



THE FBI STORY

2020

THE FBI STORY

2020



Director's Community Leadership Awards, p. 21

Welcome to the 2020 edition of *The FBI Story*—a selection of our past year’s work as told through some of the original stories and images from our website. This inside look at our people, programs, investigations, and operations only scratches the surface of the work we highlighted online in 2020 and is just a sampling of the work we do every day to protect the American people and uphold the Constitution of the United States.

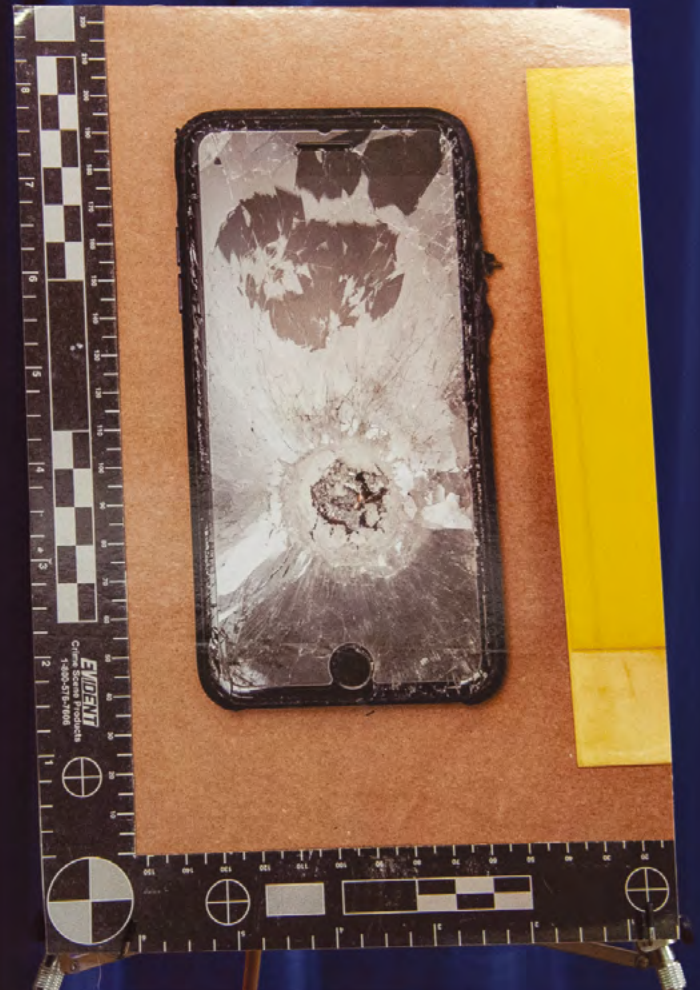
You can view the complete versions of the stories featured in this publication, as well as many more, at [fbi.gov/stories](https://www.fbi.gov/stories).



FBI Director Christopher A. Wray

SHOOTING AT NAVAL AIR STATION PENSACOLA CALLED 'ACT OF TERRORISM'

DECEASED ASSAILANT'S LOCKED
PHONES A HURDLE FOR INVESTIGATORS



The Department of Justice and the FBI provided new details about a shooting at Naval Air Station Pensacola that left three U.S. sailors dead and eight others wounded.

Attorney General William P. Barr said the December 6, 2019 attack by Mohammed Saeed Alshamrani, a member of the Royal Saudi Air Force who was studying at the Florida military base, was “an act of terrorism” motivated by “jihadist ideology.”

Barr and FBI Deputy Director David Bowdich also highlighted a significant hurdle in the ongoing counterterrorism investigation—the inability to extract information from the deceased shooter’s encrypted Apple iPhones despite court authorization and probable cause.

Alshamrani left two iPhones at the crime scene—one he shot through with a bullet before being killed. The FBI Laboratory was able to restore both phones to working order but is unable to unlock either of them.

“Even with a court order, to date we cannot access the contents of the two phones that the attorney general referred to in this investigation—and countless other investigations,” Bowdich said. “We want to work together with private sector companies so that we can lawfully access the evidence and information we need to keep our country and its citizens safe.”

“We’re not trying to weaken encryption,” he added. “After all, data security is a central part of our mission.”



We want to work together with private sector companies so that we can lawfully access the evidence and information we need to keep our country and its citizens safe.”

CONFRONTING THE CHINA THREAT

WRAY SAYS WHOLE-OF-SOCIETY RESPONSE NEEDED TO PROTECT U.S. ECONOMIC AND NATIONAL SECURITY



China is threatening the U.S. economy—and national security—with its relentless efforts to steal sensitive technology and proprietary information from U.S. companies, academic institutions, and other organizations, FBI Director Christopher Wray said during opening remarks at the half-day Department of Justice China Initiative Conference in Washington, D.C.

Wray described the threat from China as “diverse” and “multi-layered.” He noted that the Chinese government exploits the openness of the American economy and society.

Wray told the audience that China is targeting everything from agricultural techniques to medical devices in its efforts to get ahead economically. “They’ve shown that they’re willing to steal their way up the economic ladder at our expense,” he said.

The FBI is using traditional law enforcement techniques as well as its intelligence capabilities to combat these threats. He said

the FBI currently has about 1,000 investigations into Chinese technology theft.

Wray also called for a whole-of-society response to these threats. He urged U.S. companies to carefully consider their supply lines and whether and how they do business with Chinese companies. While a partnership with a Chinese company may seem profitable today, a U.S. company may find themselves losing their intellectual property in the long run. Additionally, U.S. universities should work to protect their foreign students from coercion from foreign governments.

Wray noted, however, that these threats do not mean the U.S. shouldn’t welcome Chinese students or visitors. “What it does mean is that when China violates our criminal laws and well-established international norms, we are not going to tolerate it, much less enable it,” he said. “The Department of Justice and the FBI are going to hold people accountable for that and protect our nation’s innovation and ideas.”

CHINESE MILITARY HACKERS CHARGED IN EQUIFAX BREACH

INTRUSION AFFECTED NEARLY HALF OF ALL AMERICANS

The U.S. Department of Justice announced charges against four Chinese military-backed hackers in connection with carrying out the 2017 cyberattack against Equifax, a consumer credit reporting agency. The intrusion led to the largest known theft of personally identifiable information ever carried out by state-sponsored actors.

Investigators had previously discovered and announced the type of malware that allowed the hackers to harvest addresses, birth dates, Social Security numbers, and other data on approximately 145 million Americans. This indictment charges that members of the People's Liberation Army—the armed forces of the People's Republic of China—were behind that malware attack.

According to the indictment, Wu Zhiyong, Wang Qian, Xu Ke, and Liu Lei exploited a vulnerability in the dispute resolution website within the Equifax system. From that initial access point, the hackers used a number of techniques to force their way into the company's network and back-end databases.

In announcing the charges, U.S. Attorney General William Barr said that the Equifax intrusion is among other efforts by the Chinese government to steal the personal data of Americans. The Justice Department believes the Chinese were also responsible for breaching systems controlled by the Office of Personnel Management, Marriott hotels, and the health insurance company Anthem.

FBI Deputy Director David Bowdich said that although these types of breaches have become disturbingly common, businesses cannot become complacent about protecting data and consumers. "And as American citizens, we cannot be complacent about protecting our sensitive personal data," Bowdich emphasized. "We in law enforcement will not let hackers off the hook just because they're halfway around the world. We've got to do everything we can to keep people safe, secure, and confident online."



LOOKING FOR ASHA

CLUES SOUGHT IN CASE OF 9-YEAR-OLD GIRL WHO DISAPPEARED 20 YEARS AGO



Twenty years ago, Asha Degree, a shy 9-year-old North Carolina girl, went missing in the middle of the night. The spirited fourth-grader's disappearance shook her rural community of Shelby and remains an enduring mystery, even as police, the FBI, and her family continue to actively search for clues.

The case remains an open investigation, with a local detective reviewing leads—old and new—and FBI investigators from the Charlotte Field Office consolidating and combing through case files for unexplored patterns or clues. Investigators believe someone in area may hold the key that could unlock the case.

"We strongly believe that there is someone out there that may have a piece of information that will help her," said Cleveland County Sheriff's Office Detective Tim Adams, who came out of retirement in 2014 to lead the department's probe. In 2015, the sheriff's office teamed up with the FBI and the North Carolina State Bureau of Investigation in a top-to-bottom re-examination of the case, which has since generated more than 350 leads, including 45 in the past year.

What is known from the earliest hours of the investigation is that Asha disappeared from her bedroom sometime between about 2:30 and 6:30 a.m. on February 14, 2000. There was no sign of forced entry and no promising scent trail for search dogs to follow. That afternoon, investigators received at least two separate reports from individuals who said they saw a young female walking along Highway 18, in the opposite

direction of the Degrees' home, around 4 a.m. One person said they went back to check on the girl but she had left the roadway and disappeared into the woods.

On August 3, 2001, some 30 miles north of the last sighting, construction workers digging an access road for a new home in neighboring Burke County found a book bag that belonged to Asha. Inside was a concert T-shirt featuring boy band New Kids On The Block and a children's book, *McElligot's Pool*, by Dr. Seuss. Neither belonged to Asha, though the book was from the library at Asha's school, Fallston Elementary. Investigators released images of the shirt and book in 2018, hoping to jog the memories of people who may have helpful information.

The 2015 re-investigation also turned up another possible lead: Asha may have been seen getting into a dark green 1970s-model Lincoln Continental Mark IV or Ford Thunderbird with rust around the wheel wells. The FBI publicly announced the potential lead in 2016 and released images of the vehicle models.

Working with the National Center for Missing & Exploited Children, the FBI has released multiple age-progressed photos of Asha, including a new version this month showing what Asha may look like as a 29-year-old. The FBI is offering a \$25,000 reward on top of \$20,000 set aside by the Cleveland County Sheriff's Office and the community.

If you have information regarding this case, visit tips.fbi.gov.



\$45,000 REWARD

MISSING

Asha Jaquilla Degree

Age 9 Age-progressed to 21

Asha Jaquilla Degree has been missing from her home in Shelby, North Carolina, since February 14, 2000. Family members last saw her asleep in her bedroom at approximately 2:30 a.m. At 4:00 a.m., she was seen by drivers walking along North Carolina Highway 18 in Cleveland County. More than a year later, Asha's bookbag was discovered buried along North Carolina Highway 18 in Burke County. The FBI is offering a reward of up to \$25,000 for information leading to the arrest and conviction of the person or persons responsible for her disappearance. An additional \$20,000 reward is being offered by the Cleveland County Sheriff's Office and community. Anyone with information should call law enforcement.

704-672-6100 / 704-484-4822



FBI TOP TEN LIST TURNS 70 PUBLIC REMAINS CRUCIAL TO HELPING CATCH FUGITIVES

The seeds of the FBI's Ten Most Wanted Fugitives list were planted on February 7, 1949, after *The Washington Daily News* published the article "FBI's Most Wanted Fugitives Named." The FBI's public affairs function at the time had given the reporter—who'd asked for a list of the "toughest guys" the Bureau wanted to arrest—the names of 10 dangerous individuals.

The resulting news story became so popular that the FBI created the Ten Most Wanted Fugitives list on March 14, 1950.

This week marks the 70th anniversary of the list, which is commonly called the Top Ten. The program uses public outreach to capture offenders wanted for serious crimes.

Over the years, 523 fugitives have been placed on the list, with 488 of them having been caught. As a testament to the effectiveness of the program, 162 of those captures were made with the public's direct assistance.

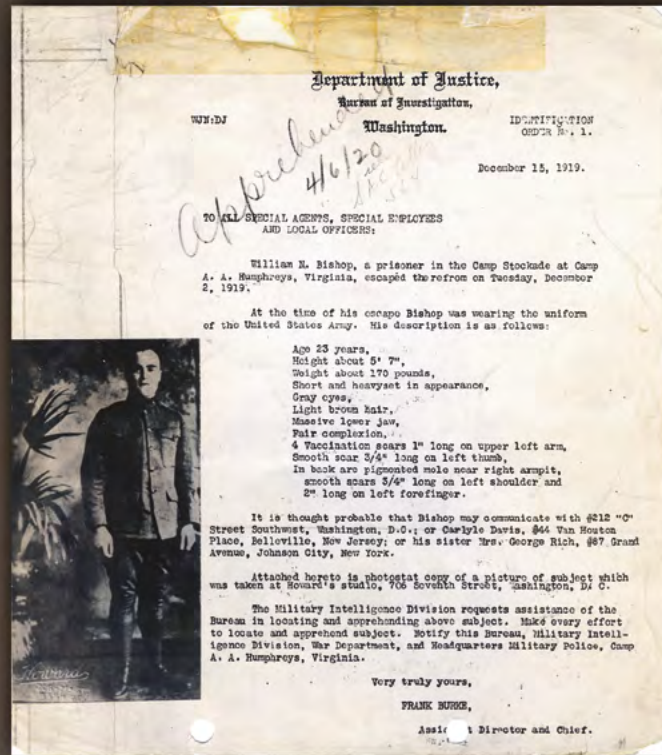
Historically, the Top Ten list has reflected the concerns of the time. In the 1950s, bank robbers, burglars, and car thieves populated the list. The 1960s saw fugitives wanted for kidnapping, sabotage, and destruction of government property. Members of organized crime groups and murderers were present on the lists of the 1970s. Drug kingpins and serial killers were a priority in the 1980s. And in the 1990s, the list reflected the increasing threat of international criminal activity.

Over the past two decades, the Top Ten list has focused on the most violent of fugitives sought for homicides, armed robberies, gang activities, and mass shootings.

In the earliest days, wanted posters would be placed in local post offices, and information on offenders was provided to newspapers. This quickly was supplemented with radio shows and television programs. As media has changed over the years, so have the FBI's outreach methods.

There are two main criteria for adding an individual to the list. First, they have to be considered dangerous—based on crimes already committed—or likely to continue committing crimes. Second, a fugitive may be added if investigators believe publicity will help lead to the fugitive's arrest. Not all fugitives meet both criteria.

All fugitives on the list are considered armed and dangerous. If you come across one of the Top Ten fugitives, contact the FBI's toll-free tip line at 1-800-CALL-FBI (225-5324) or submit a tip online at tips.fbi.gov.





THE OKLAHOMA CITY BOMBING

25 YEARS LATER

On the morning of April 19, 1995, FBI Special Agent Barry Black was tracking a white-collar fugitive a few miles from downtown Oklahoma City when he heard a loud blast in the distance.

Soon after, Black was pulled from his fugitive case to begin working the massive investigation of the deadly bombing that took the lives of 168 people, including 19 children, at the Alfred P. Murrah Federal Building.

The efforts of Black and scores of federal, state, and local investigators led to the convictions of Timothy McVeigh and

his co-conspirators, Terry Nichols and Michael Fortier, in one of the worst homegrown terrorism cases in the nation's history.

"It was a group effort. I was there doing my part just like everyone else," said Black, who recently retired from the FBI.

The Oklahoma City bombing introduced a frightening new concept for the United States: homegrown terrorism. Until the 1993 World Trade Center bombing, the country hadn't witnessed an event of this magnitude, let alone one carried out by American citizens. The event shaped the FBI's approach to investigating terrorism.



GIVING FAMILIES A LIFT

VOLUNTEERS FROM FBI PHILADELPHIA ASSIST FAMILIES WITH SICK CHILDREN



Nicole Fucci is a busy mom with a lot on her mind—she has a young son and a full-time career in law enforcement. Fucci is juggling work and family while her 18-month-old son, Trek, is a patient at Children’s Hospital of Philadelphia (CHOP). He has spent most of his life there.

Trek was born with an underdeveloped lymphatic system. Since his birth, he has had more than 75 surgeries to attempt to repair this system, which drains the body’s fluids. Trek is at CHOP to receive care from one of the few doctors in the world who specializes in this rare condition.

Fucci works full-time as a sheriff’s deputy in Jefferson Parish, Louisiana. She travels to Philadelphia as often as she can to see her son and her husband, Mark, who stays with Trek.

But one thing Fucci doesn’t have to worry about is who will drive her to and from Philadelphia International Airport. When Fucci arrived on a late-night flight from Louisiana in early March, a familiar face was there to greet her at the airport—retired FBI Special Agent Tom Cotton. Fucci calls him “Mr. Tom,” in the Southern tradition.

During their drives between the airport and the Fuccis’ temporary home near the hospital, Cotton often regales Fucci with stories from his agent days. They bond over their shared law enforcement backgrounds.

As a volunteer with an organization called Casey’s Companions, Cotton does this regularly for different families. Casey’s Companions volunteers are current and retired FBI employees who, in their off-duty hours, help law enforcement families whose children are going through treatment at CHOP.

The organization was created in memory of Casey Doolin, the daughter of retired FBI Philadelphia Assistant Special Agent in

Charge Jim Doolin. In 2012, during her senior year in college, Casey was diagnosed with leukemia. She began extensive treatments at CHOP, including two bone marrow transplants. Unfortunately, Casey lost her battle. She died in 2013 at age 23.

The Doolin family lived close enough to CHOP that they didn’t need much outside help when Casey was being treated there. But the family noticed how many children come to the hospital from all over the world and the challenges that presents.

Casey loved children and was passionate about serving those less fortunate than her. So it was a natural fit for Doolin to create Casey’s Companions and something he felt called to do.

“You’re in a club that no one wants to be in,” Doolin said of losing his daughter. “You can let it impact you and take you down, or you can help make today a little better than yesterday for a family with a child at CHOP. We’re grateful for the opportunity to honor our daughter’s memory by helping children and families in our law enforcement community.”

When a law enforcement family arrives at CHOP, a Casey’s Companion representative meets with them to gauge what the family needs. Typical services the group offers include transportation, meals, hospital navigation, errands, and support from an FBI chaplain. Since the group’s creation, they have worked with about 50 families.

“We spend our days working to protect the community, but law enforcement also has personal and family lives, and they find time to give back to their communities,” Doolin said. “This is something the Philadelphia office does and joins a long history of the FBI helping their law enforcement partners.”

MYFBI DASHBOARD APP



Quickly access customizable website and social media content from the FBI in one convenient spot on your mobile device with the myFBI Dashboard app.

From catching up on the Bureau's latest stories and podcasts to following FBI social media feeds and learning about wanted fugitives, the myFBI Dashboard app brings everything to your fingertips.

Download the myFBI Dashboard app on the App Store or Google Play.

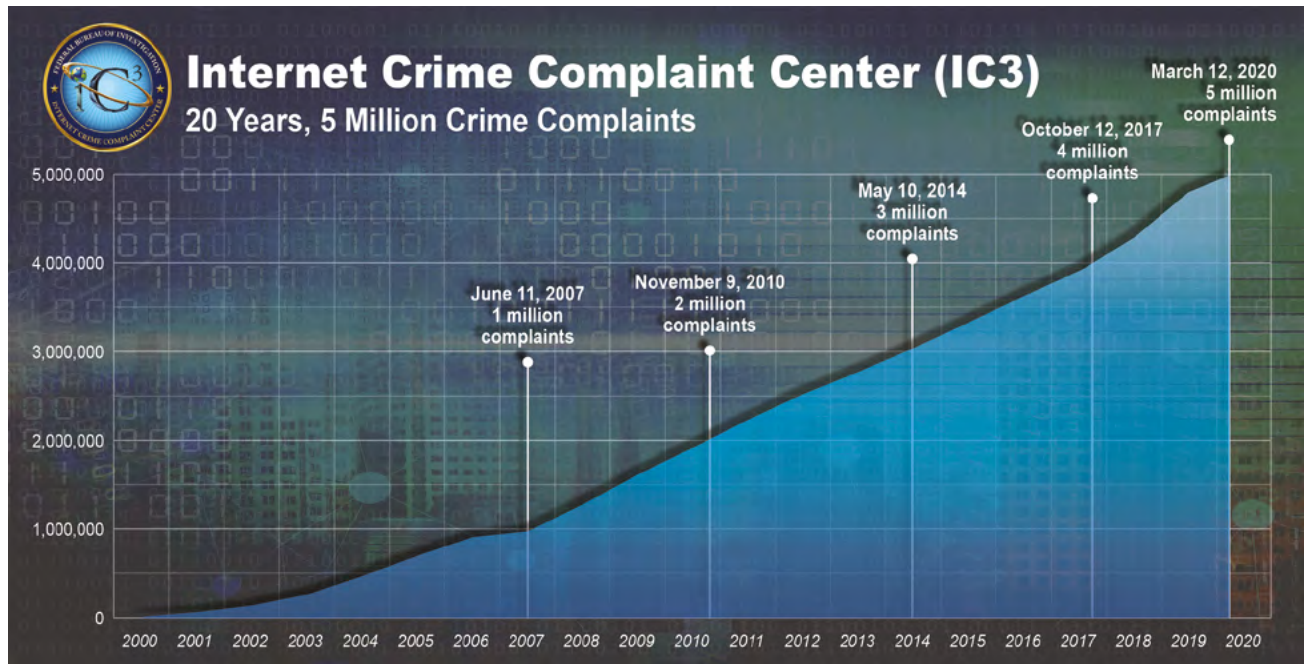
CUSTOMIZE. CLICK. CONNECT.

QUICKLY ACCESS CUSTOMIZABLE WEBSITE AND SOCIAL MEDIA CONTENT FROM THE FBI IN ONE CONVENIENT SPOT WITH **myFBI Dashboard**.



INTERNET CRIME COMPLAINT CENTER MARKS 20 YEARS

IC3 HAS TRACKED THE EVOLUTION OF ONLINE CRIME



Throughout the 1990s, Americans took to the internet in droves. The decade saw the launch of the first web browsers, the introduction of now ubiquitous search engines, the birth of online commerce, and the ascendance of email as a go-to mode of communication.

As this new landscape bloomed, so did opportunities for criminals. The web offered easy access for cyber actors to target hundreds or even thousands of people at relatively low cost and risk.

When these crimes started occurring more frequently, the public was unsure where to turn for help. "People really didn't know where to report internet scams or other online fraudulent activity," said Internet Crime Complaint Center (IC3) Chief Donna Gregory. "And law enforcement agencies were saying: 'What do we do with these? How do we handle them?'"

Recognizing the need to collect and assess information on cyber crime, the FBI started the Internet Fraud Complaint Center in May 2000 as a pilot project with the National White Collar Crime Center.

That center turns 20 this month. Renamed the Internet Crime Complaint Center (IC3) in 2002, the IC3 logged its 5 millionth

complaint in March 2020. All that data has improved the public's awareness of online crimes and helped the FBI and other law enforcement agencies better address internet-enabled attacks, fraud, thefts, and scams.

The crimes catalogued by the IC3 mirror the evolution of the web across two decades—growing in sophistication and number as the internet grows ever more essential to our professional and personal lives.

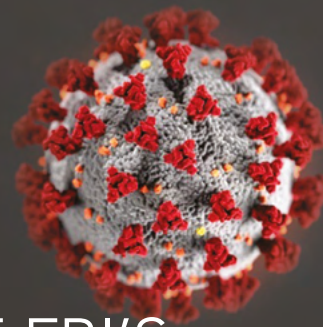
Losses recorded by the IC3 in recent years reflect the greater financial damage of this evolution. In 2019, victims reported more than \$3.5 billion in losses—an average of \$7,500 for each of the 467,361 complaints recorded that year. In 2001, the average victim lost \$435.

The IC3 collects and reports out its data in an annual report and educates the public by sending out notices about new scams or upticks in certain type of crimes. Its other key role is to support law enforcement. Federal, state, local, and tribal agencies can access the IC3's data through a secure database.

To report a crime or see the IC3's annual reports and warnings about current crimes, scams and frauds, visit ic3.gov.

STAYING SAFE DURING THE PANDEMIC

PROTECTING CHILDREN AND UNCOVERING SCAMS CENTER OF FBI'S COVID-19 RESPONSE



While the COVID-19 crisis has changed so much about daily life, it has also been a boon for criminals and con artists. But the FBI and our partners are working to protect your family and your wallet.

"The FBI and our law enforcement partner agencies are very much open for business, and we've been very successful in finding and prosecuting COVID-related cases," said FBI Financial Crimes Section Chief Steven Merrill.

Crimes Against Children

Since the onset of the pandemic, school, work, and many other aspects of social life have moved online. And while these tools help keep people connected while they are apart, the FBI has seen a disturbing new crime emerge. Criminals are using virtual meeting platforms like Zoom to broadcast child sexual abuse material to unwitting participants of school, church, or other online gatherings.

The FBI has seen more than 300 of these incidents in the last three months, according to Leonard Carollo, chief of the FBI's Crimes Against Children and Human Trafficking Unit.

Perpetrators usually target a large, openly publicized Zoom meeting. So if you're organizing a Zoom meeting, remember to use a password, disable screen sharing, and never share a Zoom link on an open social media account or website. Instead, send the link individually to each participant.

If you've witnessed the broadcast of child sexual abuse material during a virtual meeting, notify the FBI. Each time child sexual abuse material is viewed, the child involved is re-victimized. That's why broadcasting these images and videos is a serious violent crime, and the FBI is committed to apprehending both those who distribute the material and those who create these egregious images and videos.

"A participant who inadvertently views these images or videos can also be severely traumatized by just seeing this material," Carollo said. "These are very young children who are being sexually abused. Our goal is to identify and apprehend the people responsible for these horrific images and videos."

The FBI is also concerned about a rise in sextortion as children spend more time online and out of school. Carollo encouraged parents to have candid discussions with their children about the dangers of the internet.

"Online child sexual exploitation occurs everywhere, during all times of the year, in big cities and small towns. No one is immune," Carollo said. "The nature of the internet is people have access to anyone anywhere in the world. So parents need to talk with their children about these online dangers."

Financial Crimes and Scams

Although fraud schemes from the early days of the coronavirus pandemic are still happening, many scammers have now turned their attention to two new targets—unemployment insurance and the Paycheck Protection Program. Merrill says that the FBI is investigating dozens of cases every day of suspected fraud against both programs.

With the Paycheck Protection Program, scammers try to get loans to pay employees they don't have or to support businesses they created just to get government benefits. Criminals are also using stolen identities to file unemployment claims and pocketing the funds for themselves.

The FBI is working closely with other agencies, as well as banks, to uncover this fraud.

Because banks notify the FBI of suspicious activity, many criminals use money mules to hide their crimes. Everyone should learn about money mules and understand that if you're participating in a scheme like this, you're supporting criminal activity.

"People receiving and moving money believe they're doing this for a job or a request of someone, but what they're doing is collecting criminal proceeds and laundering them," Merrill said.

Tips from the public have also been vital in investigating these cases, and Merrill encouraged the public to report tips to tips.fbi.gov or ic3.gov.

"Every dollar that is illegally routed to a criminal is money out of the pocket of a small business owner or an employee," Merrill said. "A lot of businesses operate month to month, so time is of the essence to get this lifeline of support to them. We're working to get the funds out of the hands of criminals and back to those who deserve them."

Federal Resources

- For accurate and up-to-date information on COVID-19, please visit coronavirus.gov and cdc.gov/coronavirus
- Learn about the FBI's response at fbi.gov/coronavirus
- Learn about the Department of Justice's response at justice.gov/coronavirus
- Learn more about what the federal government is doing at usa.gov/coronavirus

'EMPATHETIC PIONEER' RETIRING KATHRYN TURMAN LED CREATION, EXPANSION OF FBI'S VICTIM SERVICES



On the eve of her college commencement in 1976, Kathryn Turman and her roommate—like many of their fellow seniors—pondered how their lives would unfurl in the years ahead.

The roommate dreamed of being a teacher and followed that path. Turman, who majored in sociology, wasn't as certain about the way forward. But she had an earnest goal: "I knew I wanted my life to be more than just long," she said. "It was a desire to make a contribution."

Now, on the verge of her retirement as assistant director of the FBI's Victim Services Division (VSD), Turman is arguably the Bureau's most consistently called-upon contributor. She presided over the FBI's victim-centered responses to every major case since 9/11, including the Boston Marathon

bombings, multiple mass-casualty shootings, international kidnappings and murders, and scores of federal crimes.

Her division ensures that crime victims in FBI cases are tended to and provided resources—as required by federal law. It has grown under her watch from a handful of well-intentioned staff to a world-renowned corps of more than 300 specially trained personnel.

"I'm very proud of where VSD has come and the people that are a part of it," said Turman. "I think building the team that I have—and I haven't done it alone—and professionalizing and hiring good people and letting them do their work and develop the program—that's what I'm most proud of."



'MILES OF FILES'

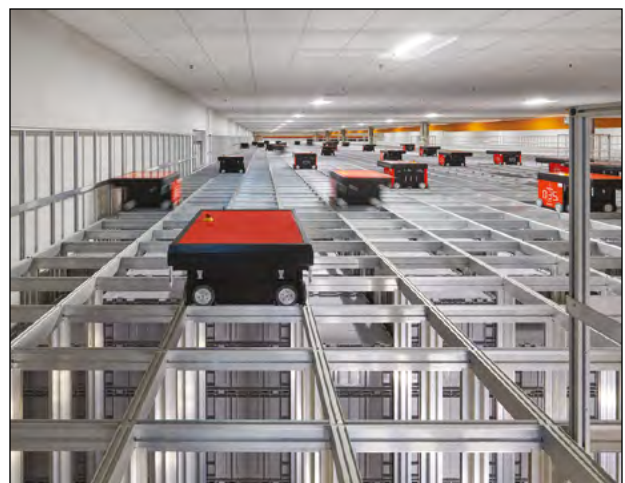
ROBOTS HELP MANAGE BILLIONS OF PAGES AT FBI CENTRAL RECORDS COMPLEX

Inside the Bureau's cavernous new Central Records Complex in Winchester, a squad of automated, wheeled robots has dutifully begun the enormous task of filing away millions of paper records from FBI offices around the country.

The 256,000 square-foot facility, located about 90 minutes from Washington, D.C., will consolidate the storage of truckloads of archived records now housed at each of the FBI's 56 field offices and other sites.

Work on the \$135 million warehouse began in late 2017. The complex opened earlier this year, and in June, staff began loading the first records into custom-designed bins to be shuttled away by robots into darkened, climate-controlled confines for safekeeping and easy retrieval.

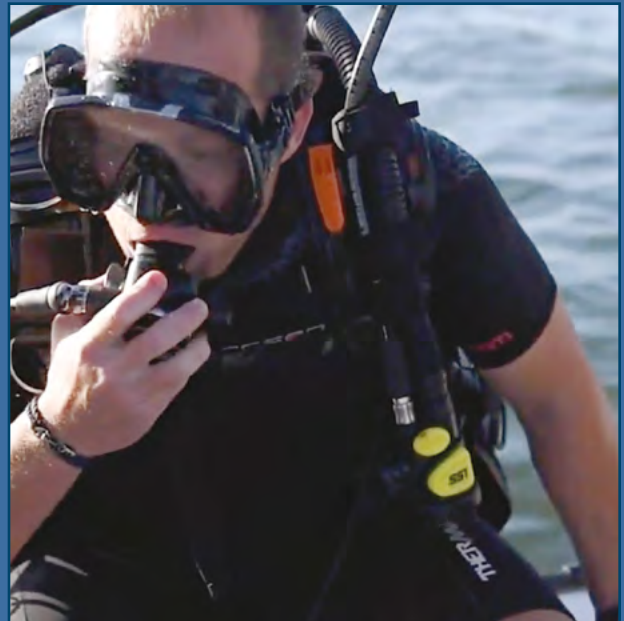
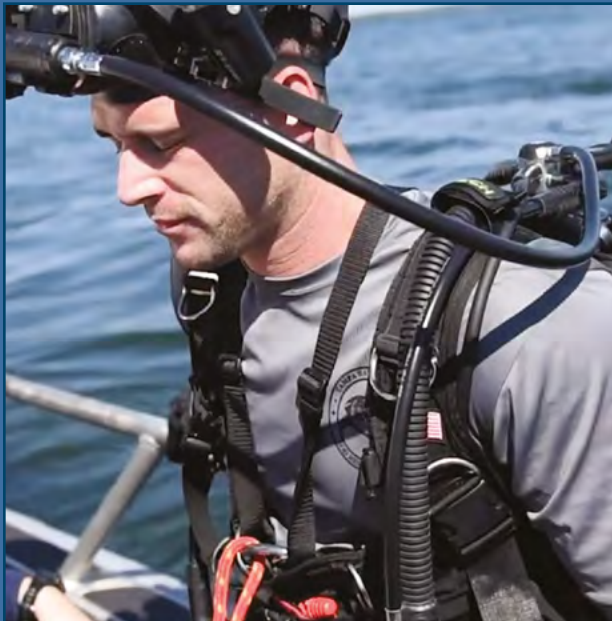
The warehouse complex and its state-of-the-art automated storage and retrieval system is one of the biggest in the world. The National Archives and Records Administration (NARA) partnered with the FBI on the facility's design and standards.



DANGER BENEATH THE SURFACE

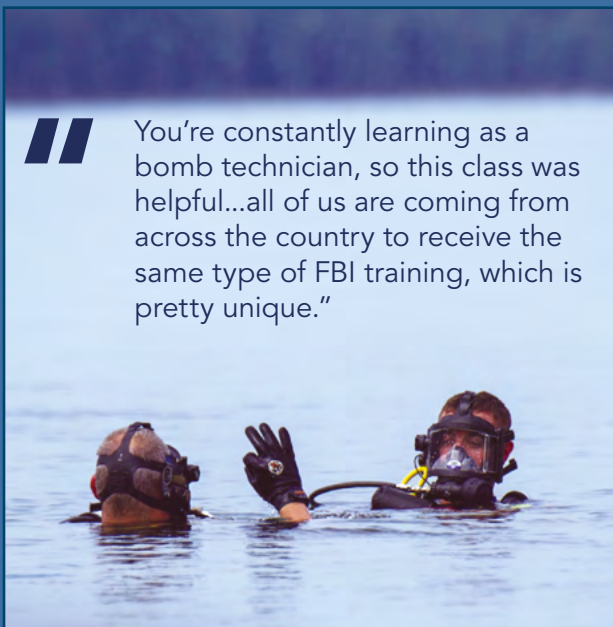
INSIDE THE FBI'S UNDERWATER POST-BLAST INVESTIGATION COURSE

The FBI's Underwater Post-Blast Investigation course prepares the nation's public safety bomb tech divers to counter threats in their home harbors and waterways.





You're constantly learning as a bomb technician, so this class was helpful...all of us are coming from across the country to receive the same type of FBI training, which is pretty unique."



OPERATION LEGEND

EFFORTS ARE TARGETING AN INCREASE IN VIOLENT CRIME



In support of Operation Legend, the FBI is combining resources with its federal, state, and local law enforcement partners in nine cities where there has been a troubling uptick in violent crime.

The initiative was named after a 4-year-old boy, LeGend Taliferro, who was killed by gunfire while asleep in his Kansas City, Missouri, home. LeGend's city was the first area to receive additional resources when Attorney General William Barr announced the launch of Operation Legend on July 8, 2020.

The operation has since expanded to include support for Albuquerque, Chicago, Cleveland, Detroit, Indianapolis, Memphis, Milwaukee, and St Louis.

"There's been a significant increase in violent crime in various parts of the country," said Calvin Shivers, the assistant director

of the FBI's Criminal Investigative Division. "Operation Legend is an initiative to surge resources across the Department of Justice to those cities to address that spike in crime."

Shivers said the FBI has provided additional agents, but has also brought in support from across the Bureau. The FBI's intelligence analysts, digital evidence experts, field office personnel, and professional staff are supporting efforts to get to the root causes of the crime increases in Kansas City, Chicago, and other Operation Legend cities.

"What we bring to the table is the ability to target some of the most violent offenders in the short term while pursuing a longer term strategy to dismantle entire criminal organizations," Shivers said.

"Operation Legend has allowed us to surge additional resources to these areas that are seeing an unacceptable increase in violence," said FBI Deputy Director David Bowdich. "These crimes unsettle communities and threaten the sense of safety we all deserve to have when we put our children to bed at night or when we step out in our neighborhoods."

Operation Legend has already produced results. One of the most heartening developments was the arrest of a suspect in the murder of LeGend Taliferro on August 13.

Within the first 30 days, efforts in Kansas City resulted in more than 200 arrests, according to U.S. Attorney Tim Garrison. Among those apprehended were suspects in homicides, assaults, robberies, and drug trafficking.

"There is a significant uptick in violent crime in Kansas City, and while every agency participating in this operation has a different role and responsibility, fighting violent crime is a responsibility we all share," said FBI Kansas City Special Agent in Charge Timothy Langan.

Shivers said that since mid-July, the FBI has opened 111 new cases, made 116 arrests, and recovered 92 firearms across the Operation Legend cities.

"What we want to do," Shivers said, "is have a significantly positive impact on an entire community that's being affected by violent crime."

Wanted or Seeking Information

Operation Legend is a coordinated initiative across law enforcement to address a recent surge in violent crime, especially gun violence.

If you have any information on the cases found at fbi.gov/operationlegend, please contact the FBI at tips.fbi.gov or 1-800-CALL-FBI. Tips can be submitted anonymously.

DIRECTOR'S COMMUNITY LEADERSHIP AWARDS

A DISTANT BUT HEARTFELT CELEBRATION OF DCLA RECIPIENTS

In light of health and travel concerns related to COVID-19, the annual ceremony celebrating the Director's Community Leadership Awards (DCLA) at FBI Headquarters was canceled this year.

FBI Director Christopher Wray and the entire FBI family missed the opportunity to celebrate in person with the DCLA recipients, but we honor their service no less.

"Although we were not able to honor these amazing recipients in person this year, we hope our gratitude for their extraordinary contributions will be felt through the awards package each of them will receive," said Lorie Campbell, who chairs the event for the FBI's Community Relations Unit.

While the current health emergency prevented the DCLA celebration from taking place, it has underscored how much we need those who give of themselves to lift up families, neighborhoods, and towns.

The DCLAs honor organizations and individuals who are doing the hard work of improving their communities. This year, many of the awardees were recognized for supporting the FBI's mission and fostering the Bureau's connections to those we serve.

Others are addressing urgent needs through addiction services or supporting adults and children affected by human trafficking, trauma, and abuse. Many of the awardees stepped up when natural disasters or tragedies affected their communities. And others turned personal hardships into action.

"Instead of waiting for someone else to take the initiative to make our streets safer or our future brighter, you acted," FBI Director Christopher Wray said in a message to the awardees. "You rolled up your sleeves and righted a wrong."

The FBI celebrates and thanks each of the DCLA recipients. We honor your work, dedication, and service.





We want to make sure we're doing everything we can to help our partners do what they need to do."

FBI STRATEGY ADDRESSES EVOLVING CYBER THREAT

WRAY EMPHASIZES PARTNERSHIPS TO COMBAT THREATS AND IMPOSE GREATER COSTS TO CYBER ACTORS

FBI Director Christopher Wray announced the Bureau's new strategy for countering cyber threats in remarks at the National Cybersecurity Summit.

The strategy, Wray explained, is to "impose risk and consequences on cyber adversaries"—making it harder for both cyber criminals and foreign governments to use malicious cyber activity to achieve their objectives.

"We've got to change the cost-benefit calculus of criminals and nation-states who believe they can compromise U.S. networks, steal U.S. financial and intellectual property, and hold our critical infrastructure at risk, all without incurring any risk themselves," he said.

The centerpiece of the new strategy is the role the FBI plays as an "indispensable partner" to federal counterparts, foreign partners, and private-sector partners. "We want to make sure we're doing everything we can to help our partners do what

they need to do," said Wray. "That means using our role as the lead federal agency with law enforcement and intelligence responsibilities to not only pursue our own actions, but to enable our partners to defend networks, attribute malicious activity, impose sanctions for bad behavior, and take the fight to our adversaries overseas."

The strategy recognizes that no single agency—or even government—can combat cyber threats alone, and that when possible, actions by the FBI and its partners will be sequenced for maximum impact.

Wray said that the most significant current threats are coming from the Chinese government targeting our intellectual property, Russian efforts to undermine our critical infrastructure, and increasingly sophisticated criminal cyber syndicates that seek to steal from individuals and institutions.

COMBATING THE IRANIAN CYBER THREAT

REPUBLIC AT CENTER OF CYBER CRIME CHARGES IN THREE CASES



Criminal charges against multiple alleged hackers in Iran show the breadth of the cyber threat emanating from that country and the FBI and partner agency efforts to neutralize it and hold the individuals accountable.

The hacks included cyber intrusions and fraud, vandalism of U.S. websites, and intellectual property theft from U.S. aerospace and satellite technology companies. In each of the cases, the suspects were believed to be operating at the behest of the Iranian government, or in support of it.

While the cases filed are separate and unique, prosecutors and FBI investigators said they send a message that hackers will face consequences regardless of distance and borders.

Behzad Mohammadzadeh, of Iran, and Marwan Abusrour, of the Palestinian territories, were indicted in Massachusetts on charges of damaging multiple websites as retaliation for U.S. military action in January that killed the head of the Islamic Revolutionary Guard Corps-Quds Force, a U.S.-designated foreign terrorist organization.

Hooman Heidarian and Mehdi Farhadi, both of Iran, were charged in New Jersey in connection with a coordinated cyber intrusion campaign. Investigators allege that the pair, sometimes at the behest of the government of Iran, targeted computers in New Jersey and around the world. In addition to stealing hundreds of terabytes of sensitive data, the defendants also vandalized websites, often under the pseudonym "Sejeal," and posted messages that appeared to signal the demise of Iran's internal opposition, foreign

adversaries, and countries identified as rivals, including Israel and Saudi Arabia.

And an indictment unsealed in Virginia charged Said Pourkarim Arabi, Mohammad Reza Espargham, and Mohammad Bayati, all living in Iran, with engaging in a coordinated campaign of identity theft and hacking on behalf of Iran's Islamic Revolutionary Guard Corps, a designated foreign terrorist organization. According to the charges, the defendants' campaign began in 2015. At one time, they had a target list of more than 1,800 online accounts, including those of aerospace or satellite technology and international government organizations in Australia, Israel, Singapore, the United States, and the United Kingdom. The three allegedly used social engineering techniques to make contact with those on the target list and assume their identities online. This allowed the defendants to send messages to other unsuspecting individuals that contained malware hidden in links and documents. The malware allowed the hackers access to many additional computer systems.

The FBI also released the details of eight separate and distinct sets of malware used by a front company in Iran to raise awareness of the threat and provide tools to help companies defend their computer networks.

The efforts were reflective of the FBI's new cyber strategy, which is to impose risk and consequences on cyber adversaries—making it harder for both cyber criminals and foreign governments to use malicious cyber activity to achieve their objectives.



LIFE AS AN FBI FIELD PHOTOGRAPHER

FBI field photographers are essential to conducting investigations. Jon Fletcher, a photographer in the FBI Jacksonville Field Office, shares some of his favorite projects, photos, and guidance for those seeking a career in law enforcement photography (see corresponding story online).





'EVERY SECOND COUNTS'

CARD TEAM DEVELOPS CHECKLIST TO AID SEARCHES FOR MISSING AUTISTIC CHILDREN



The search for a missing 6-year-old with autism in 2018 left a profound impression on the North Carolina community where the boy went missing—and on the FBI's teams that specialize in finding children who suddenly disappear.

Hundreds of law enforcement and search and rescue personnel assisted in the search for Maddox Ritch, who walked away from a park in Gastonia on September 22, 2018. His body was found five days later partially submerged in a creek near the park. His drowning was accidental and it likely occurred soon after he disappeared. But the outcome—following extraordinary search efforts that included playing the boy's mother's voice and music he liked over a loudspeaker to draw him out—left some wondering how they can better prepare for the next time.

Since then, a special agent on the FBI team that assisted in the search for Maddox has developed a one-page questionnaire for investigators to use when a child with autism goes missing.

"I wanted to make sure that if I had another opportunity, I'd be ready," said Special Agent James Granozio, who works in

the Bureau's Charlotte Field Office and also leads one of the FBI's four regional Child Abduction Rapid Deployment (CARD) Teams. These teams are composed of agents, intelligence analysts, operational specialists, and behavioral analysts who deploy on short notice when police departments request FBI assistance in missing child cases.

After the Maddox case, Granozio learned all he could about autism and autistic children, reaching out to local and national organizations for information. The feedback led to the development of the checklist of baseline questions that Granozio said should be asked immediately of parents or caregivers of missing autistic children.

"I want to know from the family early on: Does the child have a tracking mechanism? Is the child afraid of water or do they like water? If they like water, do they know how to swim?" said Granozio. "What about traveling at night? Is the child scared at night? Will they hunker down or will they like to move? All these things I want to know early on, and hopefully we can save a life."

One of the autism specialists Granozio contacted during his research said the checklist was a good idea, particularly if time is critical. "Having a checklist and a fact sheet about a child can be very helpful, especially if the child has specific interests," said Kim Stroble, clinic director of the Early Autism Project in Rock Hill, North Carolina. "Given that no child or person with autism is the same, I think this is great."

The questionnaire has been circulated among the FBI's CARD Team, which includes approximately 75 members in FBI field offices across the country. They, in turn, have distributed the

material to local law enforcement agencies during training exercises on child abductions and joint search and rescue operations. The CARD Team holds multiple table-top-style exercises every year to prepare local law enforcement on how to properly respond to the infrequent events.

The questionnaire, which is only available to law enforcement, has been part of the CARD Teams' deployment toolkits for more than a year now and is one of the rare positive developments from the Maddox Ritch case.



OPERATION DISRUPTOR

JCODE ACTIONS SHUT DOWN MAJOR DARKNET DRUG VENDOR

The storage shed by the modest yellow stucco house in Sunland, California, was tidy and organized. Mailing supplies, tape, and materials were stacked or sorted into labeled bins, and a large box held packages that were addressed and ready to be dropped at the post office. It looked like a run-of-the-mill mail-order business. Until the search went further into the space.

There, agents from the FBI, United States Postal Inspection Service (USPIS), and Homeland Security Investigations (HSI) found about 50 pounds of methamphetamine and bags and containers full of thousands of Adderall pills. There were also scales, package sealers, and three firearms.

Each of those packages that were filled or waiting to be filled would bring drugs to someone in the United States—where an individual is now more likely to die of a drug overdose than in a car accident.

The search of a second site used to package drugs for the same operation yielded another huge supply. Agents uncovered well over 100 pounds of methamphetamine and some 30,000 pills in the two locations—a bundle of dangerous drugs worth several million dollars.

The two search operations, combined with law enforcement actions in other locations and at later dates, led to the arrests of multiple people linked to an online drug trafficking organization that sold under several monikers on the darknet. The individuals are now facing some combination of narcotics

trafficking, conspiracy, money laundering, and firearms charges that could lead to sentences of between 10 and 25 years in federal prison.

Law enforcement believes this may be one of the biggest bulk methamphetamine darknet seller yet uncovered. Investigators said that the evidence indicates that the group was supplying other darknet vendors and street drug dealers in addition to shipping drugs to individual buyers throughout the U.S. and abroad.

These operations in the Los Angeles area and similar efforts throughout the U.S. and Europe were part of a concentrated effort called Operation DisrupTor, carried out by the partner agencies that form the Joint Criminal Opioid Darknet Enforcement (JCODE) team. Law enforcement here and abroad arrested 179 individuals and seized more than 500 kilograms of illegal drugs as part of Operation DisrupTor.

Created in 2018, JCODE combines the efforts of the FBI, USPIS, HSI, Drug Enforcement Administration (DEA), U.S. Customs and Border Protection, Department of Justice, Financial Crimes Enforcement Network, Naval Criminal Investigative Service, Department of Defense, and Bureau of Alcohol, Tobacco, Firearms and Explosives. As many of these markets cross borders, Europol is also an invaluable international partner in JCODE's work to make a global impact on darknet drug trafficking.





NEW TOP TEN FUGITIVE

“EL GATO” ALLEGEDLY HAD VICTIM TRACKED AND MURDERED



FBI TEN MOST WANTED FUGITIVE

JOSE RODOLFO VILLARREAL-HERNANDEZ

Interstate Stalking and Conspiracy to Commit Murder-for-Hire

Photograph taken in 2014

Photograph taken in 2011

DESCRIPTION	
Alias: "El Gato"	
Date(s) of Birth Used: January 16, 1978	Place of Birth: Mexico
Hair: Black	Eyes: Brown
Height: 5'4"	Weight: 165 pounds
Sex: Male	Race: White (Hispanic)
Nationality: Mexican	Language(s): Spanish

REWARD
 The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to \$1 million for information leading directly to the arrest of Jose Rodolfo Villarreal-Hernandez.

REMARKS
 Jose Rodolfo Villarreal-Hernandez has ties to or may visit Monterrey, Mexico and Mexico City, Mexico.

CAUTION
 Jose Rodolfo Villarreal-Hernandez, also known as "El Gato," is wanted for his alleged involvement in the interstate stalking and conspiracy to commit murder-for-hire of a 43-year-old male victim on May 22, 2013, in Southlake, Texas. A federal arrest warrant for these charges was issued on June 20, 2018. Villarreal-Hernandez allegedly holds an active leadership position in the Beltran Leyva drug-trafficking organization within the region of San Pedro Garza Garcia, Tlaxcala, Mexico.

SHOULD BE CONSIDERED ARMED AND EXTREMELY DANGEROUS

If you have any information concerning this person, please call +1 817-213-6640 through the WhatsApp mobile application. You may also call 1-800-CALL-FBI or contact your local FBI office or the nearest American Embassy or Consulate. Tips can also be provided online at tips.fbi.gov.

Field Office: Dallas

Jose Rodolfo Villarreal-Hernandez, wanted for allegedly directing his associates to track and murder a man in Southlake, Texas, has been added to the FBI's Ten Most Wanted Fugitives list. The Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to \$1 million for information leading directly to his arrest.

Villarreal-Hernandez, also known as "El Gato," is believed to hold an active leadership position in the Beltran Leyva Drug Trafficking Organization within the region of San Pedro Garza Garcia, Nuevo Leon, Mexico. He is also believed to be responsible for numerous murders in Mexico.

The victim of the Texas murder, 43, was shot while sitting in the passenger seat of his vehicle outside an upscale shopping center in a Dallas-Fort Worth suburb on May 22, 2013. His wife was standing near the driver's side door when her husband was killed. And the brazen ambush occurred in the early evening hours, while the center was full of shoppers.

According to evidence and testimony gathered in the trials of those accused of tracking and killing the man, Villarreal-Hernandez ordered and financed a multi-year effort to find and watch the victim and then kill him. Investigators believe Villarreal-Hernandez had a long-standing personal grudge against the victim.

Several of the individuals involved in tracking and killing the victim have already pleaded guilty, have been tried and convicted, or are awaiting trial in federal court.

"The fact that Villarreal-Hernandez was willing to send people to the United States to track someone within the United States and then execute that person in a neighborhood in Texas—we need to set the example that this will not be tolerated," said Special Agent Gary Koenig.

Koenig has been investigating Villarreal-Hernandez with the FBI's Dallas Field Office since the shooting occurred in 2013. El Gato's apparent role in trafficking drugs into the United States and the evidence linking him to more than 10 murders in Mexico have made this case a top priority for both U.S. and Mexican authorities. "He's a ruthless guy," Koenig said.

The FBI and Mexican authorities feel the publicity of the Top Ten list and such a large reward will help generate the tips they need to bring El Gato to justice.

Villarreal-Hernandez is 42 years old. He has black hair and brown eyes and stands 5 feet 4 inches tall. He is believed to weigh about 165 pounds and is likely hiding in Mexico. Villarreal-Hernandez should be considered armed and extremely dangerous.

Anyone with information on Villarreal-Hernandez's whereabouts should call 1-800-CALL-FBI, or contact your local FBI office or the nearest American Embassy or Consulate. You can also submit a tip online to tips.fbi.gov.

THE EYES HAVE IT

IRIS BIOMETRIC ADDED TO NEXT GENERATION IDENTIFICATION SYSTEM

The division of the Bureau that manages the national database of fingerprints recently implemented the Next Generation Identification (NGI) Iris Service, which gives the FBI and partner agencies the ability to capture, catalog, and make rapid comparisons of iris images with a high rate of accuracy.

The human iris—the part of the eye that controls the size of the pupil and defines one’s eye color—contains a unique pattern of ridges and folds that are specific to individuals. In the new system, which went in service on September 29, a subject’s irises are captured using a near-infrared camera, which takes just seconds. The FBI hopes law enforcement agencies will adopt the technology and incorporate it into their existing biometric processes, like police department booking stations or jail intakes and releases.

To date, the iris image repository contains 1.38 million enrollments submitted from federal, state, and local databases after they were collected during criminal bookings, incarcerations, or other legal proceedings. The iris images won’t replace fingerprints, which the FBI has collected and analyzed for nearly a century; they are a secondary biometric, or supplement, to the traditional collection of 10-finger prints and palm prints.

The Bureau’s fingerprint database—Next Generation Identification—contains more than 70 million prints of criminal

subjects and more than 30 million civil fingerprints from background checks.

During the pilot period, which began in September 2013, several correctional systems incorporated iris collection into their processes, which enabled staff to get positive identifications—without physical contact—on inmates as they transferred in and out of facilities. The seven-year pilot enabled the FBI to build the criminal iris repository as well as assess privacy policies, best practices, and other requirements.

In the new system, so-called probe images of a subject’s left and right irises are captured at close range in a controlled setting. The images can then be searched against all the irises in the FBI’s repository. The process takes about a minute. A match will return the subject’s biographic data along with their criminal record, select National Crime Information Center record data, and, in some cases, a mug shot.

The Iris Service is the latest addition to the Bureau’s NGI System, which is the world’s largest and most efficient electronic repository of biometric and criminal information. In addition to repositories for irises and fingerprints, NGI includes 30 million criminal mugshots that law enforcement partners can search against.



NEW CHARGES IN PAN AM FLIGHT 103 BOMBING

190 AMERICANS KILLED IN 1988 TERROR ATTACK; CASE REMAINS UNDER INVESTIGATION

Thirty-two years to the day after the terrorist bombing of a Pan Am jet over Scotland killed 270 people, including 190 Americans and 11 residents in the town of Lockerbie, federal investigators today announced charges against a Libyan man they say was involved in making the bomb.

The investigation has been open for more than three decades, even after a Libyan intelligence officer was convicted in 2001 on 270 counts of murder in the case in a Scottish court. The FBI, working closely with authorities in Scotland, has continued to pursue leads over the years pointing to others that may have been involved in the attack.

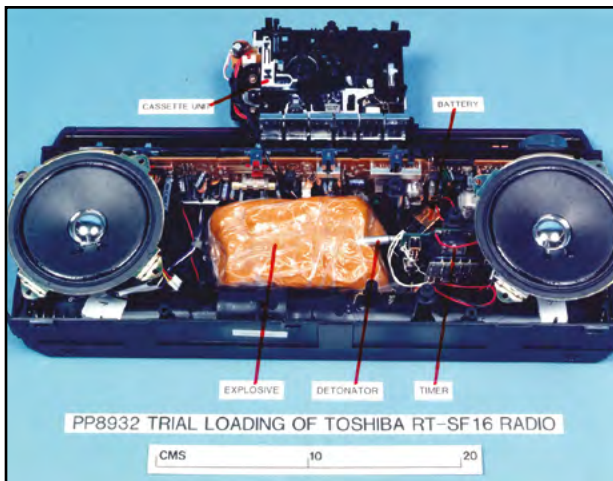
In a press conference in Washington, D.C., federal officials announced the criminal complaint against Abu Agela Mas'ud Kheir Al-Marimi for his alleged role in the attack. He is currently in prison in Libya.

The charges are the result of hundreds of interviews and leads that took investigators to 16 countries to pore over decades-old evidence. The investigation has relied heavily on foreign partners, many in Scotland, where remnants of the plane fell, creating an 845-square-mile crime scene.

The December 21, 1988 bombing, along with the ensuing investigation and the trial of two suspects in 2000, have



(AP Photo)



played pivotal roles in how the FBI works on international cases and how it serves victims of crimes. The Bureau's work with investigators in Scotland helped create a template for how the FBI handles international investigations. And the Bureau's Victim Services Division is modeled largely on the extraordinary compassion Lockerbie residents showed to victims' families in the delicate care they took to preserve and return personal effects collected during the early days and weeks of the investigation.

In 1991, the British and American governments charged Abdel Basset Ali al-Megrahi and Lamem Khalifa Fhimah in the case. Their trial in 2000 was held in Scottish court built for the occasion on a former U.S. military base in the Netherlands. The court acquitted Fhimah and convicted al-Megrahi in 2001, sentencing him to life in prison. He was released in 2009 when he was believed near death from cancer, but he survived almost three more years.

The new charges are the first in the case since 1991. Over more than three decades, victims' families have continued to

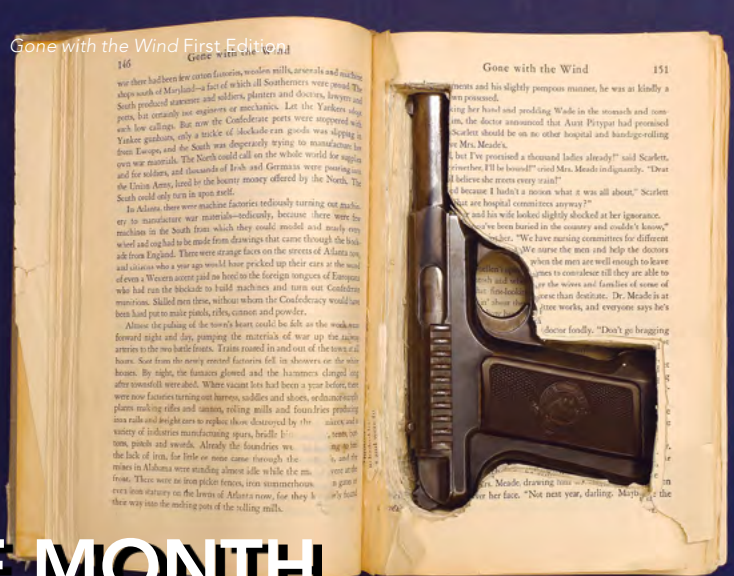
push to advance the investigation, believing the plot and its execution were not limited to Fhimah and al-Megrahi. Agents in the Washington Field Office, which has been leading the FBI investigation since the outset, have made repeated trips to countries with a nexus to the plot. And in private briefings, FBI officials have steadfastly assured victims' families the investigation remains robust and ongoing. Every year, for example, FBI and Scottish investigators meet with Victims of Pan Am Flight 103, Inc. to brief any developments. The meeting is held during Remembrance Week every fall at Syracuse University, which lost 35 study-abroad students in the bombing. They were flying home for the holiday break.

FBI Director Christopher Wray provided a reminder that the FBI's resolve does not diminish with the passage of time. "Today's announcement should remind the world that when Americans are harmed, the FBI and the United States government will never stop pursuing justice for our citizens, no matter where that takes us, how long it takes us to get there, or how difficult the road might be," he said.

Brinks Robbery Cap



Gone with the Wind First Edition



ARTIFACTS OF THE MONTH

View details on all artifacts of the month at fbi.gov/aotm.



Microdot Doll



Special Agent Barry Black's Hard Hat

Alarm Clocks from 2010 Times Square Bombing Attempt



Laptop from Operation Ghost Stories





9/11 Hijacker's Car



Charles "Pretty Boy" Floyd's Death Mask



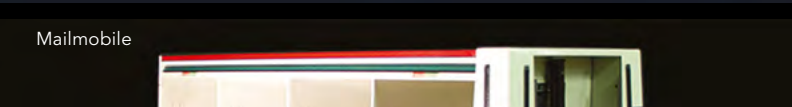
Ross William Ulbricht's Laptop



Richard Reid's Shoes



Eyemo Camera



Mailmobile



MORE AT [FBI.GOV/AOTM](https://www.fbi.gov/aotm)



FBI OFFICE OF PUBLIC AFFAIRS

935 Pennsylvania Avenue NW

Washington, D.C. 20535

