ISSUE: SUMMER 2023

THE SHIELD

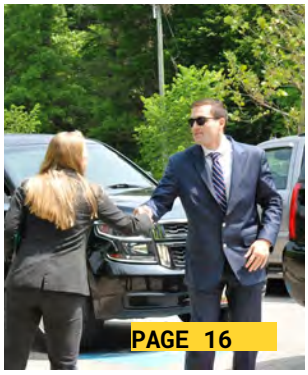
OFFICIAL PUBLICATION OF THE
ARMY CRIMINAL INVESTIGATION DIVISION

INSIDE:


CRIME SCENE DO NOT CROSS

CONTENTS

FEATURES



ON THE COVER: SARA GREEN, USACIL FORENSIC BIOLOGIST, PERFORMS A DNA SWAB DEMONSTRATION DURING A LABORATORY VISIT MARCH 28 IN FOREST PARK, GEORGIA. (PHOTO CREDIT: ARMY PHOTO BY CHRISTOPHER HURD)

THE SHIELD

The Shield is an official professional publication published by Army CID Public Affairs Office. We aim to provide our audiences with the latest news, trends and transformation updates within Army CID.

Army CID PAO | Need to contact us? Send a message to cidpao@army.mil and reference *The Shield*
Russell Knox Building | 27130 Telegraph Road | Quantico, VA 22134-2253 | www.cid.army.mil

We're on LinkedIn and X (formally Twitter!)
Follow us @REALARMYCID

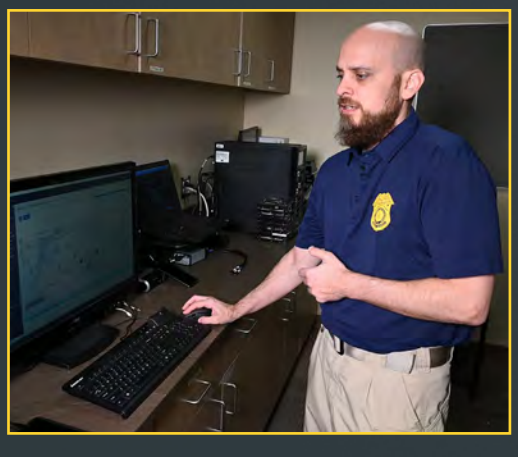
DEPARTMENT OF THE ARMY
CRIMINAL INVESTIGATION DIVISION

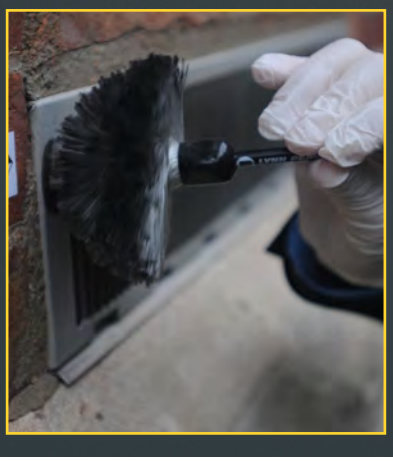
MISSION

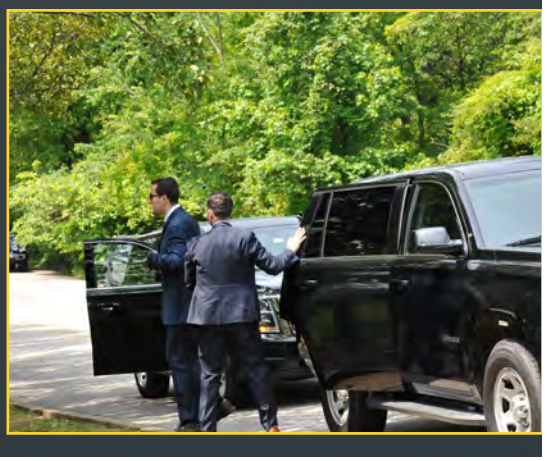
Army CID is an independent federal law enforcement agency consisting of nearly 3,000 personnel assigned to 124 world-wide locations, responsible for felony criminal investigations and operations; war crimes and terrorism investigations, criminal intelligence collection and analysis; cybercrime investigations and operations; multi-dimensional forensic support; and protective service operations for the Secretary of Defense, Chairman of the Joint Chiefs of Staff and other high risk personnel.


DEPARTMENT OF THE ARMY
CRIMINAL INVESTIGATION DIVISION
1775
SPECIAL AGENT


ARMY CID
POLICE
FEDERAL AGENT







ABOUT ARMY CID

WHAT WE DO

Army CID investigates and provides intelligence while working to proactively prevent crimes which impact the operational readiness of the Army. CID investigates felony crimes of serious, sensitive, or special interest matters to support commanders and preserve the Army's resources in peacetime, combat, and contingency operations.

Additionally, Army CID conducts worldwide investigations of classified Army programs and sensitive activities; acquisition fraud affecting Army programs and systems, major construction, and Soldier safety; intrusions, related malicious activities, and insider threats involving U.S. Army computers; and terrorism activities.

Join our team! Search CID opportunities at USAJobs.gov

USAJOBS "WORKING FOR AMERICA" Search Jobs

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

ABOUT ARMY CID

WHO WE ARE

Army CID is in the process of transforming from a military command into an independent civilian led federal law enforcement organization enabling the Department of the Army's mission, and supporting active duty, Reserve, Guard and Civilian workforce and their families.

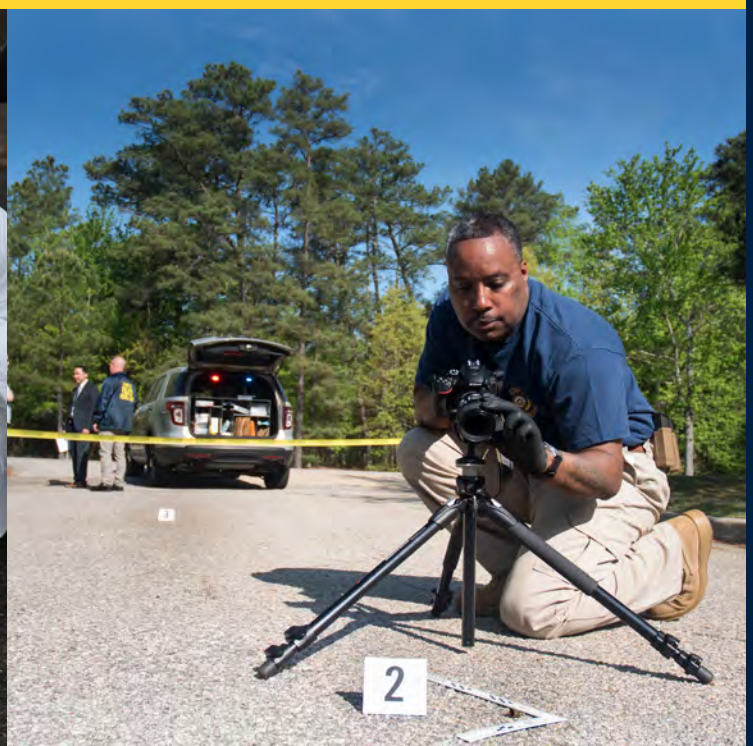
During this transformation, Army CID strategic lines of effort include four main points – Operational Excellence, Talent Management, Modernization and Partnerships. Our efforts are focused on how to increase investigative support functions and investigative capability and capacity, increase collaborative efforts with local, state, and federal law enforcement partners, meet our wartime requirements and exercise investigative independence.

As the Army's primary criminal investigative organization, Army CID is responsible for conducting felony-level criminal investigations in which the Army is, or may be, a party of interest.

Army CID is an independent Federal Law Enforcement Agency that employs military and civilian, credentialed federal Special Agents. CID directly supports the Army world-wide, through its protective services for High-Risk Personnel; as well as its expeditionary capability to support wartime requirements. Additionally, the agency is led by a civilian Director, a law enforcement professional who reports to the Secretary of the Army via the Under Secretary of the Army.

Headquartered at Quantico, Virginia and operating throughout the world, Army CID Special Agents conduct criminal investigations that range from death to fraud, on and off military reservations and when appropriate, with local, state and other federal investigative agencies.

Army CID supports the Army through the deployment, in peace and war, of highly trained Special Agents and support personnel, the operation of a certified forensic laboratory, a executive protection unit, computer crimes specialists, polygraph services, criminal intelligence collection and analysis and a variety of other services normally associated with law enforcement activities.



The Importance of Strong Email Security Practices

October is Cyber Awareness month, it is the perfect time to refocus on email safety, a cornerstone of our digital lives. Email, often the first point of contact in our online interactions, can unfortunately become a gateway for cyber threats if not properly secured. From personal communications to professional exchanges, it's crucial that we safeguard this digital mailbox from potential invaders.

Cybersecurity is not just a concept for tech experts to worry about, it's a vital aspect of our everyday online lives. When it comes to email, complacency can turn this essential tool into a critical vulnerability. From phishing scams to data breaches, emails safety risks are plentiful, but with a bit of knowledge and precaution, scams and breaches are largely preventable.

> **"Cybersecurity is not just a concept for tech experts to worry about, it's a vital aspect of our everyday online lives."**

TIPS FOR EMAIL SAFETY

- **Create Strong Passwords.** Use a combination of upper and lowercase letters, numbers, and symbols. Make sure it's not easily guessable, like "password123."
- **Enable Multi-Factor Authentication (MFA.)** This adds an extra layer of security by requiring a second form of verification beyond just your password.
- **Beware of Phishing Scams.** Never click on links or download attachments from unknown senders. They could lead to malicious websites or contain malware.
- **Never Share Sensitive Information.** Banks and other institutions will never ask for your personal details via email. If you receive such an email, it's likely a scam.
- **Keep Your Device's Operating System and Installed Software Updated.** Regular updates often contain security patches that protect you from new threats.

- **Use a Secure Connection.** When accessing your email, always use a secure connection (HTTPS) to prevent interception of your information.
- **Do Not Use Public Wi-Fi for Sensitive Activities.** Public networks are less secure. If you must use them, consider using a Virtual Private Network (VPN.)
- **Use a Spam Filter.** Enable a spam filter to help sort out potentially harmful emails.
- **Regularly Monitor Your Email Settings.** Check your settings regularly to ensure no changes have been made without your knowledge.
- **Avoid Using Your Email for Multiple Services.** Using your email for multiple services increases the risk if one service is compromised.
- **Regularly Back Up Your Emails.** Regular backups ensure that you don't lose important emails and can recover quickly in case of an attack.
- **Watch for Email Impersonation.** Be wary of emails from familiar names but unfamiliar addresses.

GETTING HELP:

Email safety is a continuous, integral aspect of our personal and professional digital lives. Each interaction with your inbox is an opportunity to reinforce your defenses against cyber threats. During and after Cyber Awareness Month, make a commitment to maintain and enhance your email security practices. Staying cyber aware isn't an option, it's a professional necessity in our interconnected world.

If you become a fraud, identity theft, or deceptive business practice victim, file a report with the Federal Trade Commission (https://www.ftc.gov/) and the Internet Crime Complaint Center (https://www.ic3.gov/).

CID Cyber Directorate

Internet safety is paramount in our increasingly connected world. However, complacency can leave us vulnerable to cyber threats and criminals that can compromise personal and financial information. Staying informed about best internet safety practices is our most effective defense.

TIPS FOR INTERNET SAFETY

ANTIVIRUS
- Keep your browser and antivirus software up to date.

SOFTWARE UPDATES
- Keep your software updated. Software updates fix bugs and resolve security issues.

STRONG PASSWORDS
- Use strong passwords, change them often, and do not use the same password for multiple devices and accounts.

MULTI-FACTOR AUTHENTICATION
- Use multi-factor authentication whenever possible.

SECURE WEBSITES
- Make sure websites have a secure connection. Verify the URL begins with https instead of http and the browser displays a padlock icon next to the URL.

SUSPICIOUS LINKS
- Do not click suspicious links or attachments as they sometimes lead to malicious downloads. Always verify the origin of a link.

PERSONAL INFORMATION
- Be cautious when posting personal information or photos that could reveal important information to criminals.

PRIVACY SETTINGS
- Update privacy settings on new or existing online accounts; never use the default settings.

FINANCIAL INFORMATION
- Do not send money or bank account information to anyone that you do not know.

SPONSORED LINKS
- Avoid clicking on sponsored links when using search engines as they could have malicious links in them or on the linked web page.

CID Cyber Directorate

Diversity, Equity & Inclusion

DIVERSITY, EQUITY & INCLUSION

The Impact of Diversity, Equity & Inclusion

The impact of Diversity, Equity, and Inclusion are even more powerful than we realize. While it may feel more comfortable to surround ourselves with like-minded people, when we have the courage to remove the barriers that exclude different perspectives, skillsets, generational differences, and experiences, we invite the building blocks for a stronger, more inclusive team.

So, why is inclusivity important? While working with people who think differently from you, who look at a problem from a different perspective, may feel a little less comfortable.

> **"Diversity promotes innovation by unearthing ideas that create better problem-solving skills."**

While taking the time to consider a different perspective, you will discover that diversity is not just about traits protected by law such as race, gender, and religion, but it also encompasses one's experiences with education, socioeconomics, and culture. Embracing these different mindsets, we can produce a wider variety of resources and solutions in the best interests of your company, agency or workplace such as The Department of Army, and Criminal Investigation Division.

There are times when diversity and inclusion are mentioned that some individuals feel excluded or forgotten. Left unchecked, this could lead to people disengaging from the healthy debates that promote innovation and even a lack of commitment to diversity overall. But diversity and inclusion does not mean trading in one set of ideas for another, rather it means we embrace our differences to reach creative solutions for the benefit of all. We all play a critical part of the mission to build an inclusive agency leaving no one out of the conversation. An open dialogue while sometimes uncomfortable, helps promote progress. Engaging in the more difficult discussions versus avoiding them challenges biases, invites new perspectives, and evokes reflection ultimately creating space where everyone feels welcomed.

Implementing and advancing Diversity, Equity, and Inclusion throughout CID, our vision and mission detailed below, provides a foundation ensuring shared input, transparency, and participation:

VISION

A seamless, valued, and all-inclusive workforce that embraces and leverages unique individual backgrounds, knowledge, and perspective to maximize organizational success and creative thought.

MISSION

To integrate a talented pool of high performing professionals from diverse backgrounds, skills and cultures that are committed to Army CID excellence promoting a continuous process of improvement.

In this section, our intent is to offer transparency highlighting what diversity truly means for CID. We are a team of individuals with different backgrounds and skill-sets working together to achieve the CID Mission. This space will serve as a forum in which we initiate meaningful dialogue that embraces our differences as we move forward. Stay tuned to our corner as we reveal segments of valuable insights and inspiration in our efforts to improve Diversity, Equity and Inclusion among our workforce.

Special Agent Karen Spidell
CID Chief Strategy Officer

Training & Partnerships

Army CID and the Korean National Police Academy

Work to Improve the International Crime Investigations Course

Army CID is committed to building strong relationships with host nations and combating felony-level criminal activity. One partnership in particular is with the prestigious Korean National Police Academy.

Special Agents from Army CID have been invited to share their expertise and insights with Korean detectives enrolled in the International Crime Investigations Course at the Police Academy.

The primary focus of this partnership is to enhance the capabilities of Korean detectives in deterring crime and fostering partnerships with the international community. Army CID Special Agents have been delivering regular blocks of instruction on the Status of Forces Agreement in Korea.

This important legal framework governs the presence and activities of U.S. military personnel in the country and plays a crucial role in maintaining security and promoting cooperation between the United States and Korea.

Tae Kim a Korean National Criminal Investigator, instructs Korean National Police Detectives

The presence of Army CID Special Agents in the International Crime Investigations Course has brought invaluable knowledge and experience to the participating Korean detectives. The sessions have provided a comprehensive understanding of the status of forces agreement provisions, which has enhanced the detectives' ability to navigate complex legal matters related to criminal investigations involving U.S. military personnel.

The primary focus of this partnership is to enhance the capabilities of Korean detectives in deterring crime and fostering partnerships with the international community.

By gaining a deep understanding of the SOFA, these detectives can ensure fair and effective collaboration with their American counterparts in addressing criminal activities that have an Army interest.

This partnership has facilitated the exchange of best practices and innovative approaches in investigating international crimes. Army CID Special Agents have been able to share their expertise in areas such as cybercrime, human trafficking, and financial crimes, which are increasingly prevalent in today's globalized world. The students at KNPA have greatly benefited from these specialized instruction sessions, expanding their knowledge base and equipping them with the tools to tackle emerging challenges in crime prevention and detection.

By actively engaging with law enforcement agencies and educational institutions, such as the Korean National Police Academy, Army CID aims to strengthen international cooperation in combating felony-level criminal activities that have an Army interest. Through these partnerships, Army CID is working towards a safer environment for all stakeholders, fostering trust and understanding, and promoting shared security objectives.

Ruben Santiago, Assistant Special Agent-in-Charge CID Far East Field Office

Department of Homeland Security specialized Targeted Violence and Terrorism Prevention Training

Since last year, more than 105 CID Special Agents, Military Police, and Soldiers from the 200th MP Command and Active Duty CID have taken part in the Department of Homeland Security (DHS) accredited Threat Evaluation and Reporting Overview (TERO) training. This four-hour, interactive training was conducted by DHS certified instructor, Army CID Special Agent Anthony (Tony) Campbell. This training was tailored to meet the demands of the special agents in both their military and professional law enforcement careers and for non-agents to better understand how to prevent acts of targeted violence within their workplace and community.

> **"This training was tailored to meet the demands of the special agents in both their military and professional law enforcement careers and for non-agents to better understand how to prevent acts of targeted violence within their workplace and community."**

The TERO training was developed by the Department of Homeland Security (DHS) National Threat Evaluation and Reporting (NTER) Office, which works to prevent targeted violence and terrorism through training, increasing public awareness, and developing partnerships across every level of government and the private sector. The TERO raises awareness about the risk factors, triggers, stressors, and warning behaviors that could affect a person's decision to commit an act of targeted violence. Further, it outlines the mitigating factors that could help prevent acts of targeted violence, while emphasizing the importance of community involvement in seeking help for individuals, and respecting their privacy, civil rights, and civil liberties.

DHS developed two additional targeted violence and terrorism prevention courses, which more thoroughly discuss triaging verbal and written threats and behaviors of concern, and trains students to utilize a four-step Behavioral Threat Assessment and Management (BTAM) model to identify, investigate, assess, and manage individuals who display threats or observable behaviors that may concern others. Special Agent Campbell became a certified instructor, titled Master Trainers, for these three programs last year and within weeks of becoming an instructor was able to share this vital knowledge at the Guardian Shield training event. So far this year, Campbell has facilitated courses in Washington D.C. and Missouri, and has two courses scheduled for Department of Defense partners in Virginia.

These DHS trainings are all conducted at no charge to participating private, public, and government organizations, to include the military services, and their surrounding communities. Each training includes engaging discussions, small group activities, case studies, and videos. Additional training on triaging threats, case development, reporting, and case/ person of interest management are included in the most comprehensive three-day training program.

Feedback from Soldiers attending the trainings was incredibly positive and enthusiastic. Special Agents appreciated the discussions around the identification and assessment of concerning behaviors and case studies portions of the training. Non-Special Agents valued the thorough discussion of risk factors, protective factors, how we may identify and support service members, our families, and the military and non-military communities we serve and live in. Campbell incorporates knowledge related to mental health and substance use challenges, to include discussing suicide prevention.

"Threat Evaluation and Reporting Overview (TERO) training raises awareness about the risk factors, triggers, stressors, and warning behaviors that could affect a person's decision to commit an act of targeted violence.

Special Agent Anthony (Tony) Campbell teaches at a training event held in Washington, D.C. (Gov Photo)

A key component to assessing the likelihood a person is considering conducting an act of violence or dying by suicide is understanding a change in behavior for those we serve with, family members, friends, acquaintances, and loved ones. Intervening as early as possible to support any potential mental health challenges they may be experiencing is key to improving the individual's ability to conduct their normal daily functions. Campbell found 99% of behavior related concerns were a result of the person needing support resources to cope with what they were experiencing, yet the person did not intend to act violently towards anyone. More often, the individual was at a higher risk for suicide. Campbell states, "through developing trust within our organization, personnel felt confident that our unit would manage their concerns thoroughly, discreetly, and appropriately resulting in getting the person of concern the help they needed."

Campbell believes the DHS programs may be beneficial to the DoD's Prevention, Assistance, and Response (PAR) and/ or overall efforts in preventing targeted acts of violence on and around military communities.

Interested Soldiers can become certified, just as Campbell has been, to teach these courses to their own units, on their bases, and to their communities. The DHS Master Trainer Program certifies Federal, State, Tribal, and Territorial partners in the instruction of Behavioral Threat Assessment and Management (BTAM) techniques and best practices. This train-the-trainer program is available to all active duty, reserve, national guard, and civilian members of the armed services and prepares individuals certified as Master Trainers to empower their local communities and organizations to mitigate threats and prevent acts of targeted violence.

For more information about becoming a National Threat Evaluation and Reporting (NTER) Master Trainer or about the training programs, please contact NTER.MTP@hq.dhs.gov.

ADDITIONAL RESOURCES:

Targeted Violence and Terrorism Prevention Grant Program

Centers for Prevention Programs and Partnerships (CP3) partners with DHS's Federal Emergency Management Agency (FEMA) to administer the Targeted Violence and Terrorism Prevention Grants Program, which provides funding for communities to expand their prevention and intervention activities or address gaps in current prevention capabilities. This program funds projects that will replicate promising practices as well as those that will explore new or innovative approaches. For more information, please visit www.dhs.gov/tvtpgrants.

Special Agent Glen Gerald

CID EMPLOYEE SPOTLIGHT

Highlighting the hardworking force necessary to provide superior criminal investigative support to the Army

Join our team! Search CID opportunities at USAJobs.gov

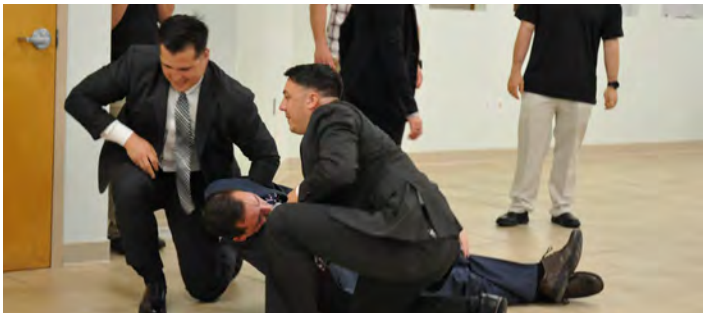
Interview with Brandi Little
Supervisory Special Agent, Executive Protection Field Office

QUANTICO, Va. - Supervisory Special Agent, Brandi Little manages the operation of the Training and Tactics branch for the CID Executive Protection Field Office. She has been working in CID Executive Protection for the past 10 years.

"When I originally became an Agent I worked investigations in North Carolina and loved it. In 2013 I moved to Virginia to join the CID Executive Protection Directorate. I started from the ground up working on the Department of the Army Security Detachment. I worked local mission here in the NCR and quickly moved to support travel both stateside and overseas," said Little.

After completing several missions, Little was selected to be a personal security officer for the Secretary of the Army. After that time, she participated in operations to help move security details around for missions. This eventually led her to a new opportunity in the training and tactics branch.

Once she moved into training and tactics Little said she "fell in love with the training side of things."



Protective Service special agents conduct scenario-based tactics training to sharpen key skills needed to identify a threat quickly and adapt.

The focus of her role as the Supervisory Special Agent is to manage and oversee the training and tactics programs. "We have four different programs that focus on new agent training, in-service training, agent advanced refresher training, and export training for COCOM details. Additionally we conducted other government agency training and liaison work with other protection providing organizations," described Little.

"Hard skills training for daily protective services operations and testing and trying new techniques, are essential while keeping up with industry standards to make teams the most effective," explains Little.

Protective Services industry standards is based on the requirements followed by protection providing organizations as a whole. Little explains, "we're just one of the protection providing organizations that is here in the northern capital region. We work with a lot of our sister agencies; Air Force Office of Special Investigations, Navy Criminal Investigative Service, and we've also partnered and continue to work with the U.S. Marshal's Service, State Department, FBI and U.S. Secret Service."

Special Agent Brandi Little greets a protected official during the role-playing portion of the scenario-based tactics training.

She stressed the importance of partnerships within the protective services field, "Continued partnerships with the Secret Service details and the FBI and protection teams help protective services identify exactly what they're doing in the field now and how we measure up to other agencies. This information is then used to advance techniques that will continue to keep our protectees, teams, and agents safe."

> **"Hard skills training for daily protective services operations and testing and trying new techniques, are essential while keeping up with industry standards to make teams the most effective."**

Little describes the Executive Protection and Special Investigations role and how it contributes to Army CID's overall mission as an "important mission."

"We're protecting those senior DoD officials that are protecting our nation and making those critical decisions that help keep us all safe. It's completely different from the investigative side and equally as important. We are contributing in a way that allows those senior officials to do what they need to help the investigative process and the military branches to be where they are needed," she stated.

Special Agent Little says the best part of her job is "interacting with the people."

"Getting to work with each of the protection details, both inside and outside of our organization. Getting to learn from their experiences and in turn sharing my own so we can all continue to learn and grow together. "

To learn more visit https://www.cid.army.mil/Our-Capabilities/#PSI

Jessica Hanley, CID Public Affairs Office

Army lab provides expansive capabilities to entire DOD

FOREST PARK, Ga. — Whether by standard mail truck or full-blown big rig, evidence from around the world continuously flows into the U.S. Army Criminal Investigation Laboratory in Forest Park.

USACIL, the Department of Defense's only full-service forensic laboratory, provides criminal investigators from every military branch with 24 forensic services ranging from DNA testing to latent print and trace evidence analysis.

> **"Our goal is to always be timely enough in our quality forensic results to be impactful in an open investigation."**

"We, in forensic science, play a critical role in the criminal investigation," said Debra Glidewell, USACIL assistant director. "The scientific analysis could be the piece of the puzzle that helps unravel the mystery of what happened."

Ryan Coffey, USACIL firearms examiner demonstrates how fire arms are tested in the lab's indoor range.

Jeanette Hernandez, USACIL physical science technician demonstrates the process of evidence triage.

The lab, which falls under the Department of the Army Criminal Investigation Division, constantly strives to continuously improve their efficiency and effectiveness. Before packages arrive, a pre-submission screening takes place where criminal investigators contact the lab to determine what evidence they can test. This screening process prioritizes the evidence that is tested, which allows technicians in various disciplines to focus their efforts in key areas.

When the packages finally arrive, technicians use a parallel process to intake evidence. That allows the techs to take DNA samples, trace evidence, drug samples and latent prints before sending that evidence to each branch to work on simultaneously.

This process contrasts with the previous sequential system that passed evidence from one branch to the next. The improvement has cut turnaround times for evidence analysis from 180 days to less than 60 days in most cases.

"Depending on how long that turnaround time is, it can negatively impact a case," Glidewell explained. "Our goal is to always be timely enough in our quality forensic results to be impactful in an open investigation."

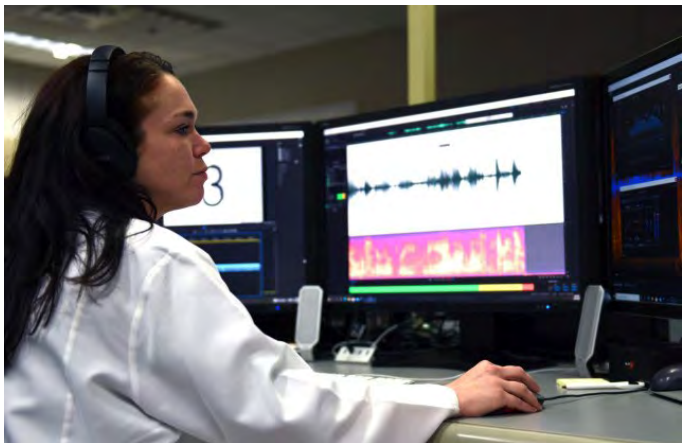
"We are the voice of the evidence. Whether they're a victim of a crime or a person of interest in a crime, all of our military members deserve quality forensic science to impact their investigation."

The lab also faces a challenge with informing criminal investigators of the robust capabilities they provide. They include firearms examination, digital evidence collection and analysis, drug chemistry, Combined DNA Index System (CODIS) databasing and indexing search. They're tackling this issue head on by hosting a laboratory training course several times a year.

Kim Westberry, USACIL chemist, performs a demonstration during a laboratory visit.

During the course, agents learn about each forensic discipline, their capabilities, what to look for at crime scenes, and how to collect and submit evidence to the lab. USACIL also conducts monthly forensic lab talks to get updated information to agents out in the field.

When the scientists are not in the lab, they're usually traveling around the world providing expert testimony in court cases. The traveling and testifying under



Christina Malone, USACIL digital forensic examiner, performs an audio/video analysis demonstration.

extreme pressure can take a toll on the scientists. That is why USACIL constantly looks at ways to care for its employees' mental, physical and emotional well-being.

"Taking care of people is not a sound bite, it's about making sure that these folks can be on the bench with their head in the game getting those quality forensic results out the door that impact our criminal investigations," Glidewell explained.

As part of the Army Criminal Investigation Division's ongoing transformation from a military command into an independent civilian-led federal law enforcement organization, the lab added 14 scientists that helped make a direct impact on turnaround times in cases.

As the demand for the lab's services increase, USACIL continually strives to provide world-class analysis that hopefully leads to justice through science.

"We are the voice of the evidence," Glidewell said. "Whether they're a victim of a crime or a person of interest in a crime, all of our military members deserve quality forensic science to impact their investigation."

Learn more about CID's capabilities: https://www.cid.army.mil/Our-Capabilities/#CIL

Christopher Hurd, Army News Service

HONORING ARMY CID'S FALLEN AGENTS

SACRIFICE | COMMITMENT | SERVICE

WASHINGTON – The Director of the Army Criminal Investigation Division, Gregory D. Ford, led a remembrance ceremony for fallen Army CID Special Agents during National Police Week at the National Law Enforcement Officers Memorial in Washington, D.C., May 17.

National Police Week is a time for the nation to remember and honor the women and men who have given their lives in the line of duty. Ceremonies and services are held in our nation's capital during this time and are attended by surviving spouses, partners, and family members as well as federal, state, and local law enforcement officers.

> **"A law enforcement career comes with the expectation that we will find ourselves in harm's way. Every one of the over 23,000 names on this memorial represents a person who was doing their job when they made the ultimate sacrifice."**
> **-Director Ford**

The family of Special Agent Elmer "Bud" Heggen provide each other support as the Director of the Army Criminal Investigation Division, Gregory D. Ford and the Division Chief Warrant Officer, Chief Warrant Officer 5 Paul D. Arthur, present a wreath of remembrance during the Army CID Fallen Agent Ceremony.

Red Roses lay above the engraved words at the entrance of the National Law Enforcement Officers Memorial in Washington D.C.

The National Law Enforcement Officers Memorial is a physical reminder of the sacrifices our nation's special agents, investigators, deputies, and officers have made to protect and make safer the places we live. The memorial has more than 23,000 names engraved on its walls.

"A law enforcement career comes with the expectation that we will find ourselves in harm's way. Every one of the over 23,000 names on this memorial represents a person who was doing their job when they made the ultimate sacrifice," Director Ford said.

The ceremony was not only an event to reflect and remember the Special Agents who gave their lives in the line of duty, but to honor the profession of law enforcement and its never-ending pursuit of the preservation freedom.

In attendance were the family members of Special Agent Elmer "Bud" Heggen who were recognized during the ceremony. At the conclusion of the ceremony Director Ford escorted the family to place a rose of remembrance at Special Agent Heggen's engraved name on the memorial wall.

> **"This was a very meaningful ceremony, and our family is grateful to have attended."**
> **-Leanne Heggen Eckstein**

A remembrance placard and red roses are placed near the engraved name of Army CID Special Agent Elmer "Bud" Heggen at the National Law Enforcement Officer Memorial in Washington D.C.

The family of Special Agent Elmer "Bud" Heggen place a rose of remembrance near his engraved name on the National Law Enforcement Officers Memorial in Washington D.C. along with the Department of the Army Criminal Investigation Division Director Gregory D. Ford.

"This was a very meaningful ceremony, and our family is grateful to have attended," said Leanne Heggen Eckstein. "It was a wonderful memorial for the eleven special agents whose names are on the memorial wall. It is difficult to find the way to say thank you to all involved in the planning of this event. You have given my children another memory of their father."

Special Agent Heggen, along with fellow Special Agent Henry H. Tibbs, was killed July 23, 1973, in an aircraft accident while traveling to testify at a court-martial for a Soldier convicted of murder.

As a final act of commemoration, Director Ford and Division Chief Warrant Officer, Chief Warrant Officer 5 Paul D. Arthur, laid a wreath of remembrance in the center of the atrium and held a minute silence before Taps was played.

NAMES AND DATE OF DEATH FOR THE FALLEN HONORED DURING THE CEREMONY:

- Special Agent Liquat Kahn, April 30, 2019.
- Special Agent Joseph M. Peters, October 6, 2013.
- Special Agent James C. Mayo, September 18, 1987.
- Special Agent Dirk A. Miller, December 12, 1985.
- Special Agent Norman E. Larson, September 24, 1973.
- Special Agent Elmer "Bud" Heggen, July 23, 1973.
- Special Agent Henry H. Tibbs, July 23, 1973.
- Special Agent James T. Abbott, January 11, 1971.
- Special Agent Leroy E. Halbert, December 31, 1970.
- Investigator John A. Hanson, May 9, 1970.
- Special Agent Walter E. Snyder, May 9, 1948.

We honor the commitment and sacrifice of the Special Agents who have lost their lives in service to our country.

To learn more about CID Fallen agents, visit: https://www.cid.army.mil/The-Agency/Fallen-Agents/

Thomas B. Hamilton III, Public Affairs

CID IN THE NEWS

OWNERS OF MILITARY CONTRACTING COMPANIES SENTENCED FOR BID RIGGING IN TEXAS

Texas (Aug. 31, 2023) – Two military contractors were sentenced today in the U.S. District Court for the Eastern District of Texas, Texarkana Division, for their roles in a bid-rigging scheme involving the maintenance and repair of military tactical vehicles in Texas. The multi-year scheme secured more than $17 million in taxpayer dollars.

Aaron Stephens, of Queen City, Texas, was sentenced to 18 months in prison and ordered to pay a criminal fine of $50,000. According to a plea agreement filed on Jan. 12, Stephens and his co-conspirators rigged bids on certain government contracts from May 2013 to January 2018 to give the false impression of competition and secure government payments. The conspirators submitted coordinated, higher-priced and non-competitive bids to ensure a designated company won each contract. Stephens and his co-conspirators rigged six different contracts for work performed for the Red River Army Depot in Texarkana, Texas. The projects included heavy military equipment work like refurbishing armor kits for military trucks and turrets for Humvees.

John “Mark” Leveritt, of Heath, Texas, was sentenced to six months in prison and ordered to pay a criminal fine of $300,000. According to a plea agreement filed on July 13, 2022, Leveritt engaged in the same conspiracy from May 2013 to April 2018 involving seven bids.

“Today’s sentences demonstrate our commitment to safeguarding the integrity of the military contracting process,” said Assistant Attorney General Jonathan Kanter of the Justice Department’s Antitrust Division. “We will hold accountable those who enrich themselves at the expense of our armed forces and ultimately the public.”

“Servicing heavy military vehicles and equipment are critical to the functioning of the U.S. military and its mission, so anticompetitive practices such as those used by the defendants in this case harm the military, taxpayers, and legitimate businesses alike,” said U.S. Attorney Damien M. Diggs for the Eastern District of Texas. “The Eastern District of Texas will vigorously prosecute those who compromise the integrity of the procurement process for greed and personal gain.”

“This sentencing should stand as a deterrent to those who would engage in fraud and corruption for personal gain and is a testament to the thorough and professional effort of our investigative partnerships with the United States Attorney’s Office and the FBI,” said Acting Special Agent-in-Charge Michael Curran of the U.S. Army Criminal Investigation Division’s Major Procurement Fraud Field Office. “We will diligently continue our efforts to pursue those engaged in criminal activity that impacts the integrity of the U.S. Government and the U.S. Army.”

“Today’s sentences are the result of the tireless work and dedication of multiple agencies to hold these individuals accountable for conspiring to defraud the United States government,” said Special Agent in Charge Chad Yarbrough of the FBI Dallas Field Office. “The public can rest assured that we remain committed to aggressively pursuing anyone that uses government programs for their own personal gain.”

The division’s Washington Criminal II section, the U.S. Army Criminal Investigation Division’s Dallas Fraud Resident Agency, and the FBI Dallas Field Office investigated the case

Trial Attorneys Jillian Rogowski, Daniel Loveland, and Aidan McCarthy of the Antitrust Division’s Washington Criminal II Office prosecuted the case.

In November 2019, the Justice Department created the Procurement Collusion Strike Force, a joint law enforcement effort to combat antitrust crimes and related fraudulent schemes that impact government procurement, grant, and program funding at all levels of government — federal, state and local. To contact the Procurement Collusion Strike Force, or to report information on market allocation, price fixing, bid rigging and other anticompetitive conduct related to construction or infrastructure, go to www.justice.gov/procurement-collusion-strike-force.

SOUTHERN DISTRICT PROSECUTES NEARLY $11 MILLION IN COVID FRAUD AS PART OF NATIONAL ENFORCEMENT ACTIONS

SAVANNAH, GA (Sept. 5, 2023) – As part of a coordinated nationwide effort to fight COVID-19 fraud, the Southern District of Georgia has taken action against individuals who illegally obtained nearly $11 million in funds intended to help struggling small businesses during the global pandemic.

As announced by U.S. Attorney Jill E. Steinberg, and in conjunction with the Justice Department's nationwide effort, the Southern District of Georgia conducted more than 20 enforcement actions from May through July 2023, involving a total of $10.9 million in alleged COVID-19 relief fraud.

"Funding through the 2020 Coronavirus Aid, Relief and Economic Security (CARES) Act provided more than more than $650 billion to assist small businesses navigating the financial challenges of the pandemic," said U.S. Attorney Steinberg. "Unfortunately, fraudsters tapped into this program for their own profit, and this nationwide effort seeks to hold them accountable for their widespread fraud."

The CARES act provided small business assistance primarily with grants and forgivable loans available through the Paycheck Protection Plan (PPP) or Economic Injury Disaster Loans (EIDL). The Southern District of Georgia U.S. Attorney's Office, working with its law enforcement partners, conducted multiple enforcement actions during the May-June period including:

- Kamario Thomas, 42, of Augusta, Ga., was sentenced to 38 months in prison for Conspiracy to Commit Wire Fraud and Money Laundering. Thomas submitted more than 60 fraudulent loan applications for pandemic relief and received hundreds of thousands of dollars in kickbacks for his fraud. Thomas was ordered to pay full restitution in the amount of $4,546,945.
- Bernard Okojie, 41, of McDonough, Ga., was convicted of Conspiracy to Commit Wire Fraud and Money Laundering after a three-day jury trial. As detailed during trial, Okojie used information for non-existent companies to file more than 20 fraudulent loan applications for pandemic relief aid, causing losses in excess of $3.5 million. He awaits sentencing.
- Jacqueline Somesso, 55, of Savannah, was sentenced to 18 months in prison for Bank Fraud and Misprision of a felony. Somesso submitted a fake pandemic relief loan application resulting in losses of $570,736.87. She was ordered to pay restitution in this amount and to forfeit a money judgment in that amount. The Court also entered a consent order forfeiting her interest in a certificate of deposit of $350,236.54 and a bank account of $3,520.91, both containing fraud money seized from her during the investigation.
- Kyle Waldron, 58, of Douglas, Ga., received service of a civil forfeiture complaint arising from his filing of numerous fraudulent loans applications for pandemic relief aid. The complaint seeks forfeiture of $326,461.33, the amount of fraud money seized from his bank account.

A civil forfeiture complaint was filed and continues to be litigated concerning an Atlanta condominium on Peachtree Road Northwest. This property, valued at $328,000, was purchased with money obtained fraudulently through pandemic relief loans.

Anyone with information about allegations of attempted fraud involving COVID-19 can report it by calling the Department of Justice's National Center for Disaster Fraud (NCDF) Hotline at 866-720-5721 or via the NCDF Web Complaint Form at: https://www.justice.gov/disaster-fraud/ncdf-disaster-complaint-form.

These cases were investigated by the Department of the Army Criminal Investigation Division, Internal Revenue Service Criminal Investigations, the U.S. Secret Service, the U.S. Treasury Inspector General for Tax Administration, the Small Business Administration Office of Inspector General, the FBI, the U.S. Postal Inspection Service, and the U.S. Department of Labor Office of Inspector General.

The enforcement actions were prosecuted for the United States by Assistant U.S. Attorneys Matthew A. Josephson, Jennifer A. Stanley, Ryan C. Grover, Lindsay Berman-Hansell, J. Bishop Ravenel, Alex Hamner, Marcella Mateo, David H. Estes, and Senior Litigation Counsel Jennifer G. Solari.

Contact: Barry L. Paschal, Public Affairs Officer: 912-652-4422


DEPARTMENT OF THE ARMY
CRIMINAL INVESTIGATION DIVISION
1775
SPECIAL AGENT