by the assault group.

International Terror Group Ops. in the US**4/8 hours**

The module will consider the long history of international terror group intelligence collection, recruitment of new members, fund raising efforts, logistical support activities and terror operations in the US. Among the numerous groups and operations covered will be: Anarchist attacks 1900 through WWI; Armenian terror group attacks in the US from 1973-1986; the first attack of the World Trade Center in 1993; the al Qaeda attacks on September 11, 2001; and subsequent lone wolf/HVE attacks by the Islamic State.

The Road to Radicalization**4**

This module will consider the motivations, the profiles and predictors of terror. Using the data compiled by doctors Marc Sageman and Louise Richardson students will explore the myths about why young men and women become terrorist, what are the real motivations to terrorism, how terrorist recruitment works and some countermeasures to the process of terror recruitment.

The Concept of Leaderless Resistance**4**

This module will define the concept of “leaderless resistance” and apply it to both domestic and international terror groups and their operations. We will also examine numerous cases of individual and small cells of “lone wolf” terrorists and “home grown violent extremists” (HVEs) and consider several countermeasures.

Middle Eastern Intel. Services**4**

This course is an overview of the organization, goals, mission, history, major cases, tactics and tradecraft of the intelligence services of the Middle East. Intelligence service considered will be Egypt, Syria, Jordan, Iraq and Saudi Arabia.

Allied Intelligence Services - Israel**4**

An overview of the history, strategy and tactics of two of the most effective security services in history, Mossad and Shin Bet. This module will tell the story of how intelligence and counterintelligence has been successful deployed to protect Israel from foreign intelligence collection and terrorist attacks.

Israeli Behavior Pattern Recognition Technique**8 hours**

This module will focus on understand the mindset of a terrorist. It is taught by a former Shin Bet officer and considers Israeli tactics used in counterterror operations. Topics: the pre-attack terrorist mind set; terrorist’s surveillance methods; handling a suspicious situation; interrogation methods to detect deceit in field; observing a crowd looking for abnormal behavior; the differences between interrogation and questioning; how to be vigilant to the small details; analyzing the situation based on appearance, answers, character, and timing.

Israeli Intelligence Gathering Techniques**2-days**

In this module students are taught by a former Israeli Security Service officer the techniques used by that service to investigate, preempt and disrupt terrorist attacks. Topics: the Muslim cultural perspective; sources and liaison recruitment techniques; ways to maintain lines of communication into the local community; assessing and monitoring extremists and their sympathizers; a table top exercise to practice knowledge, skills and techniques taught in the class.

The Anatomy of a Terror Attack

4

This module considers the operational challenges that faced the terrorist cell in the planning and execution of the bombing of the World Trade Center in 1993. Students will also study the post attack investigation by law enforcement agencies, the preparation of the case for trial, the court proceedings and sentencing of the terrorists involved with the goal of giving students a better understanding of the complexity of terror attacks, terror countermeasures, lessons learned and how terrorists are prosecuted.

Connecting the Intelligence Dots in the September 11, 2001, attack by al Qaeda on America:

4

Students will be exposed to a detailed examination of the evolution of al Qaeda operations in America and against America around the world. Focus will include the intelligence currently in the public domain which was available to the US Intelligence Community prior the 9/11 attack and if collated and analyzed could have identified and located many of the 9/11 hijackers.

Al Qaeda Penetrates the US Army

4

This is the story of Ali Mohamed: former Egyptian major, US Army sergeant, CIA source, FBI Informant, terrorist trainer for the cell that bombed the World Trade Center in 1993 and al Qaeda double agent who penetrated the USIC. This case illustrates al Qaeda's resourcefulness and patience in their intelligence operations targeting America. It also identifies holes in the American counterintelligence responses as this complicated and complex terrorist double agent operation unfolded in America and abroad.

Bin Laden: Birth to Abbottabad

4

Osama Bin Laden, the 50 million dollar man: his life, his belief, his motivation, the threat he represented and the evolution of his organization - al Qaeda. This module will look in great detail at worldwide al Qaeda operations, the intelligence that preceded the 9/11 attacks, the counterterror responses to the man and his organization and the intelligence that led to his death in Abbottabad in 2010.

Domestic Terrorism in America

4/8 hours

This module has been designed to give students a broad understanding of the role of violence and terror in the history of America from colonial times to the present. Students will be shown the tactics and operations of modern domestic terror groups and given strategies to counter these threats:

- Right wing terror groups from the 4 iterations of the Ku Klux Klan.
- The evolution of the Christian Identity Movement.
- The explosion of state Militias.
- The role of criminal gangs in terrorism and their connections to international terror groups.
- The anti-abortion terror groups.
- The Puerto Rican terror movement.

The Sovereign Citizens Movement

4

This module considers the most dangerous domestic terror threat to America - the Sovereign

Citizen's Movement (SCM). The SCM is responsible for the death of almost 40 law enforcement officers in the last 20 years and still the mainstream Media and many Americans are unaware of the threat posed by this group. Topics covered: The confrontation at Ruby Ridge, Idaho in 1992; the Rocky Mountain Rendezvous; the 50-day Branch Davidian siege at Waco; the bombing of the Murrah Federal Building; the May 20, 2010, killing of two police officers in West Memphis, Arkansas, the Sovereign Citizen belief system, philosophy and "*paper terrorism*."

Women in Terrorism: An overview of the role of women in terror groups from the Roman Empire to the Islamic State. The course highlights the evolution of female participation in the world's terror groups, their operations, world events, terror attacks and counterterror cases which illustrates their motivations, risk taking, sacrifices, contributions, and accomplishments during more than two millennia of terrorism.

Overview of World Terror Groups and Threats: 4

Evolution, tactics and threats from terror groups from Asia, Africa, the Near East, Europe and the Americas

Professional Skills Training: Interviewing and Interrogation:

Nonverbal Communication for CI Professionals 8

Nonverbal clues to communication surround us but without training we often miss them. In this module students will be given training in techniques to recognize the clues in a broad range of communications, both in themselves and in others. Topics: personal space; facial clues; posture; gestures and movements; cultural considerations.

Nonverbal Clues to Stress for CI Professionals 4

Indicators of stress and deception are not always apparent. Through directed training and practice, these indicators become more obvious and can lead an investigator to the truth. In this module we will cover: establishing baseline behavior; truthful clues and illustrators; clues to stress and deception; involuntary physiological changes; subconscious physical responses.

Behavior Styles for Security Professionals 4

This module will focus on the identification of primary and secondary Behavioral Styles and examine how these preferences affect behavior. The primary goal of the class is to assist security and CI professional in the identification and manipulation of personality styles in interviews, interrogations and asset development.

Nonverbal Stress and Deception 4

Indicators of stress and deception are not always apparent. Through directed training and practice, these indicators become more obvious and can lead an investigator to the truth. In this

module participants will be taught to identify the basic five involuntary physiological changes in an individual under stress. Topics: establishing baseline behavior; truthful clues and illustrators; clues to stress and deception; involuntary physiological changes; subconscious physical responses.

Interpersonal Communications for CI Professionals 4

Counterintelligence and Security Professionals will gain communications skills to enhance their interaction with others. Too often we have no idea what we look like to others, and how our interpersonal communication skills affect our communications, for better or worse. This module will assist student with the matching of their nonverbal with their vocals and emotions.

Investigative Interviewing: Uncovering the Truth 4

Too often the truth remains hidden from investigators. This module will assist them in learning to use effective questioning techniques and rapport-building strategies to uncover the truth. Topics: removing roadblocks; going beyond rapport; questioning techniques that work; closing the deal; gaining the corroborating details.

Advanced Investigative Interviewing 8

In this module student will use investigative interviewing techniques to uncover the truth hidden by uncooperative individuals. Topics: removing roadblocks; going beyond rapport; questioning techniques that work; closing the deal; gaining the corroborating details.

Introduction to Statement Analysis 4

Through structured analysis of a statement, an investigator can gain critical insight to conduct a successful interview. Participants in this module will apply a structured method of analyzing spoken and written statements to identify areas of stress and deception. Major topics covered in course: clues to veracity in statements; clues to deception in statements; areas of insight in statements

Statement Analysis II 8

Through structured analysis of a statement; the investigator can gain critical insight to conduct a successful interview. Participants will apply a structured method of analyzing spoken and written statements to identify areas of stress and deception. Topics: methods of obtaining uncontaminated statements; clues to veracity in statements; clues to deception in statements; areas of insight in statements; using the analysis to conduct an effective interview

Advanced Statement Analysis 16

In this module students will apply a structured method of analyzing spoken and written statements to identify areas of stress and deception. Through case studies, intermediate students will reinforce skills learned. Topics: methods of obtaining uncontaminated statements; clues to veracity in statements; clues to deception in statements; areas of insight in statements; written statement case studies; using the analysis to conduct an effective interview.