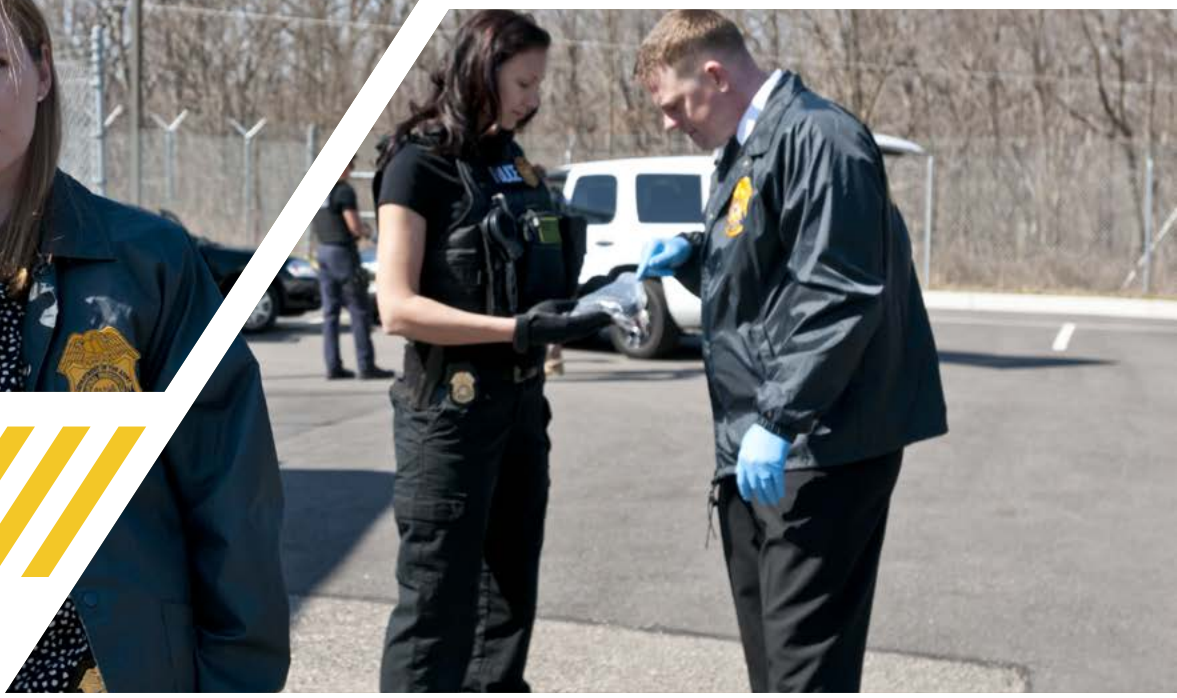
CID

ARMY CRIMINAL INVESTIGATION DIVISION

2022-2023 YEAR IN REVIEW




DEPARTMENT OF THE ARMY
CRIMINAL INVESTIGATION DIVISION
1775
SPECIAL AGENT

WELCOME

MESSAGE FROM THE DIRECTOR

I am pleased to share the 2022-2023 Army CID Year in Review. This is the first edition of what will be an annual product designed to highlight the tremendous efforts of the CID workforce. This document includes summaries of investigations, initiatives and key achievements that are representative of the work done to reduce harmful behaviors and maintain the warfighting readiness of the Army.

We are now in year three of the CID transformation and it is important to acknowledge the progress achieved, to date, as we strive to provide superior Military Criminal Investigative Organizational support to the Department of the Army. The organizational structure of the agency has been completely redesigned to better align with our federal law enforcement counterparts, which has enabled the development of stronger partnerships and better investigative outcomes. CID's operational leadership structure now includes experienced criminal investigators at every level. This ensures we remain focused on core MCIO activities, as well as the unique professional development and equipment needs of our workforce.

The agency has been infused with diverse experience through the hiring of civilian special agents from a variety of backgrounds, to include from our active duty agent corps and a multitude of criminal investigative agencies. This led to an increase in the skill sets, critical to a federal criminal investigative agency and the ability to benefit from the best practices of partner agencies throughout the government. We continue to align our policy with industry standard investigative protocols, encourage investigative curiosity, initiate investigations based on the allegation and the Army nexus and have raised the performance expectations for the entire workforce in order to provide the level of service the Army requires of CID. While the difference is evident to those within the organization, as well as to external stakeholders, we still have a long road ahead of us.

Like the Army at large, CID is facing an ever challenging and complex world. Whether an investigation or operation involving narcotics or homicide; sexual assault or cyber intrusion; logistics security or fraud; robbery, domestic violence, or criminal threats to the Army supply chain, our personnel and the proper execution of the CID mission are critical to the success of the Army and the United States as it faces sophisticated criminal and cyber actors, violent crime, terrorist and insider threats, along with criminal actions committed by or on behalf of foreign adversaries. To combat these challenges, we must continue the progress we've made with outfitting the workforce with the equipment and training needed to safely and efficiently conduct investigative steps and execute enforcement actions. We will also continue to modernize how we approach the mission, further integrate with the law enforcement community and pursue operational excellence.

Director, Department of the Army CID


USACIL

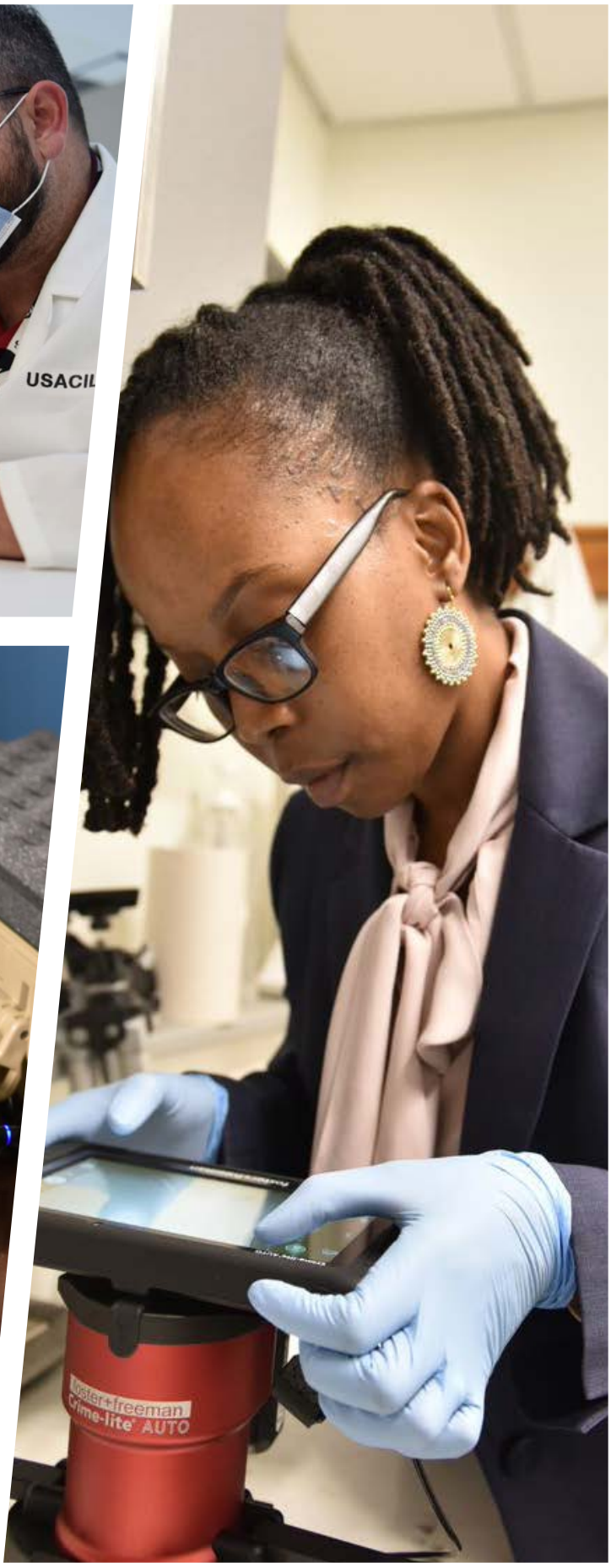
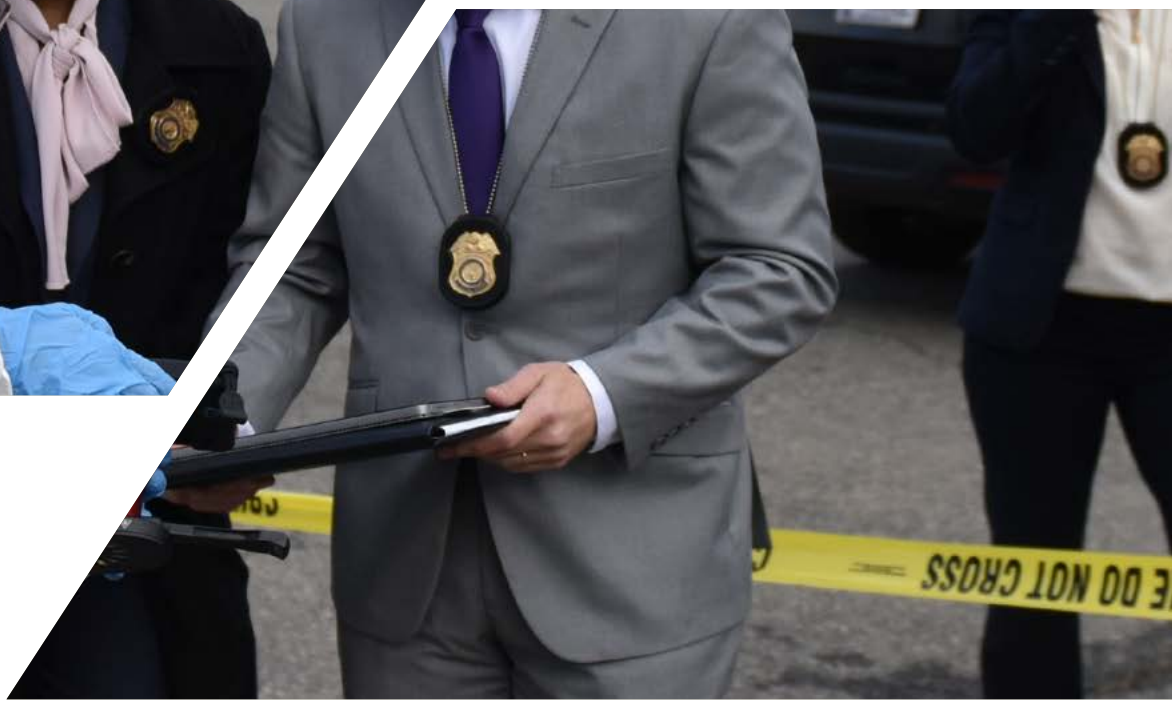

foster+freeman
Crime-lite® AUTO

TABLE OF CONTENTS

SECTION 01

INTRODUCTION



Mission Overview

The Department of the Army Criminal Investigation Division is an independent federal law enforcement agency free from undue command influence with nearly 3,000 personnel assigned to 124 locations around the world. The Department of Defense's military criminal investigation organization (MCIO) triad, which includes the Naval Criminal Investigative Service, the Department of the Air Force Office of Special Investigations, and ourselves, is housed at our headquarters in Quantico, Virginia. In contrast to our colleagues at OSI and NCIS, Army CID does not have primary counterintelligence responsibilities.

Our primary mission is investigating felonies affecting our Soldiers, their families, Army civilians and the Army's warfighting assets. Our civilian special agents, as sworn federal agents and federal criminal investigators, have both federal statutory authority (Title 10 U.S.C. Section 7377) to enforce all federal laws anywhere in the United States and military authority to enforce violations of the Uniform Code of Military Justice (UCMJ). These agents can investigate all felony crimes affecting the Army regardless of location with full authority to seize evidence and bring either military or civilian subjects to the appropriate military or civilian judicial system for prosecution.

As an MCIO, Army CID is the executive agent for the DOD's executive protection mission providing security and protective service operations for the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, Secretary of the Army, the Army's Chief of Staff, and other high-risk personnel. Army CID is also the executive agent for the DOD's only full-service, forensic crime lab, the U.S. Army Criminal Investigation Laboratory in Georgia

With more than 12,000 investigations annually, we partner with other law enforcement agencies to combat fraud, narcotics, sexual assault, cyber-crime, and other criminal threats directed at the Army by gathering and analyzing criminal intelligence to protect the warfighter. From drug suppression efforts to recovering stolen, sensitive warfighting equipment, Army CID reduces harmful behaviors affecting our Soldiers and greatly enhances total Army readiness.

Some of the Felony Crimes Investigated by CID:

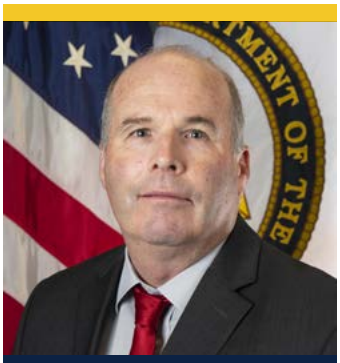
- Medically unattended/unexpected deaths of Army affiliated personnel
- Sexual crimes
- Crimes against children (physical and sexual abuse; exploitation)
- Cyber intrusions and cyber enabled crime
- Terrorism
- Law of armed conflict violations/war crimes
- Property theft (focus on sensitive equipment such as arms and ammunition)
- Domestic violence
- Financial fraud
- Procurement fraud
- Threatening communications
- Aggravated assault

Other Responsibilities:

- Collect, analyze, fuse and disseminate criminal intelligence
- Conduct protective service operations for DOD and Army senior leaders
- Provide full spectrum criminal forensic laboratory support to the DOD
- Manage all Army law enforcement records
- Protection of Army logistics pipelines
- Liaison with local, state, other federal and foreign law enforcement counterparts on functions falling under Army CID purview
- Polygraph Examination
- Crime scene processing and documentation
- Cold Case Program
- Behavioral Analysis Unit
- Protective Intelligence

Executive Leadership

Gregory Ford
Director



Robert Tracy
Deputy Director

Karen Spidell
Chief of Staff

AGENCY ASSISTANT DIRECTORS

Peter Tolentino
Assistant Director
Investigations & Operations Directorate

Adnardo Garcia
Intelligence & Analysis Directorate

Debra Glidewell
Criminal Investigation Laboratory

Michael Kowalski
Human Resources Directorate

Marc Martin
Cyber Directorate

Seldrick Moore
Protection Directorate

Caroline Frye
Business Operations Directorate

Edward LaBarge
Technology & Capabilities Development Directorate

FIELD OFFICES SPECIAL AGENTS-IN-CHARGE

Shane Watts Carolinas Field Office	Ryan O'Connor Central Field Office	Maria Thomas Central Texas Field Office	Paul DelleDonne Cyber Field Office
Ryan Hall Europe Field Office	Seldrick Moore Executive Protection Field Office	Michael DeFamio Far East Field Office	Keith Kelly Fraud Field Office
John McCabe MidCentral Field Office	Joel Kirch Northeast Field Office	Ruben Santiago Pacific Field Office	Ahmed Salem Special Investigations Field Office
Steven Ausfeldt Southeast Field Office	D. Todd Outlaw Southern Field Office	Olga Morales Southwest Field Office	
Jacob Cameron Washington Field Office	Michele Starostka Western Field Office		


SPEER
9mm LUGER


2

Personnel Overview

Army CID is a complex organization which relies on a diverse, highly skilled workforce. From Special Agents and Forensic Scientists to Cyber Investigators and Human Resources, all of our personnel play a critical role in helping the Army maintain operational readiness.


T-1954


4

SECTION 02

MISSION AREAS

Investigations & Operations

The Investigations & Operations Directorate (IOD) provides direct oversight for all criminal investigations for Army CID. IOD coaches, teaches and trains Agents at all levels. Direct support is provided to all CID Agents by means of Family and Sexual Violence, Polygraph Examination, Forensics, Technical Services, Cold Cases, National Security, Economic Crimes, Property Crimes and Death investigations.

IOD continues efforts to establish a highly trained cadre of investigative personnel and professional staff dedicated to ensuring the safety of Army personnel and their families. Focus areas include proactive engagement both internally within CID and externally with our law enforcement partners. Combating crime committed by or against Army-affiliated personnel that has or may result in harm to the physical or emotional well-being of an individual or organization continues to be IOD's top priority.

IOD FUNCTIONAL SECTIONS AND PROGRAMS:

- **Special Operations Division**: Conducted extensive training in use of force, along with weapons training. IOD policy has established several critical updates and has provided a framework to create effective policy during the upcoming year.
- **Death and Violent Crimes Section**: Developed the Field Office Death Review Panel and IOD HQ Death Review Board processes for examining death investigations to ensure investigations are conducted in accordance with CID policies and procedures. The real-time feedback and discussion assist agents in the field by conducting thorough and complete death investigations, to include arranging immediate support from outside subject matter experts (i.e. anthropology, toxicology, entomology, etc.). Cases are looked at in their entirety prior to closure, to ensure all investigative steps have been completed.
- **Forensic Training**: CID increased the crime scene response and forensic techniques training provided to agents in the field. This additional training increases capabilities at all levels and ensures they are available on scene. Internally, the section has developed two training programs for the field. The first training program reaches the Assistant Special Agents-in-Charge/ Supervisory Special Agents level with capabilities awareness and leadership topics and the second program touches the Forensic Science Consultant and Forensic Science Technician personnel for sharing best practices and new technology.
- **Cold Case Unit**: This newly established unit works with the field to provide direct forensic, genealogical and investigative support on unsolved cases to ensure that every effort is made to provide closure to the families of those lost.
- **Family Liaison Program**: This program engages directly with the unit Casualty Assistance Officer, case agents and field office leadership to ensure families of decedents are kept abreast of the cases throughout the investigative process to include navigating the request of investigative documentation through the Freedom of Information Act.

- **Family and Sexual Violence Section**: This section conducts oversight, training, and assistance in the application of any changes in law or standards for all sexual assaults, in addition to all family violence cases and ensures compliance with all applicable Department of Defense instructions, placing emphasis on timely and thorough investigations.
- **Behavioral Analysis Unit**: This special unit supports the field with analysis of 911 calls, viewing interviews and providing advice in criminal investigations. Further, the unit established Behavioral Threat Analysis Teams which consists of trained individuals from each field office to respond to situations with individuals in crisis across the Army to mitigate threats and preserve life.
- **Wellness Section**: The primary function of this section is to provide assistance and resources to agents across CID in the aftermath of traumatic cases or situations.

EVIDENCE RESPONSE TEAMS

CID established Evidence Response Teams (ERT) at each field office with specialized equipment and uniquely trained personnel and is working to standardize. ERT guidelines for response and documentation. These multidisciplinary teams will respond to on- or off-post incidents that involve Department of the Army personnel and/or their dependents.

COMPUTER STATISTICS PROGRAM (COMPSTAT)

COMPSTAT fosters agency-wide accountability. Field office leadership teams are responsible for knowing the details of criminal trends in their areas of responsibility that have relevance to the Department of the Army and devising plans to effectively investigate those crimes. Likewise, CID leadership and support directorates gain a better understanding of each field office's operating environment and resource needs. COMPSTAT encourages a shared responsibility for learning and information sharing to continuously improve the quality of investigations and operations. COMPSTAT allows agents to take rapid action to resolve any challenges, establishes 360 accountability and allows for quickly reallocating resources to address priorities, and creating opportunities to reduce crime. It also facilitates the identification and implementation of best practices across CID and the Army law enforcement community.

COMPSTAT represents a deviation from previous oversight processes. It generates mutual understanding between CID leadership and field offices, along with an open dialogue meant to inspire healthy, professional exchange of information focused on a whole-of agency approach to continuously evaluate and improve investigative processes and procedures to increase operational efficiency.

Investigations by Serious Crime

2022 & 2023 Investigations Breakdown *Information listed below are offenses that are the case counts categorized by the most serious offense per record of investigation (ROI).*	# Initiated 2022	# Initiated 2023
Death Investigations	**400**	**515**
Suicide	124	146
Undetermined Manner of Death (majority are open cases pending autopsy results)	108	176
Murder	50	65
Accidental Death	52	48
Death by Natural Causes	30	50
Involuntary Manslaughter	6	3
Negligent Homicide	18	14
Voluntary Manslaughter	3	1
Homicide	0	2
Traffic Fatality	7	9
Sudden Unexplained Infant Death Syndrome	2	1
Sexual Assault Investigations	**3,621**	**4,092**
Penetrative	2,248	1,968
Non-Penetrative	1,373	2,124
Domestic Abuse/Violence	**1,679**	**2,112**
Aggravated Assault	477	656
Assault and Battery	463	522
Sex Crimes	364	476
Other Sex Crimes	143	158
Family Abuse/Domestic Violence	122	155
Child Abuse/Neglect/Endangerment	47	56
Homicide	25	27
Kidnapping	20	36
*Other Non-Violent Felonies	16	18
*Other Non-Violent Felonies include Stalking & Communicating a Threat Note: Offenses are the most serious offense per ROI.		
Fraud Investigations	**273**	**576**
Drug Investigations	**5,967**	**4,975**
Protective Order Issued (Military & Civilian)	**1,244**	**943**

Support Operations in Europe

To better equip and support joint operations inside Eastern Europe and NATO, the Army has strengthened its presence throughout Europe. Supporting joint training exercises with Allies and creating a permanent presence in Poland have increased the cost of conducting operations and the need for supplies and equipment. The risk of criminal activity has increased due to this development.

CID conducted proactive efforts to further mitigate potential criminal activity within the European Theater to include procurement fraud, counter narcotics, cyber and logistics and supply chain investigations in addition to other criminal activities involving U.S. Army personnel and interests.

PROCUREMENT FRAUD: Given the increase in contracting required to support operations within the European theater, the Major Procurement Fraud Field Office has increased its involvement ensuring acquisition integrity is not compromised by criminal activity involving corruption or other procurement criminal offenses such as false claims. Efforts are also being taken to ensure theater level logistics are not compromised by activity directed at disruption, theft, or diversion of critical resources, by obtaining criminal intelligence and providing supported commanders with recommendations to mitigate potential criminal activity.

LOGISTICS SECURITY (LOGSEC): Since 2022, the Europe Field Office (EUFO) has continued to expand and strengthen Logistic Security support for Army Commands across Europe, the Middle East, and Africa. EUFO completed four LOGSEC threat assessments for installations in three separate countries. By completing crime prevention surveys and partnering with stakeholders, EUFO prepared holistic reports for commands to mitigate a wide range of threats to supply chains and access control programs. During this period, EUFO LOGSEC agents provided support to USAREUR-AF contingency operations, notably the Africa Lion exercises in 2022 and 2023, along with consultation support to CID CENTCOM as part of a LOGSEC-related criminal investigation. EUFO LOGSEC has established enduring partnerships with various commands: USAREUR-AF, 21st Theater Sustainment Command, Army Medical Command, the Surface Deployment Distribution Command, Military Sealift Command, Department of State and U.S. Embassy partners across its vast area of responsibility.

IOD FRAUD/PROPERTY: CID continues to support European Operations leveraging expertise and facilitating working relationships with the Department of Justice, Defense Criminal Investigative Organizations, audit, acquisition and sustainment communities internal and external to the Army.

GLOBAL STRATEGIC OPERATIONS: Given Europe's expansive footprint, CID has further established a global engagement liaison position which continues to promote CID capabilities, establishing relationships with supported embassies and NATO allies and partners.

EUROPE FIELD OFFICE: CID continues to support Army operations in locations such as Africa and Poland with an emphasis on establishing and building working relationships with host nation law enforcement. Establishing interagency support has improved postured CID to provide efficient investigative support, leveraging resources and relationships when Army interests are involved. Crime prevention efforts continue through awareness training on crime trends identifying vulnerabilities which create conditions conducive to criminal activity.

Victim Centered Agency

The transition of the Army Criminal Investigation Division (CID) into a Victim-Centered Agency (VCA) transcends compliance with Section 549C of the National Defense Authorization Act (NDAA) for Fiscal Year 2022 (FY22); it embodies an ethical imperative. This strategic shift is rooted in a conviction that upholding justice and enhancing the welfare of individuals impacted by crime is a reflection of our unwavering commitment to elevating the standards of care, dignity, and respect for victims. This signifies a profound responsibility to not only investigate but to heal and protect. Through this initiative, we are embracing a culture of empathy and integrity, ensuring that our actions align with the highest principles of honor and duty.

WHY BECOME A VCA?

The intentionality behind CID's evolution into a VCA is multifaceted, anchored in the nature and volume of its cases which predominantly encompass crimes against persons, such as sexual and domestic violence offenses, drug-related crimes, as well as death and child abuse investigations. Annually, CID handles more than 12,000 investigations, each demanding advanced investigative techniques and extensive resources. The violence inherent in these crimes not only constitutes a public health crisis but also significantly undermines the readiness and well-being of Soldiers, their families, and civilian personnel.

The immediate aftermath of a crime is pivotal in shaping a victim's recovery trajectory. Law enforcement officers, often the first point of contact for victims, possess a critical opportunity to positively influence the victim's coping mechanisms. By adopting a victim-centered approach, CID can ensure interactions with victims preserve their dignity, avoid re-traumatization, and prioritize their safety, rights, and well-being. This approach necessitates a keen understanding of the victims' needs and preferences throughout the investigative process.

GOALS OF THE VCA

The principle goal of a VCA is to help restore victims' sense of security and autonomy, which is crucial to their healing and recovery. Embracing trauma-informed care placing victims' needs at the forefront of investigative efforts not only aids victims in reconstructing their lives post-trauma but fosters greater trust, confidence, and fidelity in the military criminal justice system. This transformation is a profound shift towards a more empathetic, effective, and ethically grounded approach to criminal investigation within the military, reflecting a broader commitment to the welfare and dignity of all individuals impacted by crime. The VCA initiative is not only a strategic response to legislative guidelines but reflects CID's commitment to justice, empathy, and the well-being of the military community. The success of this initiative will serve as the premiere example for other law enforcement agencies to adopt a more considerate, victim-centered approach to criminal justice.

Suicide Prevention Efforts

In 2022, there were 11 incidents where CID contributed to locating service members (SM) safely returning them to military unit custody without self-harm. There were eight incidents in 2023. Four incidents are highlighted below.

INCIDENTS

ARMY CID NOTIFIED OF A MISSING SERVICE MEMBER

In October 2022, SM was reported missing formation and sent a concerning text message to his soon to be ex-wife referencing his life being worth $400,000 (SGLI payout amount). The spouse related she knew SM had three weapons, which were physically with her; however, there was a concern he may have had a fourth weapon. Initial CID attempts to geolocate SM's phone met with negative results. A BOLO for the SM was distributed. Subsequent CID efforts to geolocate SM's cellphone concluded the SM might have been in a local hotel. CID confirmed the SM was lodged at the hotel and attempted to contact the SM via cellphone, while simultaneously surrounding the area of his hotel room. CID was able to coax the SM out of his room and safely take him into custody.

BARRICADED SERVICE MEMBER ARMED WITH AN AXE WANTING TO CAUSE SELF-HARM AT ON-POST RESIDENCE

In December 2022, Army CID crisis negotiators contacted SM, who indicated he was experiencing relationship issues with his spouse, was armed with an axe and wanted to cause self-harm. The SM also stated he wanted to be shot in the head or he would hurt the responding agents. During communication with CID, it became apparent the SM was heavily intoxicated. After approximately 15-20 minutes of negotiation, SM voluntarily exited the residence. As he exited the residence, nonlethal tactics were used by CID to take the SM to the ground. He was ultimately subdued, evaluated by EMS and transported to the hospital for psychological evaluation.

SERVICE MEMBER REPORTED MISSING UNDER SUSPICIOUS CIRCUMSTANCES

In May 2023, SM's unit reported it had not spoken to, or physically seen, SM in several days. SM's girlfriend discovered a suicide note SM left behind after they recently ended their relationship. She knew he was driving around the local area talking to his therapist on the phone. CID pinged the SM's phone, which geolocated to a local wooded area, wherein CID responded. SM's girlfriend revealed SM had a storage unit near the area. CID sent Soldiers to search the storage unit and surrounding area. Shortly after, SM was discovered alive in his vehicle. At the time, it was not certain whether the SM was in possession of his weapon. CID and Harnett County police approached the vehicle and talked to SM through a rolled-down window. SM stated he was tired and wanted to sleep, rolled up his window and ceased communication. CID took the opportunity to open the door, escort the SM out of the vehicle and render the situation safe. After the incident, the SM was transported for medical evaluation.

SERVICE MEMBER BARRICADED IN A BARRACKS ROOM THREATENING TO KILL HIMSELF.

In April 2023, a SM under investigation for possession of Child Sexual Abuse Material (CSAM) and Abusive Sexual Contact was under unit supervision, due to previous suicidal ideations, when he went into the latrine and returned disrobed and with a knife to his neck. He subsequently barricaded himself in a barracks room and threatened to kill himself with the knife. CID responded, took control of negotiations and successfully de-escalated the situation resulting in SM voluntarily relinquishing the knife. After the incident, the SM was transported for medical evaluation.

Cyber Directorate

Cyber Directorate (CYD) conducts worldwide cybercrime prevention activities, major cybercrime investigations and digital forensics in order to preserve Army readiness. The CYD is focused on three separate but related areas. Cyber investigations which are handled by the Cyber Field Office, digital forensics conducted by certified forensics examiners and cyber program management and liaison activities.

INVESTIGATIVE HIGHLIGHTS

PARTNERSHIPS & ENGAGEMENTS (P&E)

The CYD P&E located at Quantico, Virginia, provides support to the CID field offices and other CID elements around the world. The CYD is a small element comprised of liaison officers positioned at different external partner organizations, to include: U.S. Army Cyber Command Fort Eisenhower, Georgia; U.S. Cyber Command, Fort Meade, Maryland; National Center for Missing and Exploited Children, Alexandria, Virginia; National Cyber Investigative Joint Task Force, Chantilly, Virginia and the Homeland Security Investigations Cyber Crimes Center, Fairfax, Virginia. These strategic partnerships provide immediate integration with Army, DOD and other national-level agencies to deliver timely identification, deconfliction and investigation of existing and emerging cyber threats related to Army readiness.

CYBER DIRECTORATE FORENSICS

The cyber forensics team provides programmatic oversight and supervision of the CID digital forensic program which includes nine regional digital forensic examiner (DFE) cells and the Digital Forensic Research Branch (DFRB). Since consolidating the DFE Cells under the Cyber Directorate in early 2022, the turnaround times for forensic examinations have been cut in half from 100+ days to slightly more than 50 days. This reduction in turnaround times was directly related to the ability to retain talented digital forensic examiners leaving military service along with hiring experienced examiners from other organizations. The Cyber Directorate expanded access to mobile device extraction tools and provided training to almost 150 non-cyber CID agents in advanced extractions. With more than 400 hours of training conducted in the last fiscal year, digital forensic examiners enhanced the cyber literacy of the agent workforce. The digital forensic enterprise will add four new DFE cells and will increase strategic locations to support CID investigations.

ONLINE SAFETY AND CHILD ABUSE PREVENTION

During 2022, the Cyber directorate led a whole of CID effort designated Operation Red Light driven by the CID liaison to the National Center for Missing and Exploited Children (NCMEC). This effort involved briefings to CID field office personnel to incorporate materials developed by NCMEC to further educate Army and DOD community members about issues related to child online safety and abuse to bring awareness about sextortion.

In 2023 CYD adopted the NCMEC ambassador program to continue Operation Red Light by providing better uniformity on educational materials distributed by CID on behalf of the NCMEC's NetSmartz program for children and families.

CYBER PROTECTION TEAM AND ASSESSMENT TEAM (CPAT) EFFORTS

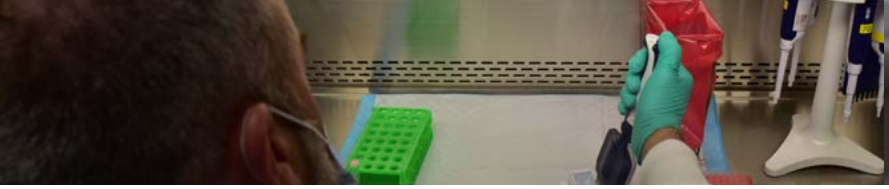
During 2022 and 2023, the Cyber directorate team partnered with the Headquarters Department of the Army mission assurance assessment team to provide cyber vulnerability assessments at 16 mission critical locations around the world. These mission assurance assessments are conducted on activities identified as critically important to the U.S. Army mission where their failure would result in the mission failure for the Army. Deficiencies are directly presented to senior Army and DOD leadership for remedial actions.

CYBER DIRECTORATE INTELLIGENCE DIVISION

This directorate provides criminal intelligence support to the cyber field office, the digital forensics program and the other CID field offices through requests for assistance. Additionally, the CYD Intel Division regularly produces cybercrime prevention flyers discussing a range of topics: scam awareness, email safety, wireless home network security, tax season cyber fraud, mobile device protection, malware and combatting online sexual exploitation of children.
Learn more at: cid.army.mil/Resources/Cybercrime-Prevention/

Students and staff were given a live demonstration of digital forensic techniques used by law enforcement as part of a community outreach program by Supervisory Special Agent Mike Roelofs from CID's Cyber Directorate, Internet Crimes Against Children.

SSA Roelofs talked about working in federal law enforcement, social media safety and fighting child-targeted online crimes. In addition to participating in critical debate regarding social media safety, students between the ages of 14 and 17 had the opportunity to interact firsthand with many of the forensic instruments now used by law enforcement.



Army Criminal Investigation Laboratory

The Army Criminal Investigation Laboratory is currently led by Assistant Director Debra E. Glidewell and is a fully manned and equipped criminal forensic laboratory located on Gillem Enclave in Forest Park, Georgia.

MISSION: The U.S. Army Criminal Investigation Laboratory (USACIL) provides quality, timely, worldwide, cutting-edge forensic science casework and crime scene support, serves as the Department of Defense's Program Manager for the Combined DNA Index System and provides educational subject matter experts to support the Department of Defense, Military Criminal Investigative Organizations, federal departments and organizations and the forensic science community in criminal investigations.

WHO WE SERVE

2022-2023 Scientific Impact to the Larger Forensic Community

Our forensic examiners are often selected to participate on national committees and working groups to advance the field of forensic science.

- **An increase from 17 to 19 USACIL scientists serving on the National Institute of Standards and Technology (NIST) Organization of Scientific Area Committees (OSAC) and Task/Working Groups in the areas of:** Forensic Science Standards Board, video/imaging technology and analysis, facial and iris identification, seized drugs, miscellaneous materials, chemistry (trace evidence, trace materials), ignitable explosives, (liquids and gunshot residue), DNA, human forensic biology, forensic nursing, friction ridge, footwear/tire track, 3D toolmark technologies, implementation Cohort Task Group and proficiency testing.
- In 2023, seven USACIL scientists participated in scientific working groups (SWGs) in the areas of DNA, digital evidence and drug chemistry.
- From 2022-2023, five USACIL scientists also served on the DNA Consensus Body, Footwear/Tiretrack Consensus Body and the Firearms/Tool Marks Subcommittee for the Academy Standards Board (ASBs) and Drug Chemistry.

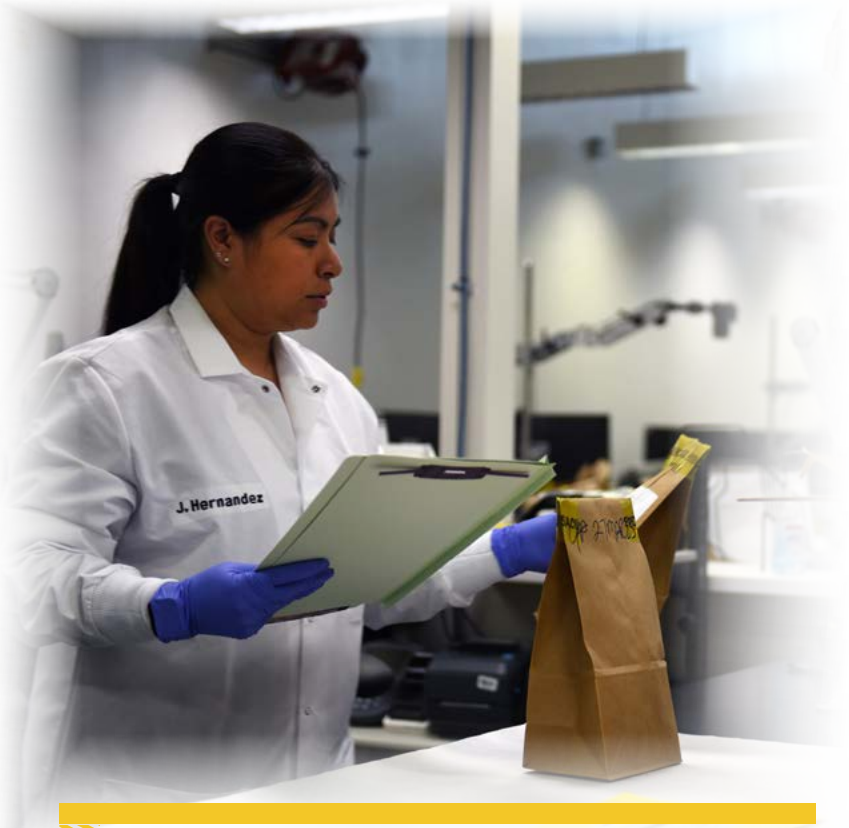
Educational Partnerships

Classes/courses taught by USACIL	Totals: 2022	2023
Special Agent Laboratory Training Courses	4	5
Trial Counsel Assistance Program Class	1	1
Defense Counsel Assistance Program Class	1	1
Evidence Custodian Laboratory Training Class	1	1

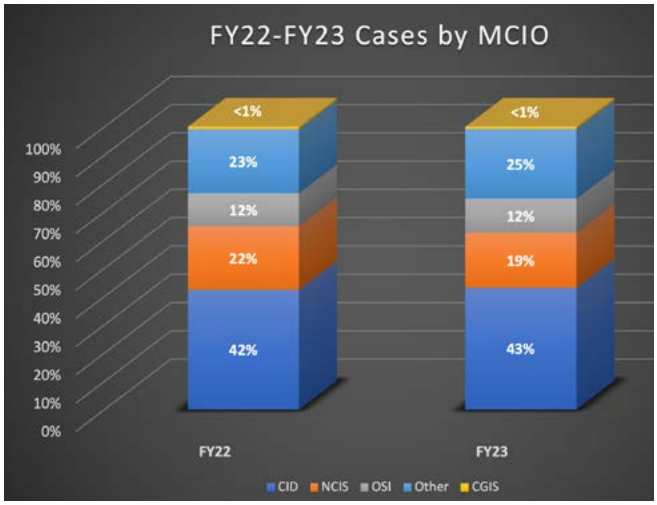
These courses trained more than 140 (2022) and 165 (2023) special agents, investigators, evidence professionals and judge advocates. USACIL also collaborated with Federal Law Enforcement Training Centers (FLETC) and U.S. Army Military Police School (USAMPS) by reviewing curriculum concerning crime scene investigations and the proper forensic techniques for the collection, preservation and documentation of evidence.

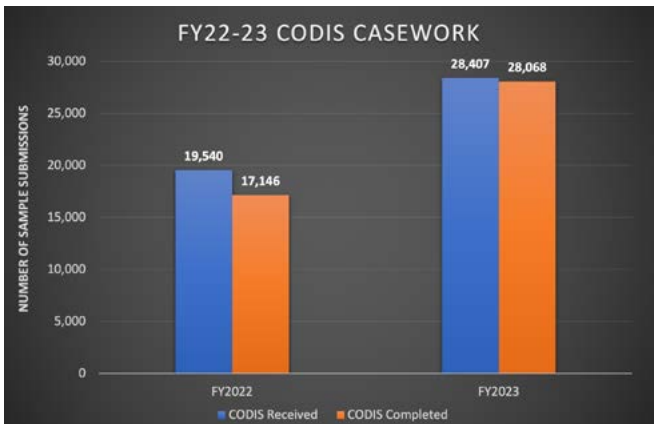
2022-2023 FORENSIC CASEWORK STATISTICS

For the past two fiscal years, USACIL processed more than 4,000 cases using 12,000+ forensic services examining 70,000+ evidence exhibits. In FY22, the USACIL team received 2,164 cases with 6,285 forensic services equaling 37,700 exhibits examined and analyzed. In contrast, in FY23, USACIL received 1,997 cases comprised of 5,932 services resulting in 32,127 exhibits examined and analyzed



USACIL's DNA database team processed more than 17,000 convicted offender and arrestee samples in FY22 and more than 28,000 samples in FY23 – a 60% increase in the past year.





SECTION 03

FUNCTIONAL FIELD OFFICES

Executive Protection Field Office

CID Executive Protection Field Office (EPFO) is based at Fort Belvoir, Virginia. This field office has the responsibility for providing worldwide executive protection for the Secretary of Defense, Chairman of the Joint Chiefs of Staff, Secretary of the Army, Chief of Staff of the Army, numerous combatant commanders and other senior civilian and military officials across DOD. EPFO also protects designated family members, former or retired DOD officials and foreign counterparts during official visits to the United States.

TRANSFORMATION

EPFO achieved remarkable transformation by adopting a team-based model in line with industry standards, a change recommended after a comprehensive four-month assessment conducted by the U.S. Secret Service. Throughout this transition, EPFO accomplished more than 1153 protective service missions, all while maintaining continuous protection for the principals, their families and residences in the National Capital Region (NCR). With the recent hiring of civilian Special Agents-in-Charge (SAC) and Assistant Special Agents-in-Charge (ASAC), this office will continue transformation efforts into 2024 and the future.

2022-2023 HIGHLIGHTS

PROTECTION OPERATIONS

The protection operations team made significant strides in ensuring the safety of high-profile individuals. Over 46 special agents and enablers were deployed to provide security for eight principals attending the Army-Navy game in Philadelphia in 2022 and in Foxborough in 2023. This effort was supported by a skilled forward intel support team and a proficient counter surveillance team. Operations encompassed not only the protection details but also involved plain-clothes surveillance detection team personnel positioned both outside and inside the stadium, working in collaboration with our partners from the local police departments and the White House. The thrilling games exemplified the success of the mission where Army emerged victorious beating Navy in back-to-back years.

PROTECTIVE INTELLIGENCE BRANCH (PIB)

The PIB's contributions were both significant and varied. Operating 24 hours a day, 7 days a week, this highly skilled team provided expert analysis across multiple platforms. It effectively responded to more than 751 requests for information from CID and external security teams, conducted 93 threat investigation/assessments, produced more than 1,000 travel assessments, 65 personal security threat assessments and 35 open-source vulnerability assessments related to assigned EPFO personnel. The PIB team conducted sensitive briefings to the Chairman of the Joint Chiefs of Staff and congressional staffers.

TRAINING AND TACTICS BRANCH

The Training and Tactics Branch (TTB) achieved remarkable progress in 2022-23 by conducting monthly and bimonthly training sessions, agent refresher training and agent integration programs. Instructors also provided an annual mobile training program to support combatant commander protection teams which ensured agents worldwide received the necessary training. Every week TTB provides firearms qualification on Quantico along with quarterly tactical and advanced marksmanship training. The success of this professional training would not be possible without the collaboration of joint partners, military service members, federal law enforcement officers and other CID field offices and directorates in the NCR to deliver exceptional training.

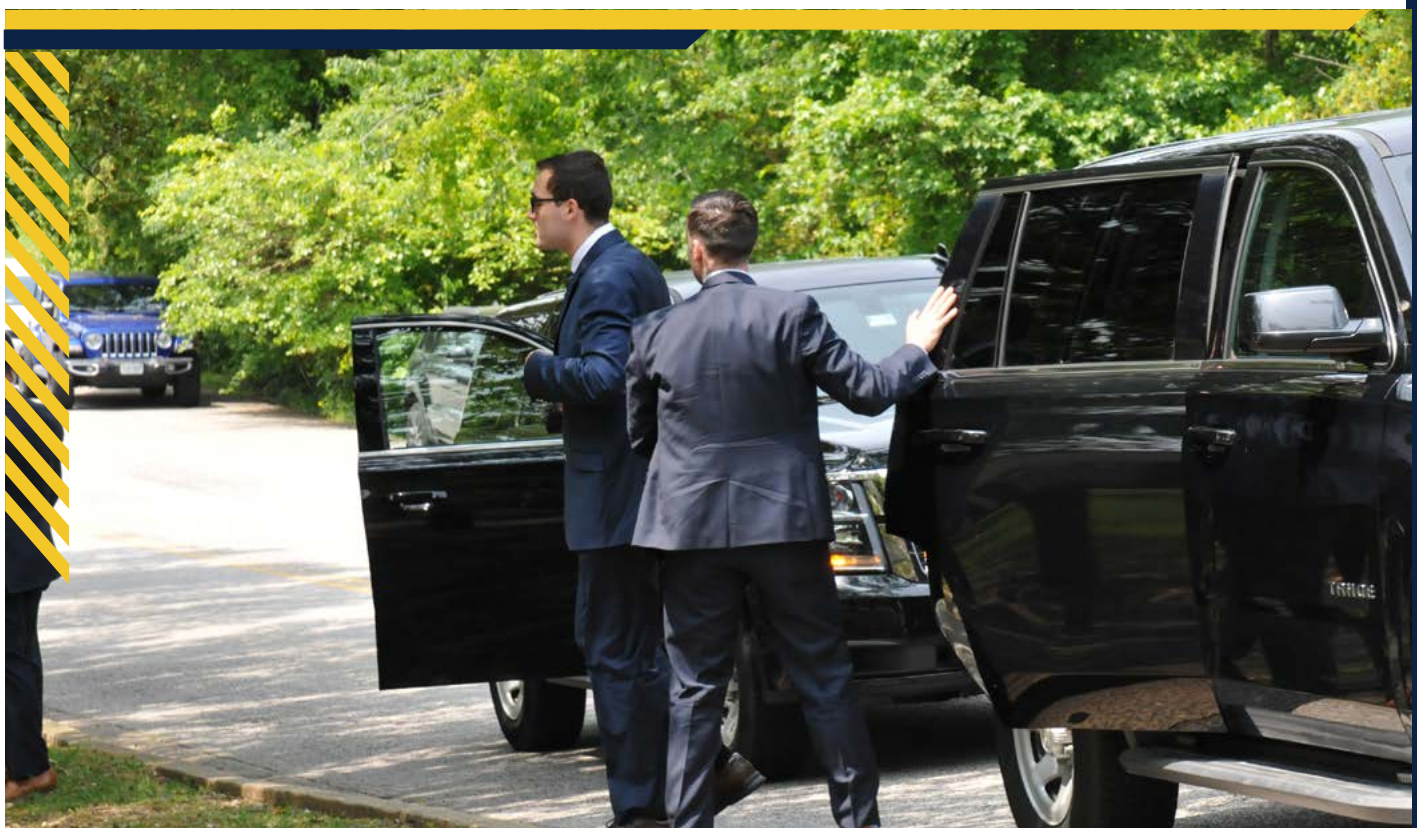
Protection completed its 24/7 NCR mission of protecting its principals, designated family members and residences.

Protection

1153 Total Missions for CY 2022 and 2023

595 CONUS Missions

558 OCONUS Missions



Special Investigations Field Office

The Special Investigations Field Office (SIFO) based at Fort Belvoir, Virginia, conducts worldwide criminal investigations by rapidly responding to emerging threats across the globe with full spectrum investigative capabilities that are responsive to both the national defense and CID strategies.

SIFO conducts criminal investigations impacting national security with an Army nexus. It conducts proactive and reactive efforts to detect, deter and disrupt national security threats surrounding U.S. Army Special Access Programs (SAP), U.S. Army Special Operations Command (USASOC), Joint Special Operations Command (JSOC), Special Mission Units (SMUs) and other sensitive activities.

It drives joint integration, collaboration and innovation between all CID field offices, CID functional field offices, CID headquarters elements, Army Counterintelligence (ACI) and other partners pertaining to national security crimes while strengthening the effectiveness of the Army's ability to eliminate these evolving and complex threats.

TRANSFORMATION

SIFO underwent a significant reorganization, merging both the Field Investigative Unit and the Transnational Criminal Investigative Units (TCIU) into a single field office. SIFO now has a new special agent-in-charge (SAC), a special advisor to the SAC and two new assistant special agents-in-charge (ASAC). As part of its restructured transformation, SIFO revamped its investigative mission and priorities. This consolidation now encompasses a comprehensive portfolio, which includes special access programs, integrated joint special technical operations, special mission units and sensitive activities including Joint Special Operations Command, U.S. Army Special Operations Command, Joint Investigations with Army counterintelligence, organized crime, surveillance support and crisis response. The structure is in place to allow future growth of embedded intelligence analysts and agents working together on the same response, surveillance and investigation teams who can deploy with short notice to combat zones or contingency operations. SIFO also provides proactive law enforcement support to vendor threat mitigation as a part of the preventive logistics security mission.

The introduction of a CID critical incident global response capability by the special investigations team has proven highly advantageous. This capability has enabled it to handle intricate and unique cases effectively leveraging it's specialized expertise. Remarkably, the swift responsiveness in classified and sensitive case work was achieved through efficiencies developed while under a suppression memorandum.

UNIQUE DIFFERENCES

SIFO cases are primarily prosecuted by the U.S. Attorney's Office in the Department of Justice and involve legal matters under Title 18 or the Uniform Code of Military Justice. To handle the sensitive nature of these cases and their connection to classified programs, SIFO operates within sensitive compartmented information facilities and special access program facilities. Key partnerships with the special operations community, intelligence community and foreign partners play a vital role in addressing the complexities of these cases.

2022-2023 INVESTIGATIVE HIGHLIGHTS

A SENIOR ARMY OFFICER STOLE OVER 500 CLASSIFIED DOCUMENTS

- A senior Army officer stole more than 500 classified documents and presented them to a DOD contractor to gain an edge in awarding a contract. The documents were seized by the Army. This was a joint investigation conducted by SIFO-SAP and Army counterintelligence.

FORMER AL QAEDA MILITARY COMMANDER RESPONSIBLE FOR ATTACKS ON COALITION FORCES

- In April and May 2023, SIFO traveled to Guantanamo Bay to interview a former Al Qaeda military commander responsible for numerous attacks on coalition forces in Afghanistan from 2002-2004. The former Al Qaeda military commander, was also slated to become the Al Qaeda leader in Iraq after the death of Abu Musab Al Zarqawi in June 2006. The interview sessions resulted in the collection of intelligence and leads. The Office of the Chief Prosecutor is currently using the collected information in criminal proceedings tied to other individuals responsible.

Output: Special Investigations Field Office

105 Foreign fighter prosecution packets produced to support international partners' pursuit of criminal prosecutions

1130 Requests for assistance to support the preparation of criminal prosecutions

50+ Intelligence products produced

26 Vendor threat mitigation products

SIFO produced 13 foreign fighter prosecution packets (FFIP) between 2022-2023. SIFO responded to 145 requests for assistance October through December 2022 and 605 in 2022. These efforts enabled the repatriation of detained foreign fighters in the CENTCOM area of responsibility and supported international partners pursuing criminal prosecutions. These FFIP's have contributed to the running total of four life sentences, 262 years confinement with 13 different countries to date. Additional numbers are available at higher classification.

SIFO's intelligence and investigative analysis section produced three main intelligence products, a U.S. Army Pacific Criminal Threat Assessment, a CID Repeat Offender Study for Army senior leader dissemination in 2023 and a brief of case reviews presented to the Army CID Deputy Director in October 2023. The intelligence section also produced multiple intelligence and investigative analysis products in support of internal and external requests for assistance and law enforcement reports related to SIFO investigations.

Cyber Field Office

The Cyber Field Office (CBFO) located in Quantico, Virginia, is the investigative arm of the Cyber Directorate and conducts highly technical investigations into network intrusions and malicious cyber events involving U.S. Army networks, defense industrial base, U.S. Army critical infrastructure and Army data in broader industrial base; cyber insider threats; investigations involving new and emerging technology; and financially motivated cybercrime.

SUBORDINATE OFFICES: CBFO-East, CBFO-West and CBFO-International.

2022-2023 INVESTIGATIVE HIGHLIGHTS

Cyber Field Office – International

CBFO-INT is located on Clay Kaserne, Germany. The CBFO-INT provides support to Army cyber equities in the Europe, Africa, Southwest Asia and Pacific theaters of operation.

NETWORK RECORDS UTILIZED TO PROTECT SOLDIERS AND ADVANCE INVESTIGATIONS

The CBFO-INT developed and implemented a program that leverages Army network logs to search for indicators of committing self-harm or harm to others. The CBFO-INT initiated 77 proactive actions in 2022 and 2023 in direct response to potential indicators of self-harm or harm to others identified within Cloud-Based Internet Isolation. Many of these actions warranted immediate contact with unit leaders to offer support and ensure Soldier safety. Feedback from unit leaders revealed they believed lives were saved.

OTHER HIGHLIGHTS TO NOTE

CBFO-INT provided instruction and assisted in the administration of the inaugural NATO Military Police Center of Excellence, Cyber Crime Investigation Course, in Bydgoszcz, Poland. The 50-hour course trained NATO MP first responders on the steps to properly identify, collect and preserve digital evidence within a joint operating environment. The course was the culmination of months of preparation by CBFO-INT and increased CID's profile with key strategic international partners.

Cyber Field Office – East

CBFO-East is located at the Russel Knox Building in Quantico, Virginia. The CBFO-E provides cyber investigative support to U.S. Army worldwide.

NETWORK COMPROMISE OF A CLEARED DEFENSE CONTRACTOR

- In December 2023, CBFO-East was notified by the FBI Orlando office of a network compromise of a cleared defense contractor by an unknown attacker. The attacker utilized a BlackCat/AlphaV ransomware affiliate and claimed to have exfiltrated 8 TB of data, encrypted multiple computers and sent a ransom note demanding $500,000 for the encryption keys. The investigation is ongoing.

OTHER HIGHLIGHTS TO NOTE

- CBFO-East agents mobilized to attend and provide expert knowledge on protecting national infrastructure assets from trending computer threats at Cyber Impact 2022. CBFO-East special agents have partnered with more than one hundred corporate partners through the Mandatory Incident Reports System to analyze and mitigate cyber incidents related to Army contracts and data.

Cyber Field Office – West

The CBFO-West is located in Denver, Colorado and provides cyber investigative support to the U.S. Army worldwide.

RACCOON MALWARE – REMOTE ACCESS TROJAN (RAT)

- The CBFO-West was notified by the FBI Cyber Task Force, San Antonio resident agency, that a recently emerged malware as a service platform offering fee-based malware to cyber criminals was used in an effort to gain unauthorized access to a U.S.-based, cleared defense contractor networks with several avionics-related U.S. Army contracts.

  CBFO-West investigation revealed more than 50 million records stolen from computer systems around the world using the Raccoon malware. While citizens from nearly every country were represented within the data, CBFO-West discovered several thousand credentials belonging to U.S. service members.

  Through investigative leads, the author and operator of Raccoon malware network was found to be a Ukrainian national. CBFO-West and FBI agents coordinated with Polish border police to identify a pattern that located the subject in the Netherlands. In March 2022, investigators with the Dutch national high-tech crime unit apprehended the subject in response to an international arrest warrant filed by the U.S. Department of Justice. The subject remains in custody in Amsterdam pending an extradition hearing. Through his U.S. based attorney, the subject has agreed to a proffer meeting with the Department of Justice. The proffer date is pending. CBFO special agent-in-charge briefed CBFO's joint role in this effort during a joint press release led by the Department of Justice and the FBI.

Cyber Field Office – Digital Personal Protection Program (CBFO-DP3)

CBFO-DP3 is located at the Russell Knox Building, Quantico, VA and provides tailored support to Army senior official and the DOD worldwide concerning data privacy, online impersonations, deepfakes and cybersecurity.

ROMANCE SCAM INVOLVING IMPERSONATION OF FORMER CJCS WITH A LOSS OF $3.4 MILLION

- CBFO-DP3 initiated a proactive investigation concerning the victimization of two U.S. Citizens who were lured into a confidence/romance scam with an individual(s) impersonating the Chairman of the Joint Chiefs of Staff and unwittingly provided $3.4 Million dollars to the online scammer in gift cards, cashier checks, money wire transfers and cryptocurrency transfers. During the investigation, CID and the Defense Criminal Investigative Service identified additional U.S. victims and a complex global money laundering network involving a U.S. citizen, who is the primary subject for this investigation and several Nigerian actors, who have come under investigation by the FBI and Homeland Security Investigations for scam-related activity.

OTHER HIGHLIGHTS TO NOTE

- From January 2022 through November 2023, CBFO-DP3 has identified over 280,000 impersonation accounts on social media for Army general officers and other DOD senior officials. Impersonation scams result in a conservative estimated loss of $2,500 per victim. CBFO-DP3 prevented a possible loss to victims of $325 million.

Fraud Field Office

The Fraud Field Office (FRFO)* is a functional field office headquartered in Fort Belvoir, Virginia. The FRFO is chartered to globally conduct major fraud and corruption investigations on matters impacting the Department of Army. The FRFO is staffed with agents and analysts who receive specialized training in the areas of procurement and financial crimes.

SUBORDINATE OFFICES

The FRFO is structured into three regions operating through subordinate resident agencies and resident units in 22 locations, worldwide. FRFO offices are strategically located throughout the U.S. and in Germany, Poland and Korea. Specific locations are based on multiple factors to include Army modernization efforts, key defense industrial base locations and the acquisition community centers.

INVESTIGATIVE HIGHLIGHTS

2018-2023

$2,470,768,693
in total monetary recoveries

FRFO investigations resulted in:

373 Indictments, **391** convictions, **663** suspension/debarment actions and
$2,470,768,693 in total monetary recoveries.

In 2023 alone:

23 Indictments, **51** convictions, **58** suspension/debarment actions and
$681,742,995 in monetary recoveries.

During 2022, the FRFO initiated a campaign to prioritize the prevention, investigation and education of matters related to the protection of Department of the Army technology being developed or fielded across the service. This campaign included the integration of FRFO agents with key Department of the Army and DOD organizations and working groups to assist in the prevention of technology loss; the development of an internal technology protection working group to identify and communicate best investigative practices; and fraud awareness briefings tailored to address technology protection concerns to hundreds of employees in the Army acquisition and research communities.

In 2023, the Major Procurement Fraud Unit/Field Office was transformed into the Fraud Field Office. This effort aligned the field office's composition to reflect the organization of the other field offices within CID. As a field office, the FRFO is better poised to integrate operations with the other field offices due to the standardization of organization and functions.

INVESTIGATIVE HIGHLIGHTS

$377,453,150.00 SETTLEMENT REACHED AGAINST BOOZ ALLEN HAMILTON

- The investigation conducted by the Washington metro fraud resident agency resulted in Booz Allen Hamilton (BAH) agreeing to resolve allegations it violated the False Claims Act by improperly billing commercial and international costs to its U.S. government contracts. BAH used costs and cost rates, including indirect expenses supporting their commercial and international businesses to seek inflated payments and reimbursements from the U.S. government. The settlement was made in compromise of disputed claims. Booz Allen Hamilton agreed to pay the U.S. government a total of $377,453,150.00, of which $209,696,195.00 was restitution.

QUI TAM INVESTIGATION RESULTS IN $143,000,000.00 SETTLEMENT

- Following an investigation by the mid-central fraud resident agency, Kellogg, Brown and Root Inc. (KBR) executed a settlement agreement between the Department of the Army and the United States. Under the terms of the agreement, KBR agreed to pay $108,750,000 to the U.S. government as a result of a Qui Tam complaint plus two percent annual interest. The investigation found that KBR had cheated the U.S. government by systematically failing to cross-level property as required by contract resulting in an accumulation of surplus property that was either underutilized or unusable. A portion of the $108,075,000.00 settlement, $56,088,000, was designated as restitution, and the government agreed to pay the realtors $31,565,149.32. KBR agreed to pay the relators an additional $34,950,000 to cover their costs and legal bills on top of the $108,075,000.

AMPHENOL CORPORATION PAYS $18,000,000.00 TO THE U.S. GOVERNMENT FOR FALSE CLAIMS

- Following an investigation by the Northeast fraud resident agency's Syracuse fraud office, Amphenol Corporation agreed to pay the United States government $18,000,000.00 to settle claims that it had submitted false claims for electrical connectors in violation of the False Claims Act. Amphenol had sold electronic connectors that did not fully comply with applicable government regulations and contract specifications because the company had not complied with necessary testing standards and other manufacturing and program requirements. Amphenol agreed to pay the U.S. government a total of $18,000,000.00, of which $9,000,000.00 was restitution.

FALSE CLAIMS CASE RESULTS IN $10,068,875 CIVIL RECOVERY

- Investigations conducted by the Sacramento fraud office, Pacific fraud resident agency, resulted in Dr. Paul Rhodes, Specific Diagnostics, Inc. and iSense, LLC. entering into a civil settlement with the U.S. government to resolve a False Claims Act allegation. The settlement resolves allegations that iSense mischarged various federal grants and U.S. Army contracts W911-SR15-C-0022 and W911-SR18-C-0013 for costs incurred by other companies with common owners, and approved compensation over and above the federal limits. The firms and Dr. Rhodes backdated documents presented to federal auditors. The settlement agreement required Specific Diagnostics, Inc. to pay the government $4,000,000. iSense paid the USG $4,000,000. Dr. Rhodes paid the $2,068,875.

$8.1 MILLION SETTLEMENT FALSE CLAIMS ACT CASE ON UNAUTHORIZED LABOR RATES

- An investigation conducted from the Sacramento Fraud Office, Pacific Fraud resident agency, resulted in the Sierra Nevada Corporation (SNC) entering into a civil settlement agreement with the U.S. Government to settle allegations they violated the False Claims Act. The investigation was initiated based upon the receipt of a Defense Contract Audit Agency, Form 2000 and Suspected Irregularity Referral Form 16055, which alleged SNC overcharged unauthorized and premium overtime rates on the U.S. Army Contracting Command, Communications-Electronic rates as a subcontractor under prime contract W15P7-T-10-DD421. In the settlement agreement, SNC paid the government $4,063,617 with $2,503,067 restitution back to U.S. Army. The remaining $1,560,550 will be paid to the U.S. Treasury Department.

SECTION 05

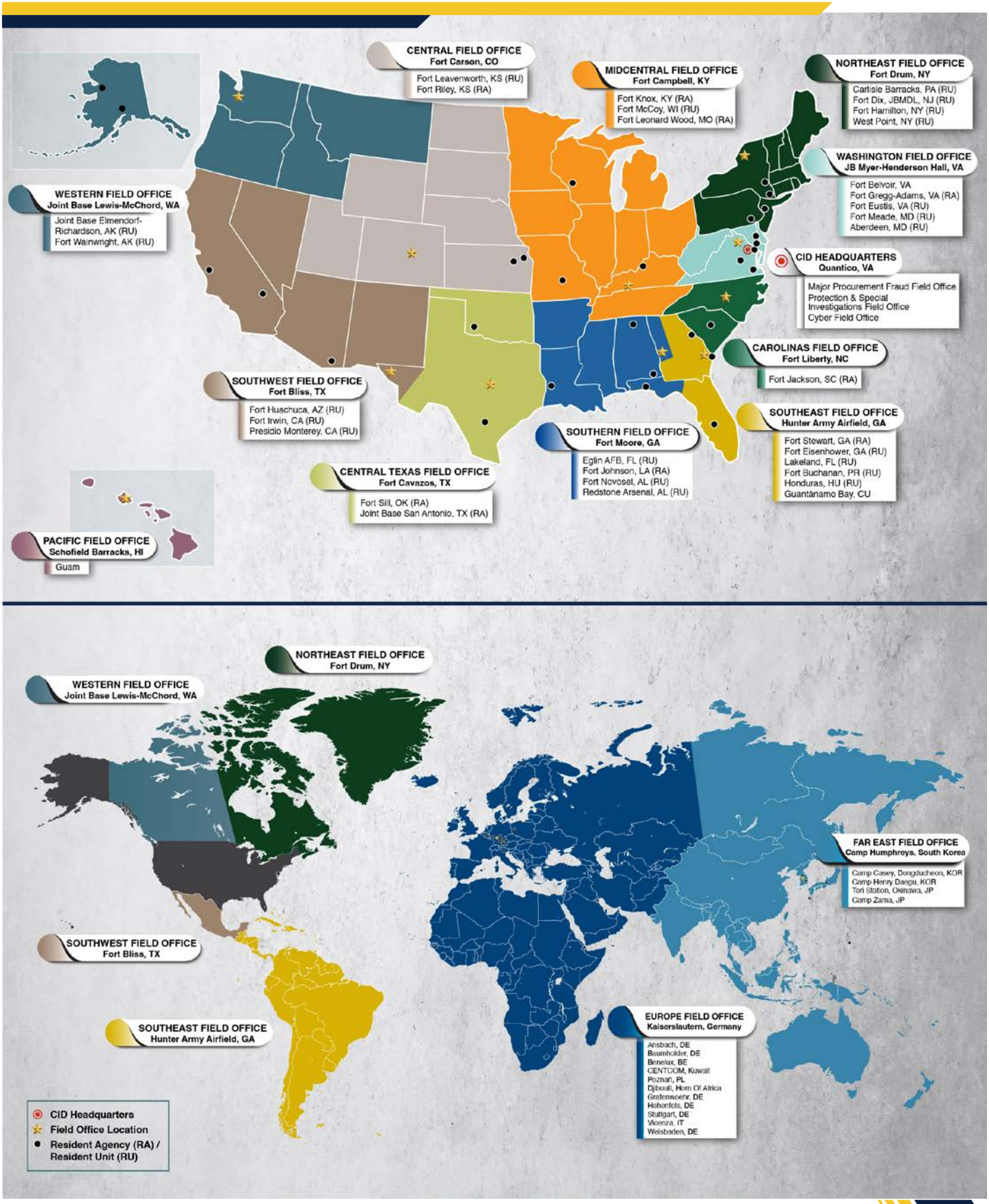
OFFICE LOCATIONS

Worldwide Locations

CONUS SPECIAL CAPABILITY LOCATIONS

OCONUS SPECIAL CAPABILITY LOCATIONS

CID FIELD OFFICE LOCATIONS AND AREAS OF RESPONSIBILITY



DEPARTMENT OF THE ARMY
CRIMINAL INVESTIGATION DIVISION
HEADQUARTERS

27130 Telegraph Road
Quantico, VA 22134-2253

WWW.CID.ARMY.MIL