



governmentattic.org

"Rummaging in the government's attic"

Description of document: Federal Bureau of Investigation (FBI) Transition Briefing for the Incoming Biden Administration, 2020

Requested date: December 2020

Release date: 21-January-2025

Posted date: 02-June-2025

Source of document: FOIA Request
Federal Bureau of Investigation
Attn: Initial Processing Operations Unit
Record/Information Dissemination Section
200 Constitution Drive
Winchester, VA 22602
[eFOIPA submission portal](#)
[FOIA.gov](#)

The governmentattic.org web site ("the site") is a First Amendment free speech web site and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



Federal Bureau of Investigation

Washington, D.C. 20535

January 21, 2025

FOIPA Request No.: 1486150-000
Subject: Transition briefing documents prepared by
the FBI for the incoming Biden Administration

The FBI has completed its review of records subject to the Freedom of Information/Privacy Acts (FOIPA) that are responsive to your request. The enclosed documents were reviewed under the FOIPA, Title 5, United States Code, Section 552/552a. Below you will find check boxes under the appropriate statute headings which indicate the types of exemptions asserted to protect information which is exempt from disclosure. The appropriate exemptions are noted on the enclosed pages next to redacted information. In addition, a deleted page information sheet was inserted to indicate where pages were withheld entirely and identify which exemptions were applied. The checked exemptions used to withhold information are further explained in the enclosed Explanation of Exemptions:

Section 552

<input checked="" type="checkbox"/> (b)(1)	<input type="checkbox"/> (b)(7)(A)
<input type="checkbox"/> (b)(2)	<input type="checkbox"/> (b)(7)(B)
<input checked="" type="checkbox"/> (b)(3)	<input checked="" type="checkbox"/> (b)(7)(C)
<u>50 U.S.C. §3024(i)(1)</u>	<input type="checkbox"/> (b)(7)(D)
_____	<input checked="" type="checkbox"/> (b)(7)(E)
_____	<input type="checkbox"/> (b)(7)(F)
<input type="checkbox"/> (b)(4)	<input type="checkbox"/> (b)(8)
<input checked="" type="checkbox"/> (b)(5)	<input type="checkbox"/> (b)(9)
<input checked="" type="checkbox"/> (b)(6)	

Section 552a

<input type="checkbox"/> (d)(5)
<input type="checkbox"/> (j)(2)
<input type="checkbox"/> (k)(1)
<input type="checkbox"/> (k)(2)
<input type="checkbox"/> (k)(3)
<input type="checkbox"/> (k)(4)
<input type="checkbox"/> (k)(5)
<input type="checkbox"/> (k)(6)
<input type="checkbox"/> (k)(7)

86 preprocessed pages are enclosed. To expedite requests, preprocessed packages are released the same way they were originally processed. Documents or information originating with other Government agencies that were originally referred to that agency were not referred as part of this release. This material is being provided to you at no charge.

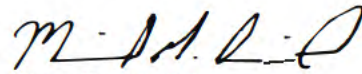
Please refer to the enclosed FBI FOIPA Addendum for additional standard responses applicable to your request. "Part 1" of the Addendum includes standard responses that apply to all requests. "Part 2" includes additional standard responses that apply to all requests for records about yourself or any third party individuals. "Part 3" includes general information about FBI records that you may find useful. Also enclosed is our Explanation of Exemptions.

Additional information about the FOIPA can be found at www.fbi.gov/foia. Should you have questions regarding your request, please feel free to contact foipaquestions@fbi.gov. Please reference the FOIPA Request number listed above in all correspondence concerning your request.

If you are not satisfied with the Federal Bureau of Investigation's determination in response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account following the instructions on OIP's website: <https://www.justice.gov/oip/submit-and-track-request-or-appeal>. Your appeal must be postmarked or electronically transmitted within ninety (90) days of the date of this response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." If possible, please provide a copy of your original request and this response letter with your appeal.

You may seek dispute resolution services by emailing the FBI's FOIA Public Liaison at foipaquestions@fbi.gov. The subject heading should clearly state "Dispute Resolution Services." Please also cite the FOIPA Request Number assigned to your request so it may be easily identified. You may also contact the Office of Government Information Services (OGIS). The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov, telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Sincerely,

A handwritten signature in black ink, appearing to read "M. G. Seidel", with a stylized flourish at the end.

Michael G. Seidel
Section Chief
Record/Information Dissemination Section
Information Management Division

Enclosures

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1486150-000

Total Deleted Page(s) = 18

Page 45 ~ b3; b5; b7E;
Page 46 ~ b3; b5; b7E;
Page 47 ~ b3; b5; b7E;
Page 48 ~ b5; b7E;
Page 49 ~ b5; b7E;
Page 50 ~ b1; b3; b5; b7E;
Page 51 ~ b1; b3; b5; b7E;
Page 52 ~ b1; b3; b5; b7E;
Page 53 ~ b1; b3; b5; b7E;
Page 54 ~ b5; b7E;
Page 55 ~ b5; b7E;
Page 56 ~ b5; b7E;
Page 57 ~ b5; b7E;
Page 58 ~ b5;
Page 59 ~ b5;
Page 62 ~ b5;
Page 72 ~ b1; b3; b5; b7E;
Page 76 ~ b1; b3; b5; b7E;

XXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXX

U.S. Department of Justice
Federal Bureau of Investigation



b6
b7C

CLASSIFIED BY: NSIDG [redacted]
REASON: 1.4 (D)
DECLASSIFY ON: 12-31-2045
DATE: 04-08-2024

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



The FBI:

*How We Protect
the American People
and Uphold
the Constitution*



OUR MISSION:

Protect the American People and Uphold
the Constitution of the United States



OUR MISSION PRIORITIES:

1. Protect the U.S. from terrorist attack
2. Protect the U.S. against foreign intelligence, espionage, and cyber operations
3. Combat significant cyber criminal activity
4. Combat public corruption at all levels
5. Protect civil rights
6. Combat transnational criminal enterprises
7. Combat significant white-collar crime
8. Combat significant violent crime

OUR CORE VALUES:

Respect • Integrity • Accountability
Leadership • Diversity • Compassion
Fairness • Rigorous Obedience
to the Constitution

(U) MESSAGE FROM THE FBI DIRECTOR

(U) The FBI's mission is simple to say but profound to execute: protect the American people and uphold the Constitution. Every day, the men and women of the FBI strive to carry out this mission. Whether it's thwarting a would-be terrorist, disrupting a spy ring, preventing cyber attacks, dismantling a dangerous gang, or returning a missing child to her family, our work never ends.

(U) Almost two decades after 9/11, many still do not fully understand the role of this national security organization. Whether investigating a threat through one of our many multiagency task forces, providing training to our international law enforcement partners, collaborating with the intelligence community on emerging technical capabilities, or producing intelligence for senior policymakers, the FBI's complementary intelligence and law enforcement capabilities uniquely position us to carry out our role as the lead for investigations of threats to the United States — both domestically and overseas.

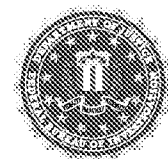
(U) For more than a century, our reputation as a premier intelligence and law enforcement organization has been based not so much on all our successes in addressing threats, but on the way we accomplish our work. At our best, we're focused on being true to our distinctive core values: respect, objectivity, and independence. Executing our mission with objectivity and independence and following the facts wherever they may lead, to whomever they may lead, is paramount. In recognition of these values, the FBI takes seriously the recommendations from various oversight elements' review of the Crossfire Hurricane investigation. We have made changes and will continue to make changes to strengthen our organization and ensure we exercise our authorities with objectivity and integrity.

(U) Transparency and accountability are the bedrock of ensuring we maintain the trust of the people we serve. As part of this effort, we share a wealth of material on our website about our organization and our work. To complement that information, the materials being shared with you provide a window into what we can't share with the public: the sensitive techniques and methods the FBI uses to carry out our mission to defend our nation from foreign adversaries, terrorists, criminals, and others who seek us harm.

(U) In these materials, you'll see four themes that describe the foundation of our work and the challenges we face. The first is about the FBI brand. It's about who we are and building on the brand that matters the most — not the views of the pundits or the prognosticators or the armchair critics, but the views of the people we actually do the work with and for. The second theme is a focus on partnership and teamwork in everything we do. The third is process — making sure we're not just doing the right thing, but also doing it in the right way. And the fourth is the need for innovation and a focus on the future.

(U) I hope these materials give you a better sense of who we are, and the depth and breadth of our unique role and capabilities. We look forward to meeting with you to tell you more about the work we do and how together we can carry out our oath and duty to the American people.

(U) Thanks for letting us share our story with you.



(U) TABLE OF CONTENTS



= FBI.gov resources available

(U// FOUO) THE FBI'S UNIQUE DOMESTIC ROLE	6
(U// FOUO) Investigations: Intelligence and Evidence.....	8
(U// FOUO) Innovation: Ahead of the Threat.....	13
(U) Current Threat Environment.....	16
(U) Partnerships and Engagement	17
(U) The People of the FBI	27
(U) Closing Summary.....	29
(U) AT-A-GLANCE	30
(U) The FBI	31
(U) Field Offices.....	33
(U) Legal Attaché Offices	35
(U) Diversity.....	37
(U) THREATS: 2020 AND BEYOND.....	39
(U) CHALLENGES	44
[Redacted]	45
[Redacted]	48
[Redacted]	50
[Redacted]	52
[Redacted]	54
[Redacted]	57
(U) FBI PROGRAM SPOTLIGHTS.....	60
(U) FBI Budget.....	61
(U) Internal Oversight and the Office of Inspector General.....	63
(U) FBI Background Investigations.....	65
(U) FBI Facilities	67
(U) FBI Cyber Strategy.....	70
[Redacted]	72
(U) FBI Critical Incident National Assets	73
(U// FOUO) National Security Threat Actor Global Detection Program.....	75
(U// FOUO) Information Technology Modernization Initiative	77
(U) Violent Crime	79
(U) Public Corruption	82
(U) FBI SUCCESSES	84
(U) Disrupting Foreign Intelligence Activities	85
(U// FOUO) Improved Intelligence Production for Policymakers	89
(U) Global Biometrics Initiative.....	91
(U) Victim Services Program	93
(U) ADDENDUM	96
(U) FBI.gov Resources	97
(U) Acronyms	99
(U) FBI Organizational Chart.....	103

b5
b7Eb1
b3
b5
b7E

~~(U//FOUO)~~ THE FBI'S UNIQUE DOMESTIC ROLE

(U) Every threat the nation faces — whether from terrorism, gang violence, espionage, or opioid abuse — is a threat to our national security. With more than a century of experience, the FBI's complementary intelligence and law enforcement capabilities and responsibilities make us uniquely positioned to address threats while protecting civil liberties. As both a component of the Department of Justice (DOJ) and a full and long-standing member of the U.S. Intelligence Community (USIC), the FBI serves as a vital link bringing the intelligence and law enforcement communities together to support policy decisions and protect the American people and uphold the Constitution.

~~(U//FOUO)~~ The FBI is the primary intelligence and law enforcement organization in the United States and the only member of theUSIC with broad authorities and responsibilities for carrying out investigations of threats to the United States — both domestically and overseas. In this role, the FBI is also responsible for coordinating clandestine collection of foreign intelligence and counterintelligence from human sources in the United States.

(U) Because of the FBI's authorities, we serve as the Domestic Director of National Intelligence (DNI) Representative. The FBI's lead role in establishing an integrated, coordinated, and focusedUSIC domestically enables the U.S. Government (USG) as a whole to inform and collaborate with our partners and mitigate threats. The FBI must understand the threats we face at home and abroad and how those threats may be connected. National security and criminal threats often intertwine, and the integration of intelligence and criminal investigations uniquely positions the FBI to identify and address threats and vulnerabilities across programs.

~~(U//FOUO)~~ The FBI has a responsibility not only to understand and identify foreign threats but also to act on this intelligence domestically to mitigate them. The Bureau does this by drawing on all our legal authorities — law enforcement and intelligence — to enable operational capabilities. The wall that separated national security and criminal investigations before 9/11 is no longer a barrier and it is important we not build it back.

~~(U//FOUO)~~ Arrest and prosecution are also valuable tools in this arsenal because the impact can reach far

beyond the individual, especially in the mitigation of threats. For instance, after the FBI issues an indictment in an investigation, other parts of the USG can use the intelligence gleaned to impose additional penalties on the responsible party — which may be a foreign nation-state actor. These actions include

[Redacted]


b3
b7E

(U) The FBI also shares with our public and private partners some of the intelligence and information we collect to help prevent and mitigate threats. As one example, to carry out our counterterrorism mission, FBI field offices may alert state and local law enforcement,USIC, and military partners, as needed, about a potential threat to swiftly coordinate and deconflict while jointly acting together to prevent an attack. As the agency responsible for investigating cyber threats from nation-states, terrorist organizations, and transnational criminal enterprises, the FBI may share information from these indictments with

b3
b7E

[Redacted] See the FBI's Cyber Strategy Spotlight for more information.

(U) FBI Authorities



~~(U//FOUO)~~ Federal law, Attorney General guidelines, and Executive Orders give the FBI jurisdiction to investigate all federal crime not assigned exclusively to another federal agency (28, Section 533 of the U.S. Code) and to investigate threats to our nation. (See Executive Order 12333, 50 U.S.C. 401 et seq.; 50 U.S.C. 4801 et seq.) This combination of authorities gives the FBI the unique ability to address national security and criminal threats that are increasingly intertwined and to shift between intelligence collection and criminal prosecution.

[Redacted]

~~(U)~~
b1
b3
b5
b7E

(U//~~FOUO~~) The FBI's reputation and law enforcement capabilities are renowned worldwide. Half of the FBI's mission priorities reflect this traditional law enforcement mission and the FBI's longstanding and continued important role in addressing federal crime and supporting our state and local law enforcement partners. The FBI plays a unique role as the sole agency responsible for protecting civil rights and combatting public corruption at all levels.

(U//~~FOUO~~) Although the FBI is not solely responsible for mitigating Transnational Organized Crime (TOC), the FBI has unique capabilities to address this threat. DOJ is the only department that can bring both criminal investigations and prosecution and intelligence authorities to bear against TOC targets. Because of these authorities, the National Security Council designated the FBI, through DOJ, as the executive agent (agency responsible for developing technical, policy, and governance mechanisms) for carrying out national policy for addressing TOC threat actors and providing vital information to both law enforcement and intelligence partners.

(U//~~FOUO~~) The FBI's international, state, local, and tribal law enforcement partners rely on those capabilities for

information sharing, operational support, and training to address crime and violence in the 21st century. Our cooperation with our law enforcement partners is especially effective in addressing violent crime and offenses against those who cannot defend themselves, such as crimes against children and human trafficking.

(U//~~FOUO~~) When a crisis does occur anywhere in the world, the FBI must be ready to respond. The FBI maintains a number of national assets, some of which require carrying out unique responsibilities for the USG to respond to even the most complex situations, including countering explosives, hostage rescue, and aviation. *See the Spotlight on the FBI's Critical Incident National Assets for more information.*

(U) The FBI's public website documents some of these capabilities and responsibilities and the indispensable role the FBI plays in keeping the nation safe. Few know or understand how the FBI marries these capabilities with our intelligence function to serve as that vital link between the intelligence and law enforcement communities to better protect national security. These materials tell that story.

00110101

(U) FBI Personnel Aboard an Air Force Plane



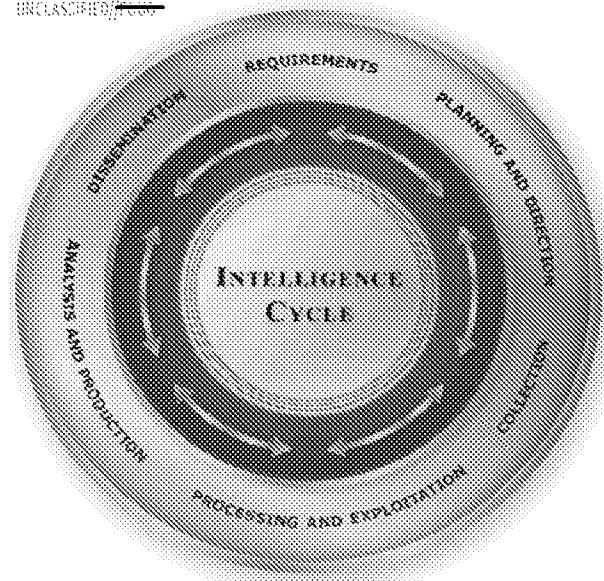


(U//~~FOUO~~) INVESTIGATIONS: INTELLIGENCE AND EVIDENCE



(U//~~FOUO~~) The FBI carries out everything we do, the investigation of reported criminal activity and the collection of intelligence, within the parameters of the Attorney General's and the FBI's domestic intelligence operations guidelines to ensure the protection of privacy and civil liberties of U.S. persons. Under these authorities, the FBI conducts activities using the least intrusive means, requiring an authorized purpose to review records outside of an authorized investigation. More invasive techniques, such as the acquisition of private records or surveillance, require an authorized investigation.

(U//~~FOUO~~) FBI special agents work these investigations with a team of FBI employees: intelligence analysts, language analysts, forensic accountants, computer analysts, and others inside and outside of the FBI to collect intelligence, evidence, or both. Whether the FBI initiates the investigation based on a violation of federal law or as a result of intelligence about a potential threat, the FBI's authorities include — depending on the circumstances — both criminal and intelligence tools to collect information. The FBI does all collection in accordance with Attorney General guidelines and with oversight from several components, including DOJ, the Office of the Inspector General, and Congress.

UNCLASSIFIED//~~FOUO~~

(U//~~FOUO~~) In the years since the 9/11 terrorist attacks, the FBI has undergone a paradigm shift in the way we collect and use intelligence. The FBI has always collected and used intelligence, but we did so primarily in the context of crimes already known to the FBI. Today, the FBI does not just use intelligence to advance our operational mission and solve a particular crime. We also prioritize collecting

UNCLASSIFIED//~~FOUO~~b3
b7E

and sharing intelligence with partners to develop a comprehensive picture of threats and to understand how those threats intersect across actors, criminal violations, and national security concerns. This strategic approach enables the FBI to disrupt threat actors before they act, either by taking action ourselves, informing other agencies with authorities to address the activities, or working with policymakers to use the broader capabilities of the USG to address the identified threat. In turn, intelligence drives how we understand threats, how we prioritize and investigate these threats, and how we target our resources to address these threats.

(U) Like other intelligence agencies, the FBI collects, exploits, disseminates, and analyzes intelligence. The FBI is a producer of both raw and finished intelligence that address the strategic, operational, and tactical intelligence needs of internal and external customers.

(U//~~FOUO~~) While the FBI uses our intelligence to advance our operational mission, we also have increased efforts to produce intelligence for external customers. This intelligence reflects the unique perspective of the FBI — the threat to the domestic territory and its citizens based in part on the Bureau's unique collection capabilities and our domestic law enforcement partnerships — to present a full picture of the threat to our partners and policymakers.

(U//~~FOUO~~) Through an array of FBI analytic products and contributions to community products disseminated through the National Intelligence Council and the President's Daily Brief (PDB), for instance, FBI intelligence reaches a broad spectrum of consumers. These customers range from the President and other policymakers, to intelligence partners, and to state, local, and tribal law enforcement partners. For FY 2019, the FBI shared more than [] analytic products. Regardless of the type of contribution, the FBI adheres to documented guidelines related to the inclusion and sharing of U.S. person or U.S. business information in intelligence products. b7E

(U//~~FOUO~~) UNIQUE CONTRIBUTIONS TO OTHER INTELLIGENCE COMMUNITY AGENCIES

(U//~~FOUO~~) The tools the FBI uses in our investigations take many forms, including recruiting potential human sources; acquiring records through various legal processes; [] b3 b7E
[] about threats overseas; and supporting our federal, state, local, and tribal partners to exercise their distinct authorities to disrupt plots before they cause harm.

(U//~~FOUO~~) These collective capabilities allow the FBI to provide several unique contributions to the intelligence

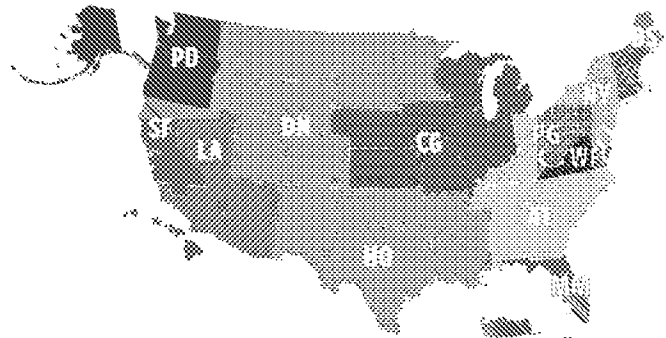
communities both domestically and overseas. Task forces, cross-agency leadership responsibilities, legal authorities, and various technical capabilities are just some of the FBI's unique contributions to the U.S. national security apparatus on a daily basis.

(U//~~FOUO~~) Domestic DNI Representative Program

(U//~~FOUO~~) Because of the FBI's responsibilities, authorities, and capabilities, the DNI designated the FBI as the Domestic DNI Representative in 2012. Across the FBI, the senior FBI executives in 12 field offices serve as Domestic DNI Representatives. In each of these locations, the FBI establishes regional issue- and threat-based working groups and holds quarterly meetings with USIC representatives, and law enforcement partners as applicable. These efforts improve cross-agency communication and integration to focus each region on priority concerns, reduce duplication of effort, and develop opportunities for engagement. This integrated, coordinated, and regionally focused USIC enhances collaboration between intelligence and law enforcement partners, enabling the USG to more effectively identify and mitigate threats.

(U//~~FOUO~~)

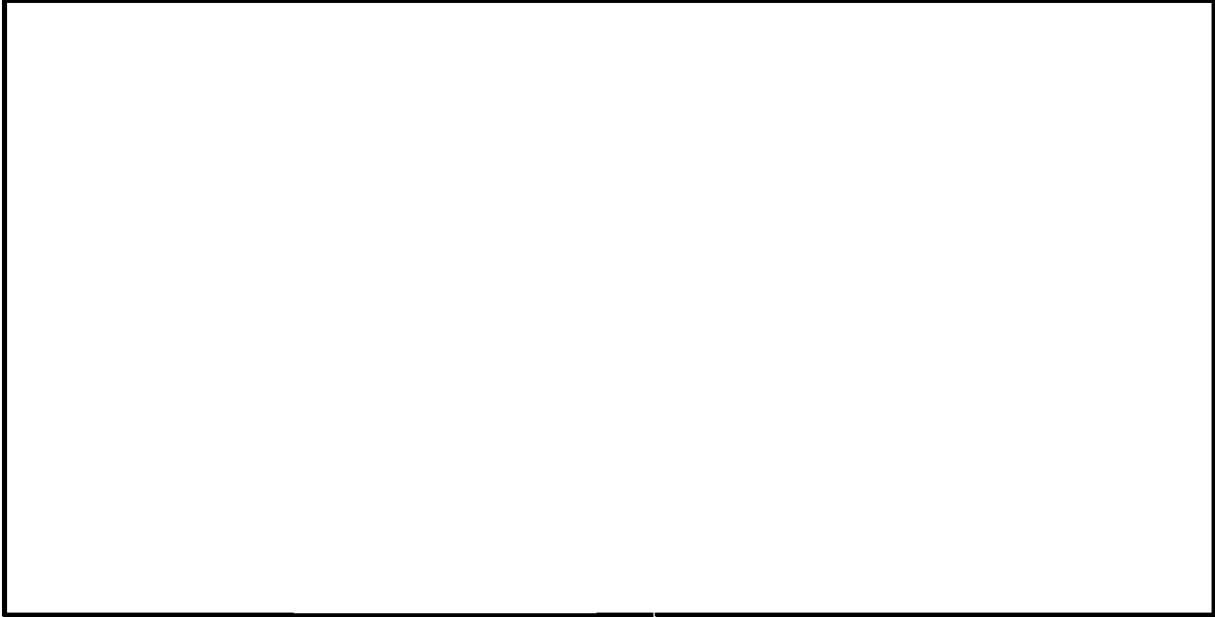
(U) Domestic Director of National Intelligence Representative Regions



(U//~~FOUO~~) Identify Intelligence

(U//~~FOUO~~) The FBI plays a critical role in implementing National Security Presidential Memorandum 7 (NSPM-7) and NSPM-9. These presidential policies direct the USG to identify, integrate, and share threat actor information using technical architectures and integrated systems as well as share immigration and visa data to identify previously unknown threat actors. Through DOJ, the FBI is serving as the executive agent for cyber and TOC, building knowledge-bases on these threat actors. In addition, because of its authorities to bridge both intelligence and law enforcement analytical and operational elements, the FBI, through the Terrorist Screening Center (TSC), is [] b5 b7E

~~PROLIFERATION/ENFORCEMENT SENSITIVE~~



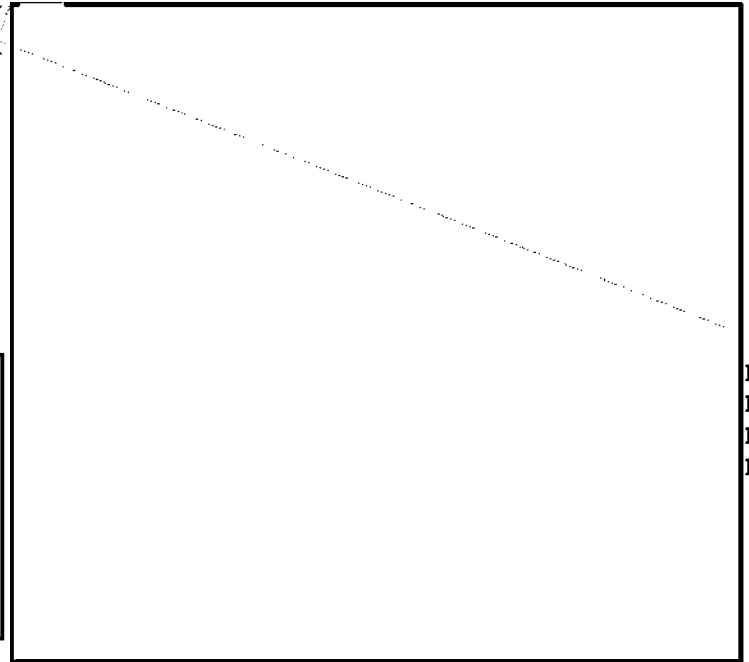
b3
b7E



(U//LES) This effort will address intelligence gaps — bridging unknown and known threat actors — and provide our international and domestic partners with a common operating picture to address converging threats. *See the Spotlight on National Security Threat Actor Global Detection Program for more information.*

(U)

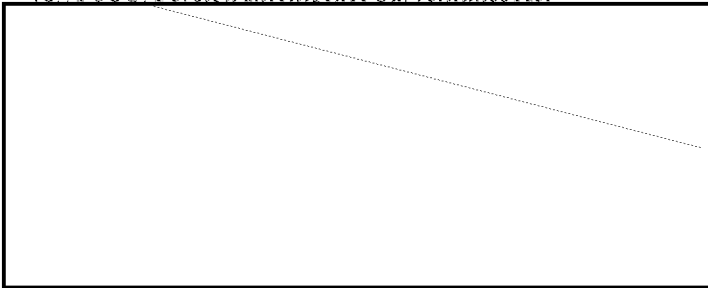
~~(S)~~



b1
b3
b5
b7E

~~(S)~~

(U) ~~(U//FOUO)~~ Foreign Intelligence Surveillance Act



(U)

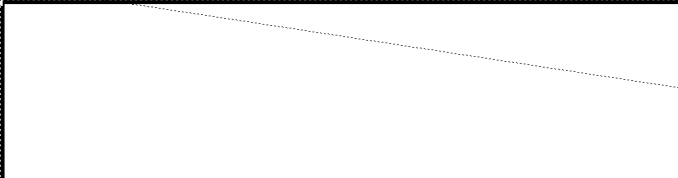
~~(S)~~

(U) FISA Reauthorization

(U//FOUO)

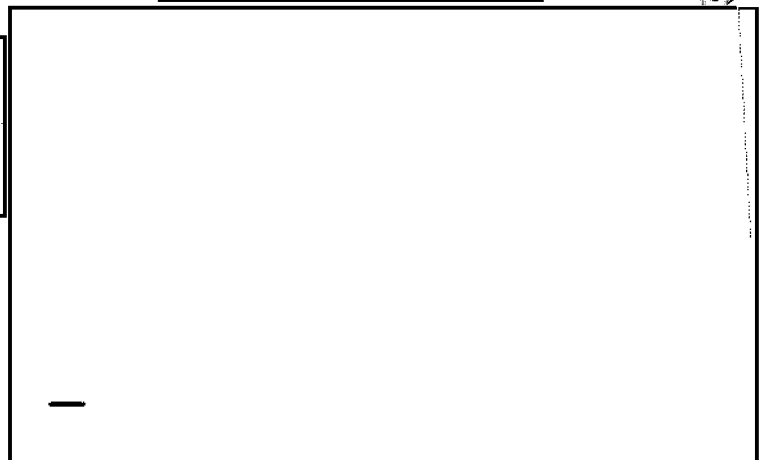


(U) ~~(S)~~



(U) First enacted in 1978, FISA established a legal framework for authorizing the USG to gather foreign intelligence by targeting agents of a foreign power, or a foreign power.

(U) Changes made to FISA in the aftermath of the 9/11 terrorist attacks helped the FBI and our USIC partners tear down walls that previously prohibited or inhibited the sharing of critical intelligence across programs. *See the FISA Reauthorization Challenge Spotlight for more information.*



(U)

THE FBI'S UNIQUE DOMESTIC ROLE

(U) **Warrant-Proof Encryption Challenge**



(U) Law enforcement is increasingly unable to access, intercept, collect, and process wire or electronic and stored communications information through court-authorized warrants, primarily because of the application of end-to-end encryption. This erodes the ability to obtain valuable information to identify and save victims and collect evidence and intelligence to inform national security threats. See the Challenge Spotlight on Law Enforcement Access for more information on this challenge.

(U//~~FOUO~~) **Committee on Foreign Investment in the United States**

(U//~~FOUO~~) The FBI played a leading role in supporting the Committee on Foreign Investment in the United States (CFIUS) even before the 2019 passage of the Foreign Investment Risk Review Modernization Act (FIRRMA), which updates CFIUS processes. FBI foreign investment experts provide analytic support to the DNI, which generates a National Security Threat Assessment for every transaction flagged for CFIUS review. The FBI also provides intelligence and operational support to DOJ, which serves as a voting member of the CFIUS committee. This input leverages the FBI's intelligence, criminal information, and expertise — particularly on the goals and intentions of foreign adversaries — to identify and help resolve any potential threats foreign investment in the United States can produce.

b1
b3
b5
b7E

(U//~~FOUO~~)

(U//~~FOUO~~) Foreign adversaries use a variety of techniques to achieve their intelligence and foreign policy objectives against the United States. FIRRMA expands CFIUS's jurisdiction to include several aspects of foreign investment brought to the attention of Congress by the FBI, particularly in the area of "non-notified" transactions. Even before FIRRMA, CFIUS relied on

b3
b5
b7E

[REDACTED] ~~(U//FOUO)~~

(U//~~FOUO~~) Homeland Intelligence Brief

(U//~~FOUO~~) To help inform policymakers with strategic and operational intelligence affecting the U.S. Homeland, the FBI developed the Homeland Intelligence Brief (HIB) product line. Launched in August 2017 to provide the USIC and relevant law enforcement agencies with a platform specifically for forecasting and explaining homeland-related threats across all threat program areas for senior policymakers, HIB products serve as a complement to the PDB, which focuses predominantly on overseas matters. Like the PDB, the HIB requires USIC coordination and aims for community consensus in explaining the captioned issues.

b1
b3
b5
b7E



(U//~~FOUO~~) INNOVATION: AHEAD OF THE THREAT

(U//~~FOUO~~) The urgency of the FBI's mission keeps us laser-focused on our day-to-day work protecting Americans. At the same time, we also work hard to position the FBI ahead of the threat. The FBI must keep finding new ways to be more efficient, nimble, agile, and resilient. At its heart, agility is more than moving rapidly from case-to-case; it is the capability to be innovative, one of the FBI's four strategic objectives. Innovation is not only about using new technology, but is also about the development of new strategies, processes, and partnerships to keep the FBI ahead of the threat. It is the ability to devise new solutions and new ways to exploit emerging technology, such as 5G and artificial intelligence, just as the FBI established the FBI Laboratory in its early days and made use of biometrics when that technology was emerging.

(U//~~FOUO~~) STRATEGIC APPROACH TO THREATS



(U//~~FOUO~~) The FBI has enhanced our agility to shift resources and priorities to address evolving threats both domestically and abroad. This strategy includes an annual Threat Review and Prioritization (TRP) process, which provides a standard method for FBI Headquarters, field offices, and Legats to identify and prioritize threats in every program. Accompanying the TRP is the Consolidated Strategy Guide, which provides the national strategy and sets expectations for mitigating each prioritized threat. This guide also features direction on each operational program's national initiatives as well as intelligence production recommendations. The FBI encourages DOJ; the U.S. Attorney's Office; and other federal, state, and local partners to participate in the TRP discussion. By assessing and prioritizing threats in this way, we strive to place the greatest focus on the gravest threats we face. This gives us a better assessment of what the dangers are, what's being done about them, and where we should prioritize our resources.

(U//~~FOUO~~) The FBI measures performance and assesses progress against the threats through the Integrated Program Management strategy; a set of performance metrics the FBI establishes at the start of the fiscal year based on input from various program representatives with the approval from the executive overseeing the operational program.

(U//~~FOUO~~) LEVERAGING ADVANCING TECHNOLOGY

(U//~~FOUO~~) For the FBI to remain agile in strategically identifying and addressing threats, we must effectively use technology and tools to help exploit the information

we are collecting. These tools help the FBI identify previously unknown subjects, associates, and potential sources more quickly.

(U) 5G

(U//~~FOUO~~) Emerging technologies such as 5G wireless are a significant evolution for communications and data connectivity and hold opportunities and risks for the FBI. The FBI anticipates vulnerabilities that pose enormous security challenges despite efforts from industry and international standards bodies to consider security when developing the 5G protocol. [REDACTED]

(U//~~FOUO~~) Many manufacturers of the 5G network architecture are non-U.S. companies, and this is challenging the FBI. [REDACTED]

(U//~~FOUO~~) To maintain and evolve the FBI's offensive and defensive capabilities related to 5G, the FBI developed a 5G strategy focusing on engagement with its domestic and international private sector, government, and non-government organizational partners. [REDACTED]

(U//~~FOUO~~) [REDACTED]

b1
b3
b5
b7E

(U)

using the Dark Web for illicit purposes pose a clear and immediate threat to public safety, both within the United States and internationally.

(U//LES) The FBI is enhancing our enterprise-wide strategy and capabilities to address this growing threat, working with our domestic and international partners to identify, disrupt, or arrest people using the Dark Web for illicit purposes. For example, in 2018 the DOJ established the Joint Criminal Opioid and Darknet Enforcement (JCDE) Initiative and designated the FBI as the lead. The FBI works with multiple federal agencies to coordinate the USG's efforts to detect, disrupt, and dismantle criminal enterprises that rely on the Darknet to traffic opioids and other illicit narcotics. [REDACTED]

b1
b3
b5
b7E

(U//FOUO) Unmanned Aerial Systems

(U//FOUO) Because the FBI serves as the lead for terrorism threats within the United States, the FBI is taking action to mitigate potential terrorists' use of new technologies, such as Unmanned Aerial Systems (UAS), as a unilateral threat or as a platform for a chemical, biological, radiological, or explosive attack on the United States and its interests abroad. This role includes identifying, preventing, and disrupting threats to special events that are attractive targets for terrorist attacks. With the passage of the Preventing Emerging Threats Act of 2018, the DOJ and the Department of Homeland Security (DHS) gained the legal authority to conduct counter-UAS operations up to and including electronic engagement of the UAS. Counter-UAS requires multiple levels of federal coordination (Federal Aviation Administration, National Telecommunications and Information Administration, etc.) and Attorney General approval. Close coordination among multiple agencies amplifies UAS detection, investigation, and prosecution.

(U//FOUO) [REDACTED]

b3
b7E

(U) Dark Web

(U//FOUO) Every day around the world, millions of people use hidden service websites on the Dark Web — overlaying networks operating on the public internet, but requiring specific software, configuration, or authorization for users to access. These hidden service websites are anonymous, increasingly encrypted, and offer users illicit marketplaces to buy illegal drugs, stolen and fraudulent identification documents, counterfeit goods, malware, firearms, and toxic chemicals using virtual currencies such as bitcoin. People

[REDACTED]

[REDACTED] The FBI's Counter-UAS program provides UAS detection, notification, and mitigation with improved security posture and situational awareness. The FBI continues to work with DOJ to refine these operations and [REDACTED]

[REDACTED]

b3
b5
b7E

THE FBI'S UNIQUE DOMESTIC ROLE

(U) CURRENT THREAT ENVIRONMENT

(U//~~FOUO~~) Staying ahead of the threat is a constantly evolving challenge. We live in a time of complex and persistent threats to our nation's security, our economy, and our communities. These diverse threats underscore the complexity and breadth of the FBI's mission: to protect the American people and uphold the Constitution of the United States. (U)

UNCLASSIFIED



(U) Fly team agents participate in the foreign transfer of custody of an FBI subject from Syria

b1
b3
b5
b6
b7C
b7E

businesses and individuals by encrypting their data and extorting victims to pay to unlock it. These criminals will also steal their money and quickly convert it into virtual currency that is hard to trace, easy to launder, and widely accepted around the world by both benign and malicious entities

b5
b7E

(U//~~FOUO~~) The FBI investigates many other types of crime;

(U//~~FOUO~~) Cyber and criminal threats continue to evolve, requiring an agile response. Cryptocurrencies changed the way financial institutions and consumers conduct commerce. Illicit actors use cryptocurrency to enable new types of fraud and cybercrime because of the perception of anonymity, avoidance of traditional banking structures, and ease of use. The FBI has seen threat actors use cryptocurrencies in terrorism, counterintelligence, violent and white collar crime, and cybercrime investigations. Cyber criminals use various schemes, such as ransomware and botnets, to target and profit from extorting U.S.

Transnational criminal organizations undermine U.S. public safety, threaten U.S. security and allied interests, and empower governments hostile to the United States. Some transnational criminal organizations engage with violent gangs to transport and distribute drugs, driving historic rates of overdose deaths. Money laundering facilitators and corrupt public officials serve as enablers for state and non-state actors as well as businesses and individual criminals. *See the Public Corruption, Violent Crime, and Threat Spotlights for more information on how these threats are currently affecting our nation.*



(U) PARTNERSHIPS AND ENGAGEMENT



(U//FOUO) The FBI does not carry out our mission alone. Much of the FBI's success can be credited to the longstanding relationships we enjoy with our intelligence, law enforcement, academic, public, and private sector partners in the United States and around the globe. In recognition of this partnership, the FBI [REDACTED]

(U//FOUO) In October 2019, the FBI established a Counterintelligence Task Force (CITF) in every FBI field office. The CITFs combine the vast authorities, capabilities, and expertise of partner intelligence and law enforcement agencies, with a mission to support more impactful counterintelligence investigations and operations. [REDACTED]

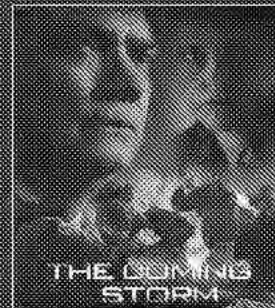
The United States faces coordinated and highly resourced campaigns by foreign powers to damage U.S. security and steal critical technology and classified information. [REDACTED]

[REDACTED] See the *Disrupting Foreign Intelligence Activities Success Spotlight*.

(U//FOUO) With thousands of private and public business alliances and task force officers, including interagency personnel from federal, state, territorial, and tribal partner agencies, the FBI's partnerships are essential to achieving our mission and ensuring a coordinated approach to the mitigation of threats and the protection of civil liberties of the citizens we serve. The FBI also is developing new partnerships on a number of fronts, including academia. The past two years, the FBI has hosted an Academia Summit to invite dialogue with representatives from major research universities across the United States. The FBI continues to develop novel ways to share information and intelligence and influence policies to ensure the FBI stays ahead of the threat. You can read more about many of the task forces on FBI.gov.

(U) Active Shooter Training

(U) One of the key ways the FBI helps mitigate threats is through our training and outreach. We use video to educate law enforcement, industry, academia, and the public about various issues, including active shooters.



(U) "The Coming Storm" is a 40-minute movie dramatizing the aftermath of a campus shooting, weaving within the story the best practices and lessons learned from active shooter incidents that have occurred throughout the United States. The movie also details what FBI resources are available to complement and enhance local law enforcement resources, providing for the longer-term needs of an investigation. The movie helps law enforcement and other first responders evaluate their agencies' preparedness for active shooter and other large-scale incidents. As preparation for a storm helps, preparation for an active shooter incident can save lives.

(U) STATE, LOCAL, AND TRIBAL LAW ENFORCEMENT



(U//FOUO) In addition to working with our state, local, and tribal partners in the task force environment, the FBI also offers support to our law enforcement partners in the form of training, technical expertise, and international investigative support. Through these efforts, the FBI is able to learn the perspectives and concerns of chiefs, sheriffs, and other officials within law enforcement organizations.

(U//FOUO) To confront current major law enforcement issues, the FBI has strong partnerships with national law enforcement associations, including the International Association of Chiefs of Police, the Major Cities Chiefs, Major County Sheriffs, and others to share best practices and identify ways to help each other. We have created programs to assist state, local, and tribal law enforcement agencies, such as the Countering Violent Extremism, Active Shooter, and Police Executive Fellowship programs.

(U//FOUO) The FBI also offers the National Academy, which has a reputation of being the gold standard for leadership training of law enforcement officers. Offered at the FBI Academy in Quantico, Virginia, the National Academy is a professional 10-week residential course of

study for leaders and managers of state and local police, sheriffs' departments, military police organizations, and federal law enforcement agencies from the United States and partner nations. In four sessions a year, more than 265 students are invited to attend each session, including 35 international law enforcement leaders. To date, law enforcement partners from 128 different countries have completed the program.

(U//FOUO) The FBI also provides numerous databases and data check services to support the day-to-day missions of our law enforcement partners, such as eGuardian, the National Crime Information Center, and Uniform Crime Report. The FBI developed this report to generate reliable statistics to support law enforcement administration, operation, and management. The demand for criminal justice information is constantly on the rise. We continue to work toward new approaches to ensure we meet this demand without sacrificing quality. *See the Challenge Spotlight on Increased Demand for Data and Statistics.*

(U) Regional Computer Forensics Labs



(U) To further enhance the FBI's support of state and local law enforcement and the growing volume of digital evidence, the FBI established the Regional Computer Forensics Laboratory (RCFL) program. The RCFLs are digital forensics laboratories jointly staffed by personnel from federal, state, and local law enforcement agencies that

enter into a Memorandum of Understanding (MOU) with the FBI. This program increases the capability of local law enforcement agencies to investigate crimes, help detect and prevent acts of terrorism, and respond to rapidly growing demand for digital forensic examination services.

(U) RCFL services include seizure and examination of computer evidence, training, consultation, and regional support to law enforcement agencies in regions. The program has supported thousands of cases during the past 15 years, including many national high-profile investigations, including the 2016 Pulse nightclub shooting in Orlando, Florida; the 2017 shooting in Las Vegas; and 2019 shooting in Pensacola, Florida.

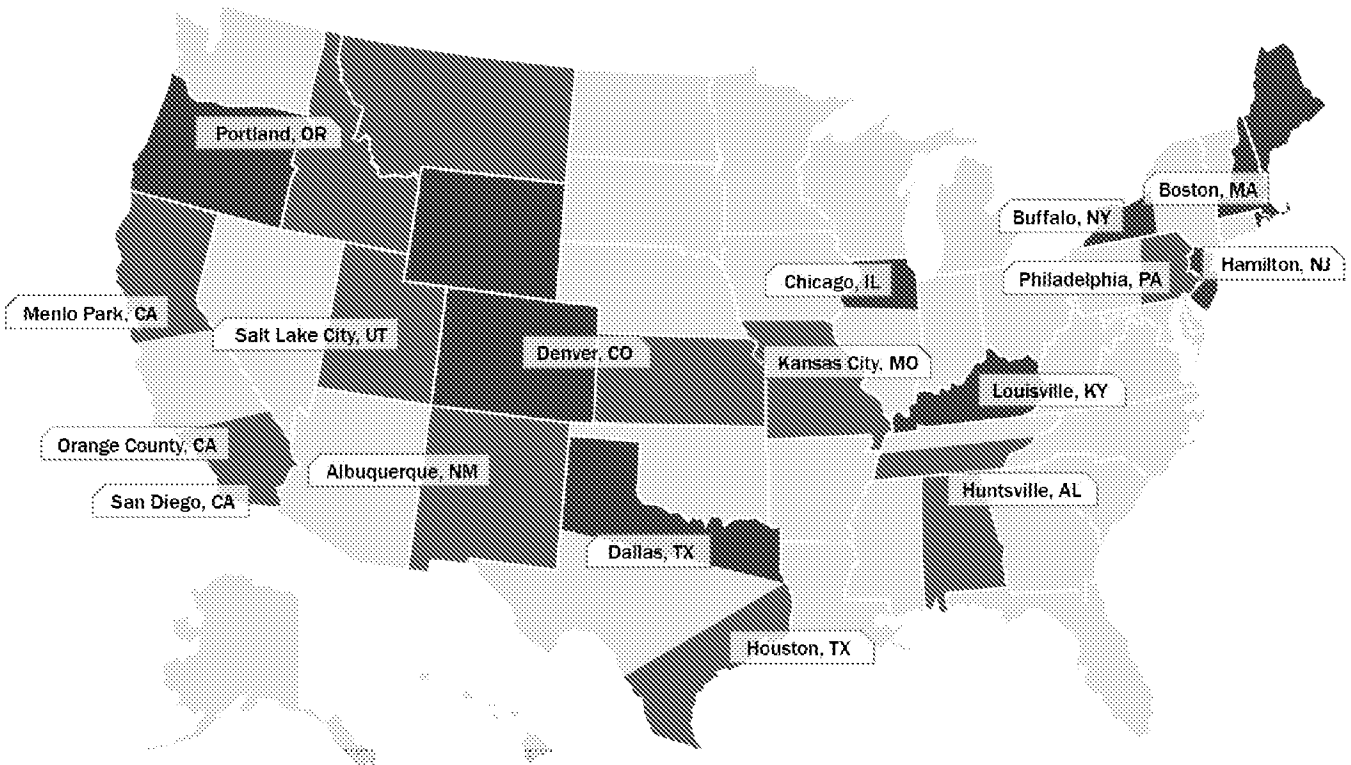


(S)
(U)

b1
b3
b5
b7E

SECRET//NOFORN//LAW ENFORCEMENT SENSITIVE

(U) Regional Computer Forensics Lab Locations



(U)

(U//~~FOUO~~) In coordination with the NCIJTF, DOJ and FBI use intelligence and law enforcement tools as part of the USG's war chest of strategic and deterrent response options for countering cyber adversaries. This includes

(U) UNITED STATES INTELLIGENCE COMMUNITY

(U//~~FOUO~~) Reflective of its role as both a law enforcement and intelligence agency, the FBI engages in a number of mechanisms to enhance our relationship and integration with other USIC and policy components.

b1
b3
b5
b7E

(U//~~FOUO~~) USG agencies have three lines of effort in a cyber-incident response: threat response, asset response, and intelligence support. Presidential Policy Directive (PPD-41) U.S. Cyber Incident Coordination designated DOJ, acting through FBI and NCIJTF, as the lead agency for cyber threat response activities including investigation, attribution, and threat pursuit. No single agency possesses all of the authorities, capabilities, and expertise to address a significant cyber incident. For that reason, PPD-41 at the same time assigned DHS as lead for asset response activities, which involves remediation and recovery. PPD-41 also assigns ODNI as lead for intelligence support — the DOJ, DHS, and ODNI responsibilities are parallel and complementary.

(U) FBI-led USIC Interagency Components

(U) NATIONAL CYBER INVESTIGATIVE JOINT TASK FORCE



(U//~~FOUO~~) Through unique capabilities and blended authorities, the National Cyber Investigative Joint Task Force (NCIJTF) directs and supports whole-of-government campaigns to protect the United States from adversaries, criminal groups, and malicious actors in cyberspace and assists U.S. allies to do the same. Led by senior executives from partner agencies, NCIJTF mission centers lead integrated whole-of-government campaigns in accordance with the National Cyber Strategy, sequence whole-of-government campaigns to maximize impact against adversaries, operationalize intelligence to provide investigative analysis and tactical targeting to counter malicious cyber activities, and represent the interagency when briefing campaigns to the National Security Council.

(U) TERRORIST SCREENING CENTER



(U//~~FOUO~~) A Presidential Directive and Memorandum established the TSC under the FBI's administration in 2003. Establishing the TSC within the FBI as the lead administering agency protects intelligence and law enforcement operations in two ways: facilitating immediate operational response to investigative leads for watchlisted subjects and ensuring the protection of privacy and civil liberties.

(U//~~LES~~) In the past 17 years, the TSC has provided

b1
b3
b5
b7E

~~(S)~~
(U)

b1
b3
b5
b7E

(U//~~LES~~) As the threat environment has shifted, TSC evolved into a key component of the country's overall threat prevention and interdiction framework for other threat actors, including TOC and foreign intelligence threat actors.

(U//~~FOUO~~) Because the TSC is within the DOJ, the nation's chief law enforcement agency, the TSC has vast experience working with the Watchlisting Enterprise to ensure the protection of privacy and civil liberties. It also protects sensitive national information from disclosure during litigation. DOJ has more experience and authorities for sharing and protecting intelligence and law enforcement information from disclosure in legal or administrative proceedings than any other federal department or agency.

b3
b5
b7E

(U//~~FOUO~~) The TSC carries out its mission through five key functions: watchlisting, screening, encounter management, information sharing to domestic and international partners, and protection of privacy and civil liberties.

(U) U.S. COUNCIL ON TRANSNATIONAL ORGANIZED CRIME

(U//~~FOUO~~) In 2017, Executive Order (EO) 12773 identified TOC as a national security priority. The FBI currently serves as the executive director for the TOC Strategic Division, established in February 2018 and co-located with the TSC. The purpose of the TOC Strategic Division is to provide a national mission management structure to drive intelligence collection and production across disciplines. This mission includes coordinating courses of action to address the threat, optimize resources, oversee their implementation, and assess results.

b3
b5
b7E

(U//~~FOUO~~) The TSC's encounter management function is an essential role.

The TSC facilitates immediate operational response to investigative leads for watchlisted subjects, furthering the FBI's responsibilities as the lead for intelligence and law enforcement investigations.

(U//~~FOUO~~) Representatives from law enforcement and intelligence components staff the TOC Strategic Division, leveraging financial, regulatory, and traditional intelligence or law enforcement reporting to develop a comprehensive threat picture.

~~(U//FOUO)~~ HIGH-VALUE DETAINEE INTERROGATION GROUP



~~(U//FOUO)~~ The FBI serves as the executive agent for the High-Value Detainee Interrogation Group (HIG), established in 2009 as the USG's focal point for interrogation best practices, training, and research. An FBI representative leads the HIG with two deputy directors — one from DoD and the other from CIA. The National Security Council chose to embed the HIG in the FBI given the Bureau's experience conducting lawful, rapport-based, and noncoercive interrogations and our ability to uphold the rule of law. Because of our intelligence and law enforcement authorities, the FBI is also able to ensure the collection of intelligence while taking steps to preserve evidence the USG can use in a court of law.

Families also described the USG's efforts to support them as inconsistent in content and frequency and reported feeling they were not trusted by government officials.

~~(U//FOUO)~~ Through the HRFC, the FBI tracks all hostage-takings of U.S. nationals abroad and regularly reports on the status of each case and the measures for each hostage's recovery to the National Security Council. The FBI also oversees the collection and sharing of intelligence related to hostages while preserving evidence for eventual prosecution of hostage-takers. Through the FBI Victim Services Program, the HRFC also supports the families whose loved ones are being held captive while coordinating engagement and support for families, intelligence sharing within the USIC, declassification of information that can be briefed to family members, and hostage recovery strategies and associated action plans.

~~(U)~~ INTERNATIONAL AND GLOBAL



~~(U//FOUO)~~ A significant international nexus develops in many major FBI investigations. The exponential growth of global security issues and transnational crime makes international partnerships critical to addressing our nation's threats. To maintain and build on those partnerships, the FBI maintains Legat offices in more than 70 nations around the globe to support our law enforcement and intelligence operations.

~~(U//FOUO)~~ HOSTAGE RECOVERY FUSION CELL



~~(U//FOUO)~~ The FBI coordinates the USG's hostage recovery efforts abroad through the Hostage Recovery Fusion Cell (HRFC), a multiagency team embedded in the FBI and representing the government's unified approach to recovering American hostages. The HRFC was organized following an internal USIC review in 2015 assessed current policy for hostage cases abroad and recommended actions to improve interagency coordination and case management. The White House chose the FBI to lead this team because of our authority to investigate kidnapping and hostage taking domestically and internationally. The FBI also possesses a depth of experience and expertise in conducting investigations, gathering intelligence, overseeing negotiations, working with partners, preserving evidence for eventual prosecution, and supporting and building relationships of trust with families of victims.

~~(U//FOUO)~~ At the time, the review found the families of U.S. hostages were dissatisfied with USG efforts to share information in terms of the amount of information provided, the lack of proactive communication from U.S. officials, and the quality of the information provided.

~~(U//FOUO)~~ Trojan Shield Investigation

~~(U//FOUO)~~ The Trojan Shield investigation highlights how law enforcement partnerships worldwide can successfully aid the FBI's interests. Trojan Shield is a joint FBI-DEA investigation targeting a communications provider (SKYCC) that services criminal groups and penetrates established criminal enterprises through the distribution of FBI-created next-generation encrypted devices. The FBI works collaboratively with international partners including the Australian Federal Police as well as Lithuanian law enforcement. As of May 2020, the FBI had identified 30 distinct enterprises worldwide and collected more than one million messages from 818 devices located in 32 countries. The investigation led to numerous interdiction operations, including seizures of 457 kilograms of cocaine in Belgium and 2.75 million Australian dollars.

~~(U//FOUO)~~ Foreign police cooperation is at the core of the FBI's mission. The FBI frequently receives requests for investigative assistance from foreign police and intelligence agencies. Investigative assistance to foreign agencies must be conducted in accordance with all applicable treaties and MOUs between the USG, the FBI, and the foreign nation or agency. The FBI will also arrange for investigations in the foreign countries covered by Legats on behalf of U.S. agencies and state or local police. The FBI and foreign police have fostered a symbiotic relationship that helps the USG and cooperating foreign countries combat crime across the globe.

b1
b3
b5
b7E

UNCLASSIFIED

(U) FBI International Law Enforcement Academy Training in Budapest



(U//~~FOUO~~) The FBI offers training at the FBI Academy for some of our most crucial international law enforcement partners, and developed an enterprise-wide framework to drive our global engagement for the next five years. The FBI's Global Partnership Strategy supports the National Security Council's strategy and provides a data-driven, repeatable process to inform and evaluate key international partnerships and the engagement tools to strengthen them.

(U) PRIVATE INDUSTRY AND ACADEMIA

(U//~~FOUO~~) With the private sector owning, controlling, or operating approximately 85 percent of all critical infrastructure in the United States, engagement with this sector is key. One of the FBI's top priorities is to

better engage private industry and academia as a force multiplier in the FBI's mission. Two of the more well-known private sector programs are InfraGard and the Domestic Security Alliance Council. InfraGard, an alliance with the private sector to promote protection of critical information systems, consists of approximately 70,000 members representing 16 critical infrastructures such as banks, hospitals, telecommunications systems, emergency services, water and food supplies, the internet, transportation networks, postal services, and other major industries that have a profound impact on American lives.

(U//~~FOUO~~) The FBI has been focusing resources on a proactive approach to engagement with critical infrastructure entities before an incident. The FBI also engages with more than 600 members in an alliance council representing almost every critical infrastructure. FBI field offices communicate regularly with representatives of organizations associated with critical infrastructure.

(U//~~FOUO~~) Although engagement and timely sharing of actionable information with the private sector is critical to our ability to stay ahead of threats, it also poses risks. Private sector companies may be hesitant to provide sensitive company information, concerned it could become public under the Freedom of Information Act or be provided to regulatory agencies resulting into inquiries into their practices.

(U//~~FOUO~~) The FBI continues to work to identify opportunities to share timely, actionable, strategic and operational information that could help private sector partners make better decisions about risk and threat mitigation while respecting the sensitivities to safeguard information. We have seen the benefits of this information exchange. When the FBI shares timely, actionable information the private sector reciprocates by providing valuable information in return to the Bureau to help us better mitigate and investigate threats.

~~(U//~~FOUO~~)~~ Our initiatives involving private industry and academia are undertaken to drive more effective engagement between the FBI and the private sector — particularly key partners — to get ahead of threats and thwart bad actors.

(U) A prime example of the benefits of successful information sharing took place when the FBI briefed Texas A&M University about the threats stemming from collaboration with institutions such as Harbin University, an institution with extensive ties to the Naval Branch of China's People's Liberation Army, and that had signed an MOU with Texas A&M's College of Engineering.

b1
b3
b5
b7E

UNCLASSIFIED

U.S. Department of Justice
Federal Bureau of Investigation



DSAC

DOMESTIC SECURITY
ALLIANCE COUNCIL



The Domestic Security Alliance Council (DSAC) is a strategic partnership between the U.S. Government (USG) and U.S. private industry that enhances communication and the timely exchange of security and intelligence information. DSAC's 600+ Member Companies, the FBI, and the Department of Homeland Security (DHS) work together to advance the USG's mission of protecting national and economic security, while assisting the U.S. private sector in protecting its employees, assets, and proprietary information.

Mission

To advance the FBI's strategic mission by building and preserving enduring relationships within DSAC among private sector member companies, the FBI, DHS, fusion centers and other government agencies.

Leadership

DSAC is led by a 10-member Executive Working Group (EWG) that serves as the primary governing body of the DSAC. The EWG consists of FBI, DHS and Private Sector executives. The EWG oversees the Membership and Engagement Committee, Education and Training Committee, Information Sharing and Communications Committee, Industry Threat Committee, and the Senior Advisory Group.

Membership Eligibility

Eligible Company Members represent for-profit enterprises with proven revenue in excess of \$1B. Membership is limited to U.S.-based private sector companies with a national or international scope of business and a clear nexus to U.S. national and economic security.

Benefits:

- ✓ Direct engagement with FBI and DHS leaders and professionals
- ✓ Ongoing access to a network of diverse security professionals at the highest levels of government and the private sector
- ✓ Tailored intelligence and security information from the FBI and DHS
- ✓ Access to a members-only portal where private sector members and government officials collaborate, resolve problems, exchange best practices, and share information
- ✓ Access to local, regional, and national executive events, continuing education, and conferences related to national and economic security

How to Join:

To learn more about DSAC membership, please visit www.DSAC.gov

To contact the DSAC program office, please email DSAC@fbi.gov.

FBI

UNCLASSIFIED

(U) In response to the information Texas A&M received from the FBI, the university terminated its relationship with Harbin University and returned millions of dollars funding joint research projects between the two universities. Several months later, seven individuals and two businesses were charged with conspiracy to steal trade secrets from a U.S.-based company. The lead subject of the investigation, Shan Shi, was a Harbin University professor sent to teach at Texas A&M. Shi was actually working on behalf of the Chinese government and Chinese state-owned enterprises to steal proprietary information on the manufacture of syntactic foam, a strong, lightweight material that has both military and commercial uses.

(U) This episode led to the establishment of the Academic Security & Counter Exploitation (ASCE) program in 2018. Now in its second year, ASCE is building relationships between the FBI, DoD, and the university community. ASCE's main goal is working together to protect campuses from abuse by foreign governments while preserving academic freedom.

(U//~~FOUO~~) To build on successes such as the one with Texas A&M, the FBI continues to enhance its ability to share timely information with the private sector through working groups and other vehicles. The FBI has a private sector engagement strategy to drive us toward effective engagement. This strategy includes expanding working groups, and developing intelligence products for private sector audiences.

(U) INTERNET GOVERNANCE

(U//~~FOUO~~) As technology shapes the future of connectivity and communications globally, consistent participation in the international internet governing bodies working to establish consensus-based standards will improve our understanding of our adversaries' long-term strategies. The FBI is enhancing our engagement and outreach to influence relevant technical standards and keep us agile against emerging threats. We are also leading outreach to international and domestic law enforcement counterparts to rally support for U.S. policy positions.

(U//~~FOUO~~) In the early evolution of the internet, the USG helped drive innovation, development, and deployments of fledgling networks. Over time, a "trusted" market evolved between U.S. manufacturers, service providers, and consumers, and the USG's role receded. Now, the global telecommunications landscape includes a vast array of foreign companies and foreign markets. Because of this, USG investment minimally affects the landscape. Additionally, the internet has no central governing body. Instead, a globally distributed network sets standards, and government and law enforcement have no special status.

The most active and engaged actor has the most influence, thus requiring persistent and proactive engagement with forums, the private sector, and academia.

(U//~~FOUO~~) The FBI is aware of this priority and is actively establishing collaborative technological partnerships with national and international government agencies and private sector entities to gain awareness and early warning of information and communications technology developments. This engagement will help identify potential risks or opportunities for the FBI and USG. Without these partnerships, the equities and operational capabilities of the USG and FBI will be increasingly eroded as device promulgation, global connectedness, and reliance on internet transactions continue to grow. Internet policy and regulatory development processes cannot keep up with internet-based development and deployment efforts, and U.S. adversaries are well organized and well represented in internet governance. Therefore, membership and participation in these standards organizations will yield opportunities to advocate for FBI and USG positions on areas such as lawful access and encryption challenges, 5G, and technical collection through speaking engagements on panels and working groups.

(U) THE PEOPLE WE SERVE



(U//~~FOUO~~) In this time of ever-changing threats, more than ever before, the FBI needs the support and confidence of the American people to be successful. In addition to information found on the FBI.gov website, the FBI also supports an array of public requests for information and statistics, including responding to Freedom of Information Act requests and maintaining the National Sex Offender public website. The more we work with the American public to share information and ensure the public's trust, the more effective the FBI will be in carrying out our mission. This partnership includes actively sharing information about our responsibilities, operations, and accomplishments as well as responding as transparently as possible when various compliance and oversight components detect deficiencies within the FBI and fix them before problems occur. Through this trusted partnership, the FBI works to empower citizens to protect themselves from ongoing threats and crimes.

(U//~~FOUO~~) Prevention also means working closely with community groups and their leaders. The FBI directly reaches out to specific communities to hear their concerns, build cultural understanding, and foster trust. Every field office has strong community outreach and works with minority groups, religious and civic organizations, schools, nonprofits, and other entities in crime prevention programs such as our Citizens Academies, Youth/Teen

Academies, Adopt-A-School, and Junior Special Agents. Our outreach also includes local and national internet safety campaigns and educational video screenings. Another effective relationship-building structure we created is the Multi-Cultural Engagement Council, composed of ethnic, religious, and minority leaders who help us better understand cultures, issues, and possible solutions within communities.

(U//FOUO) All of these outreach efforts are ways we help individuals and families stay safe from fraudsters and cyber predators, help businesses protect against hackers and economic espionage, help schools and workplaces safeguard against violent rampages and illegal drugs, and help all citizens be alert to potential acts of terror and extremism.

UNCLASSIFIED

(U) FBI Child ID App

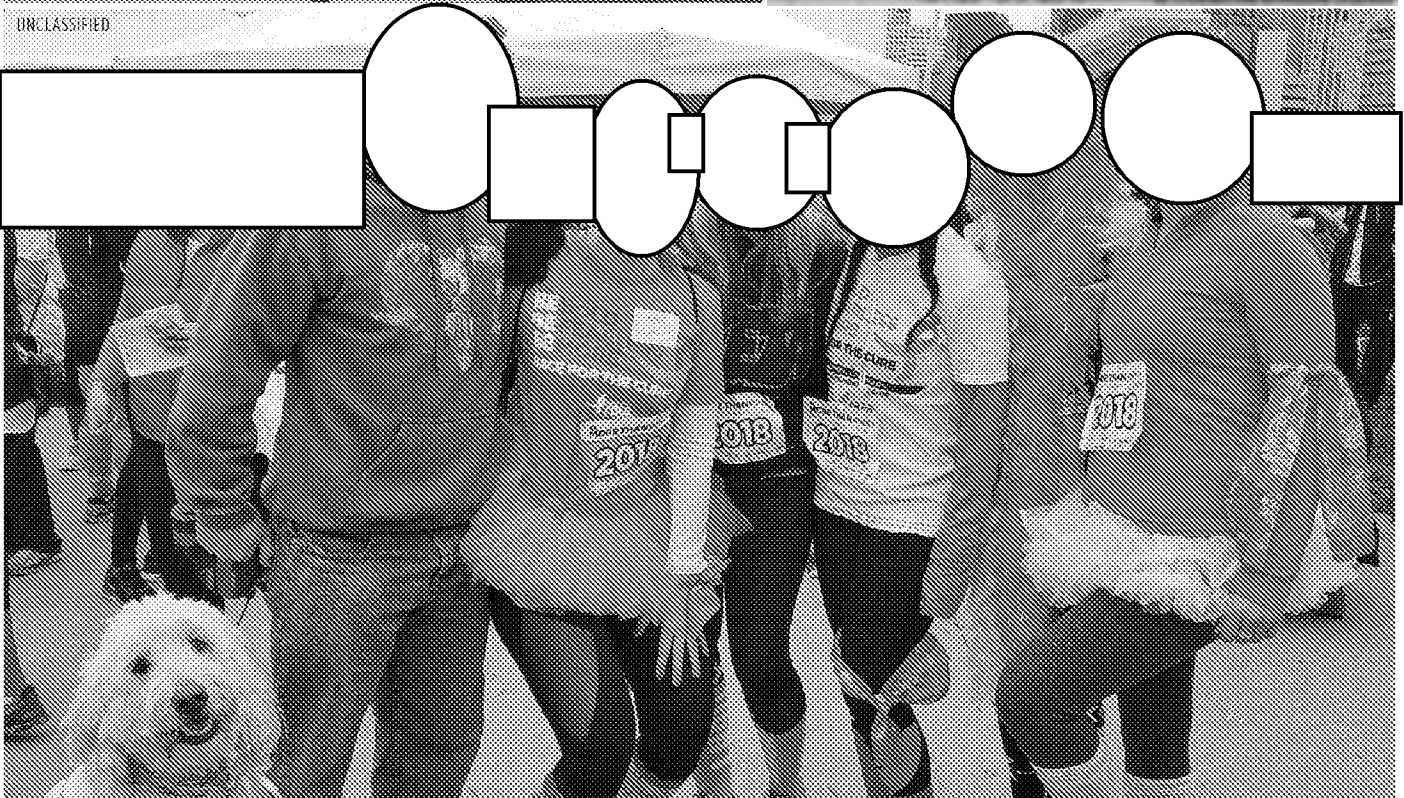


(U) The FBI created a mobile application for parents to store photos and other vital information about their children. Parents can use this to send information to authorities in case their child goes missing.

UNCLASSIFIED



(U) The FBI distributing aid throughout the island of Puerto Rico after Hurricane Maria in 2017.





(U) THE PEOPLE OF THE FBI



(U) The strength of any organization is its people. The threats we face as a nation have never been greater or more diverse, and the expectations placed on the Bureau have never been higher. Meeting these threats requires a cadre of special agents, intelligence analysts, and other professionals who understand the importance of our work and possess the skills and character to carry it out. While the best known part of the FBI workforce is our special agent cadre, special agents do not make up the largest segment of the FBI workforce. Professional staff employees, who may be serving in any one of more than 500 different job roles, make up more than half of the FBI workforce.

(U) Since 9/11, the FBI has worked to recruit, hire, and develop a specialized and integrated national security workforce, including computer and data scientists, accountants, biotechnology specialists, public affairs specialists, and psychologists. The FBI hires a highly qualified, diverse workforce that meets the Bureau's high standards for commitment, personal character, and ethics. Each year, the FBI develops a comprehensive recruiting strategy that promotes available positions both directly to key audiences for hard-to-fill positions and through social media platforms for general job applicants. These specialty, hard-to-fill positions include computer scientists, forensic accountants, cyber security personnel, and linguists. The FBI sets aggressive hiring goals for each work role and for each field office and tracks the yearlong progress. The success is evident: the FBI is regularly staffed above 95 percent and has an attrition rate below 3 percent.

(U//FOUO) USING ANALYTICS TO IMPROVE RECRUITING AND HIRING

(U//FOUO) Recruiting a 21st century workforce is a challenge the law enforcement and intelligence communities are facing. The FBI is competing with other law enforcement, USIC, and private sector companies for similarly skilled employees. The FBI has spent three years enhancing our data tools and our use of data analytics to assess and act on our recruiting needs. Scrubbing the FBI's databases, improving the platform for managing the data, and bringing in the talent team to manage the analytic process took enormous effort. The human resource analytics and tools have also enhanced the business intelligence around our hiring process, which can take six to nine months for each candidate. With these data, we have identified opportunities to re-engineer our hiring process, tracked candidates' progress through

(U) Victim Services Program

The FBI's Victim Services Program plays a critical role in providing support and resources to the victims of crime and their families. The program assists victims in understanding the physical and emotional aftermath of a crime and the criminal justice system, thus assisting in their recovery. The program is critical for the health and well-being of victims and the success of investigations. See the Success Spotlight on the Victim Services Program for more information.



the hiring lifecycle, and more accurately predicted the number of candidates needed to be put in background to result in our desired number of hired employees. Our recruitment efforts are paying off. In FY 2016, our special agent application volume had fallen to about 12,500, lower than the previous 11-year average of 28,000. Despite a new human resources application system and modifications to the special agent hiring process, applicant volume decreased slightly in FY 2017 and FY 2018. However, the volume reached an eight-year high in FY 2019 at 35,000, two years after we launched an aggressive social media campaign; the volume continued the upward trend through FY 2020.

(U) DIVERSITY



(U//FOUO) Despite our recruitment efforts, diversity across the FBI workforce, especially among the special agent cadre, continues to be a challenge. To remain the world's premier intelligence and law enforcement organization, diversity and cultural awareness are critical to ensure the FBI continues to develop new, innovative ways of thinking, has the benefit of different perspectives to make us more effective, and maintains credibility by reflecting the diversity of the citizens we serve. For example, all basic training for new special agents and intelligence analysts at Quantico includes trips to the Holocaust Museum, Martin

Luther King, Jr. Memorial in Washington DC, and the 9/11 Memorial Museum in New York City. These trips are combined with leadership and historical lessons that give the trainees important insights about the importance of cultural diversity.

(U//~~FOUO~~) In addition to educating our workforce about the importance of diversity, the FBI is working hard to attract more diverse candidates to the organization. The FBI established our first national recruiting strategy with goals focused on attracting female and minority candidates, which was accompanied by an aggressive and ongoing social media campaign to engage with these key audiences. The Diversity Agent Recruitment program introduces highly qualified female and minority candidates to the special agent role with events held in cities across the country. The FBI also reviewed our selection and testing process for special agent and intelligence analyst candidates to ensure no bias to minority candidates.

(U//~~FOUO~~) Because diversity is so important to the FBI's success, it is one of the FBI's eight core values and among our priority initiatives to strengthen how we accomplish our mission. *See the Challenge Spotlight on Recruitment of Specialty Skills and Diverse Candidates for more information.*

(U) WORKFORCE DEVELOPMENT

(U//~~FOUO~~) To ensure those hired and those who have been employed at the FBI for a long time are part of the integrated approach to preventing threats, the FBI has a robust internal and cooperative workforce development program.

(U//~~FOUO~~) For agents and analysts, this training begins on their first day of Basic Field Training Course (BFTC), which the FBI developed to be a joint training program for special agents and intelligence analysts and emphasizes an intelligence-driven, threat-based, and operationally focused FBI. The FBI established this course in 2015, replacing our stovepiped, separate training with a collaborative, interactive environment that blends intelligence and law enforcement learning. Agents and analysts train side-by-side to infuse the necessity of working as a single, integrated, cohesive team, reflecting a team-oriented environment modeled after day-to-day FBI field office operations.

(U//~~FOUO~~) The BFTC uses practical and realistic exercises and requires trainees to learn and skillfully apply investigative techniques while appropriately balancing security concerns and civil liberties. This course also educates trainees on how to engage FBI team members, intelligence community partners, and law enforcement

partners in a collaborative environment to achieve results and resolve a series of challenging intelligence and law enforcement scenarios. The development of this collaborative learning environment and curriculum is tied to the recommendations of the 9/11 Review Commission.

(U) Cyber Training

(U//~~FOUO~~) Advances in technology and application of such knowledge by nation-state and criminal cyber actors require up-to-date instruction for conducting complex cyber investigations. In response, the FBI has established a robust training to teach cyber tradecraft and methodology.



regularly attend senior trader courses for all FBI executives after enhanced familiarity with cyber topics.



(U//~~FOUO~~) In addition to BFTC, the FBI offers a variety of continual learning programs through the Leadership Development Program, the Intelligence Community Advanced Analytic Program, as well as specialty training programs such as cyber and HUMINT. Advances in technology have created needs for more cutting-edge cyber knowledge to learn how to conduct cyber investigations. It has also created challenges for HUMINT collection. The FBI has been coordinating, developing, designing, and delivering intermediate and advanced HUMINT operations training to FBI personnel, task force officers, and other intelligence and law enforcement agencies in support of FBI national and strategic priorities. This training helps ensure we identify, vet, validate, and manage the FBI's sources to ensure the information they are providing is authentic, reliable, and not subject to external control.

b7E

(U) CLOSING SUMMARY

(U) The diverse and shifting threats facing the nation underscore the complexity and breadth of the FBI's mission. As adversaries continue to evolve their capabilities, so too must the FBI and our partners.

(U) Today, the FBI efficiently and effectively uses intelligence to drive our operations while maintaining the law enforcement mission that built our reputation more than a century ago. The FBI's evolution since 9/11 has ensured the organization can successfully fulfill both missions. We will continue to execute this mission with objectivity and independence, following the facts wherever they may lead, to whomever they may lead.

(U) As the lead domestic intelligence and law enforcement organization, the FBI unifies the efforts of the intelligence

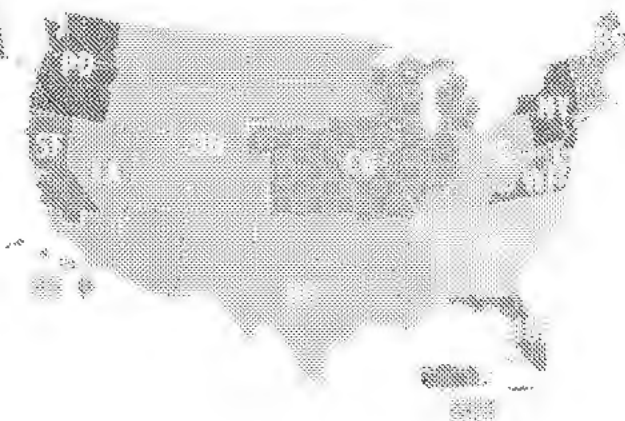
and law enforcement communities to establish a whole-of-government approach domestically to address threats and inform policymakers on a variety of issues. With these unique authorities and capabilities, the FBI applies the rigor of the rule of law to our intelligence operations to investigate threats while protecting privacy and civil liberties.

(U) By constantly enhancing our capabilities, collaborating with our partners across the community, and working toward the complete integration of intelligence and operations, the FBI will continue to identify and mitigate threats with the goal of protecting the American people and upholding the Constitution.

(U) AT-A-GLANCE

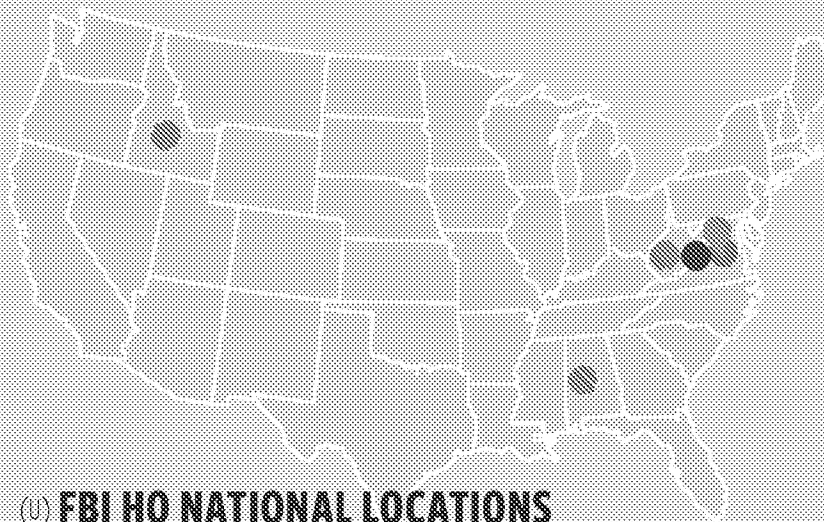
Domestic DNI
Representative
Program

Domestic DNI Rep-Offices: The DNI has fully completed the national intelligence fusion centers within 12 DNI regions across the United States to improve intelligence against threats. The chart below shows the location of





The FBI: *At-a-Glance*



(U) FBI HQ NATIONAL LOCATIONS

●(U) NATIONAL CAPITAL REGION

The executives, special agents, and professional staff who work at our national headquarters in Washington DC direct, organize, and coordinate FBI activities around the world.

●(U) QUANTICO, VA

The FBI Academy, dedicated to being the world's premier law enforcement learning and research center and an advocate for law enforcement's best practices worldwide. New Agent Trainees and New Intelligence Analysts Trainees begin their training at the FBI Academy in the BFTC, which features an expansive integrated curriculum.

●(U) WINCHESTER, VA

The FBI maintains its records here, and also provides key services to local law enforcement and the American people, including responding to a large number of Freedom of Information Act and Privacy Act requests every year from the news media, citizens, and others around the world.

●(U) CLARKSBURG, WV

The home of FBI's Criminal Justice Information Services equips our partners with the information they need to protect the United States while protecting civil liberties.

●(U) HUNTSVILLE, AL

The FBI's Hazardous Devices School and the majority of employees assigned to the Laboratory's TEDAC are located in Huntsville. The goal is to move more employees from the National Capital Region to Huntsville.

●(U) POCATELLO, ID

The new data center consolidates almost 100 DOJ data centers, allowing DOJ to reduce operational costs, create efficiencies, and modernize the technological architecture.

AT-A-GLANCE

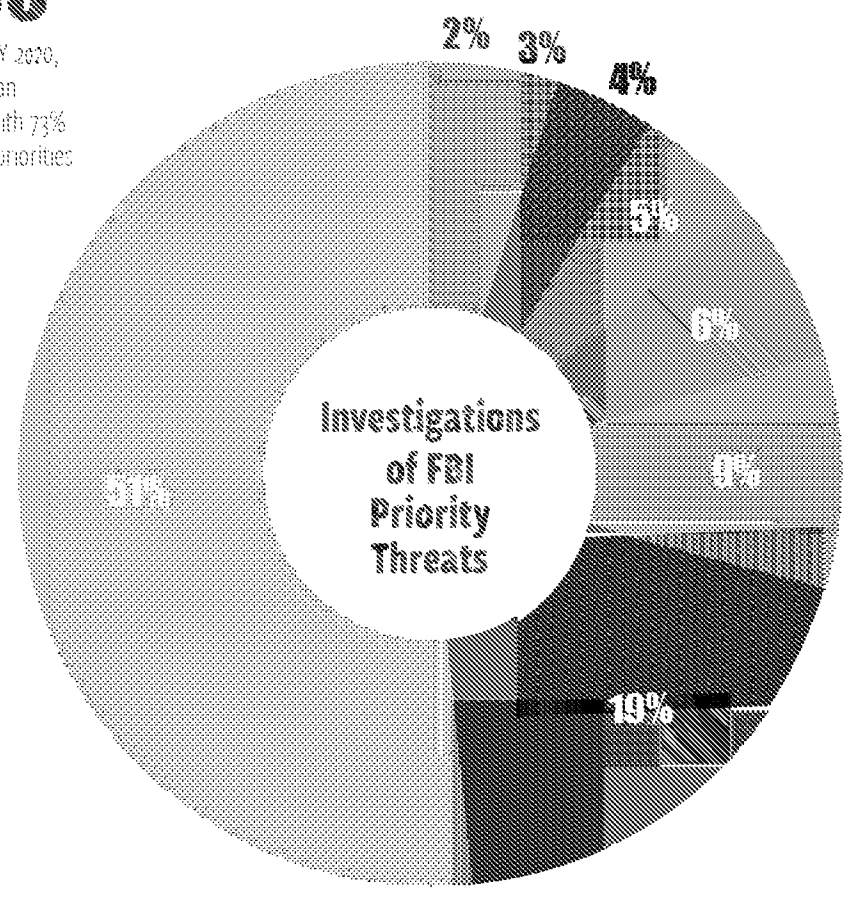
The FBI: At-a-Glance

(U) FBI INVESTIGATIONS

(U) Total Number of Priority Threat Investigations

>184,000

From FY 2016 through FY 2020, the FBI opened more than 250,000 investigations with 73% related to the FBI's top priorities



- Terrorism
- Counterintelligence/Cyber National Security
- Cyber Criminal
- Public Corruption
- Civil Rights
- Transnational Criminal Enterprise
- White Collar
- Violent Crimes

(U//FOUO) Cases with Arrests (U//FOUO) Cases with Indictments
>44,300 / >29,400

The total number of investigations resulting in the arrest/indictment of at least one subject since FY 2016.

1,400	600
190	180
540	430
1,300	1,100
300	320
4,600	3,200
3,700	3,500
32,100	19,900

(U) FBI BY THE NUMBERS

(U) Freedom of Information Act (FOIA)

144K

(U) The total number of FOIA requests the FBI received since FY 2016. This number includes the projection for FY 2020.

(U) Internet Crime Complaints

2.1M

(U) The total number of complaints ic3.gov received from FY 2016 to FY 2020. The total loss is \$9.1 billion.

(U) National Threat Operations Center (NTOC)

6.5M

(U) Total calls and electronic tips the NTOC received from FY 2016 to FY 2020.

(U) Fingerprints

341.9M

(U) The total number of fingerprints received and processed from FY 2016 to FY 2020. The average time to process a fingerprint was less than six minutes in FY 2020.

(U) Laboratory Evidence Examination

299K

(U) The total number of evidence the FBI laboratory examined since FY 2016. The FBI completed 27.4% of total examinations for outside agencies.

(U) Victim Assistance

50K

(U) The total number of victims the FBI served from FY 2016 to FY 2020.

(U) National Name Check

17.8M

(U) The total number of National Name Checks processed from FY 2016 to FY 2020.

(U) National Instant Criminal Background Check System (NICS)

143.7M

(U) The total number of transactions the NICS and state users processed since FY 2016.

(U) Social Media Followers

3.0M Twitter
2.6M Facebook
1.8M Instagram

*All numbers were been rounded to nearest approximation.



The FBI: Field Offices At-a-Glance

(U) FIELD OFFICE ORGANIZATION STRUCTURE BY SIZE

- (U) XL field offices are led by an Assistant Director in Charge (ADIC).
- (U) Each ADIC is assisted by at least 5 Special Agents in Charge (SAC), responsible for the following programs: counterterrorism, counterintelligence, criminal, cyber, intelligence, and mission support.
- (U) Small, medium, and large offices are led at the executive level by an SAC.
- (U) All SACs are assisted at the mid-level management level by Assistant Special Agents in Charge (ASAC). The number of ASACs is scaled to the size of the office.
- (U) In 30% of field offices, a Senior Supervisory Intelligence Analyst (SSIA) assists the SAC with the intelligence program instead of an ASAC.
- (U) Every office is supported by an Administrative Officer (AO) responsible for finance, facilities, and human resources in the office.

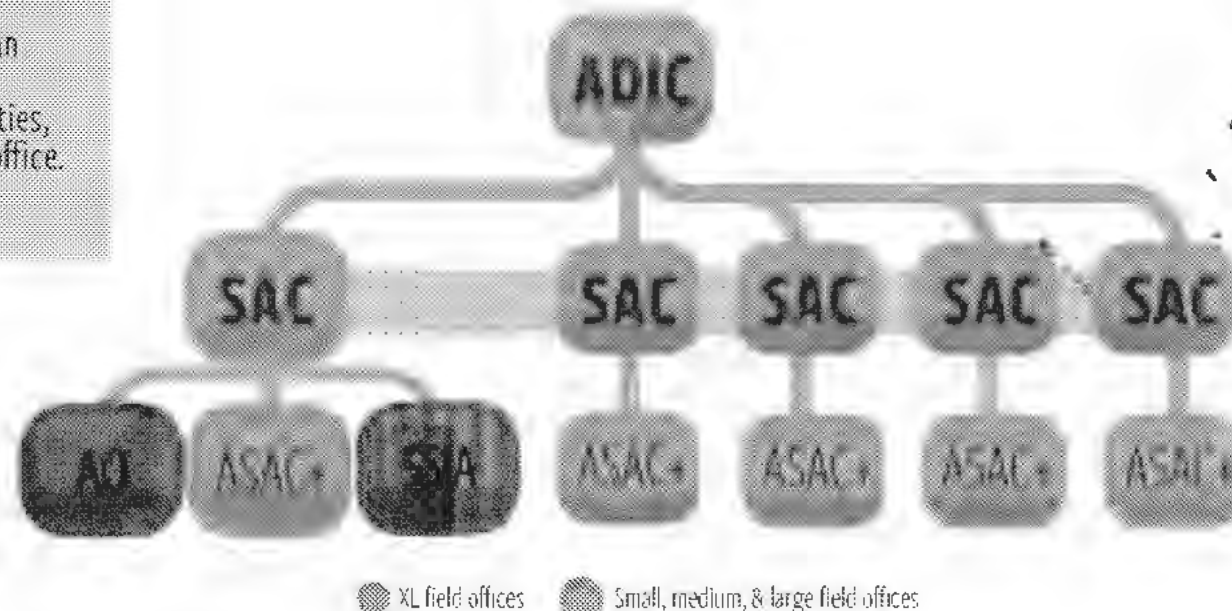
(U) BY THE NUMBERS (FY 2016 - FY 2020)



(U) FIELD OFFICE SNAPSHOT



(U) FIELD OFFICE ORGANIZATION CHART

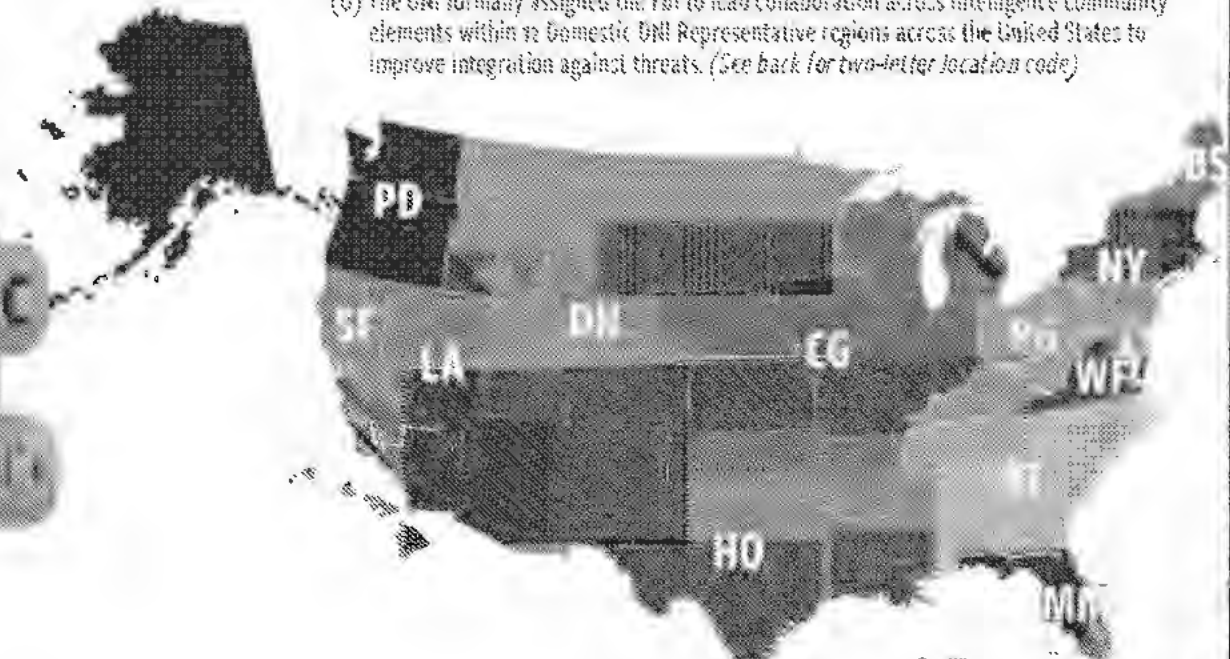


(U) FBI CASES BY FISCAL YEAR

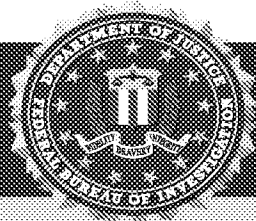


(U) DOMESTIC DNI REPRESENTATIVE PROGRAM

(U) The DNI formally assigned the FBI to lead collaboration across intelligence community elements within 12 Domestic DNI Representative regions across the United States to improve integration against threats. (See back for two-letter location code)



~~SECRET//NOFORN//LAW ENFORCEMENT SENSITIVE~~



The FBI: Legal Attaché Offices At-a-Glance

Legats are the FBI's representatives overseas

(U) GLOBAL PARTNERSHIP STRATEGY (GPS)

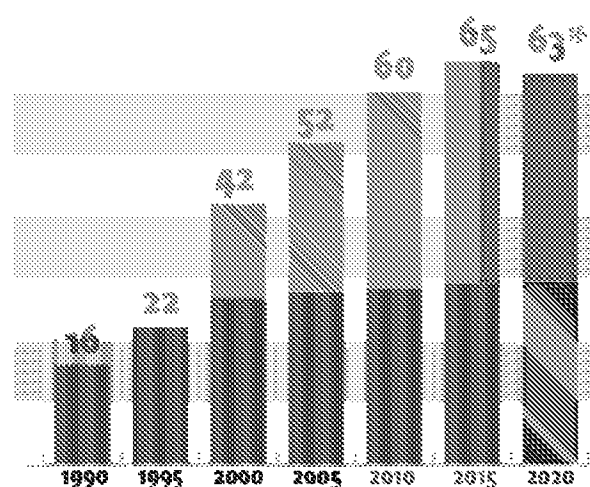
(U) The GPS comprises three key components and provides a framework for prioritizing and adapting the FBI's international presence to the evolving global landscape:

(U) Global Partnership Report (GPR): socializes the FBI's philosophy, accomplishments, priorities, and goals for international partnership building.

(U) Regional Partnership Strategies (RPSs): companion pieces to the GPR and outline the action plan for engagement with priority partners, including

(U) BY THE NUMBERS

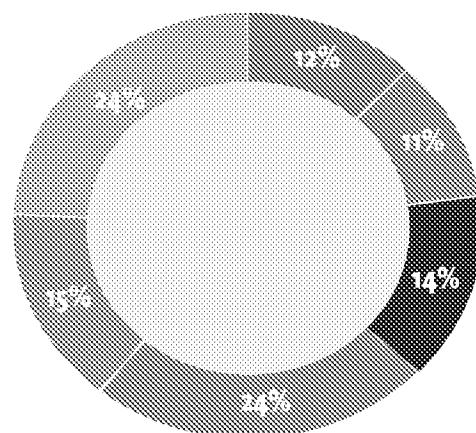
(U) Growth in Legat Offices



*The decrease in number of Legat offices during this period was the result of specific geopolitical factors.

(U) National Academy Students FY 2016 - FY 2020

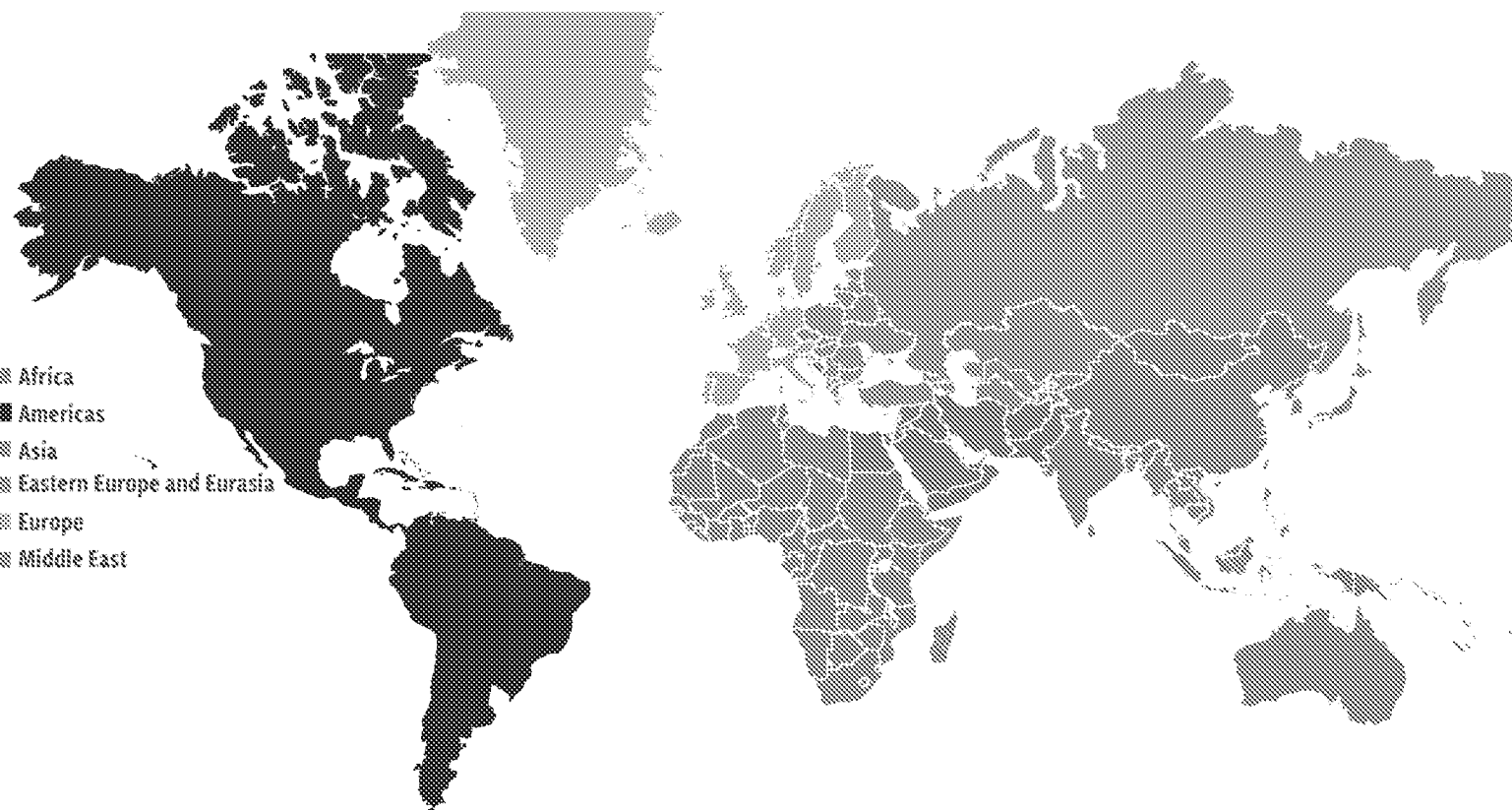
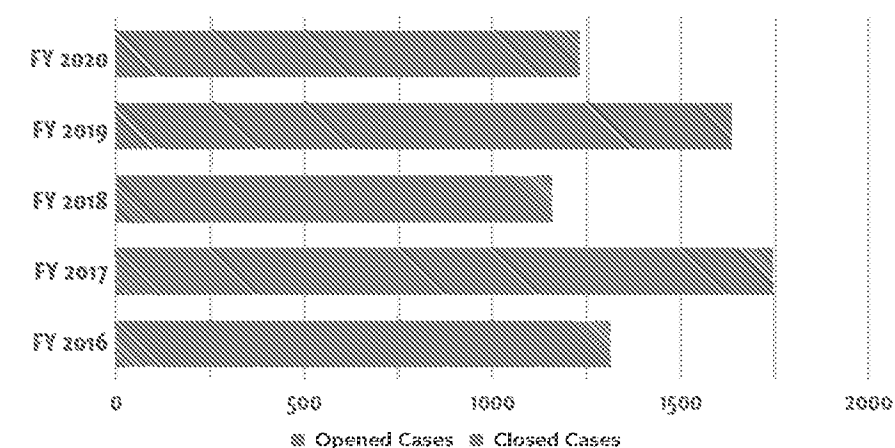
(U) Between FY 2016 and FY 2020, 474 international students representing 128 countries attended the FBI National Academy.



Africa
 Americas
 Asia
 Eastern Europe and Eurasia
 Europe
 Middle East

(U) Mutual Legal Assistance Treaty (MLAT) Requests

(U//FOUO) An MLAT is an international agreement between two countries for use by authorities conducting criminal investigations or prosecutions. MLATs outline the countries' legal obligations to assist. Requests to the FBI result in the opening of an MLAT case. The number of requests made to the FBI from FY 2016 to FY 2020 are outlined below.



The FBI: Legal Attaché Offices At-a-Glance



(U) OVERSEAS SNAPSHOT

- 63 Legal Attaché offices
- 30 Sub-offices
- 8 COMBATANT COMMAND detainees
- 300+ Employees in Legal offices supported by
- 200+ Employees at FBI HQ

Year Office
Opened

- Before 1991
- 1991-2000
- 2001-Present





The FBI: Diversity At-a-Glance

(U) DIVERSITY: A PRIORITY INITIATIVE

(U) Diversity is one of the FBI's eight core values and one of the Director's Priority Initiatives (DPIs). The six projects under the Diversity DPI are:

- (U) Revision of the Intelligence Analyst Selection Process
- (U) Diversity Agent Recruiting Program
- (U) Cross-Cultural Mentoring and Sponsorship Program
- (U) Employee Lifecycle Barrier Analysis
- (U) Bias, Diversity, and Inclusion Training Program
- (U) Inclusion Campaign for the FBI Workforce

(U) BY THE NUMBERS

26.6%

(U) Minorities in the FBI

Professional Staff: 31.9%
Intel Analyst: 22.8%
Special Agent: 18.6%

13.8%

(U) Minorities in SES

ADIC/SAC: 18.3%
HQ SES: 12.4%

44.0%

(U) Women in the FBI

Professional Staff: 58%
Intel Analyst: 55.2%
Special Agent: 20.1%

24.2%

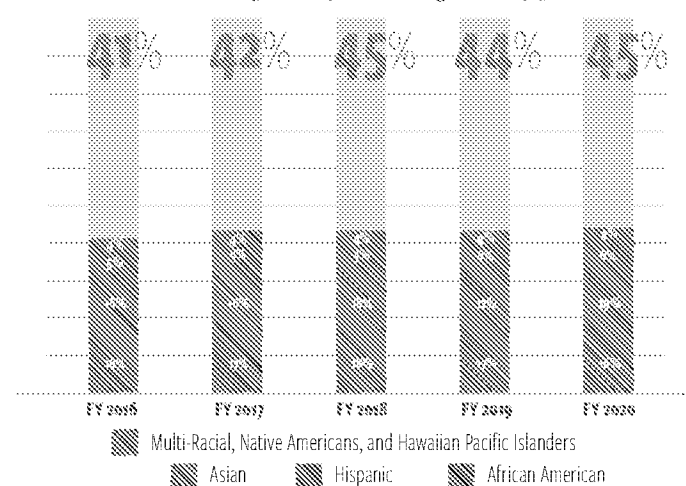
(U) Women in SES

HQ SES: 27.1%
ADIC/SAC: 15.5%

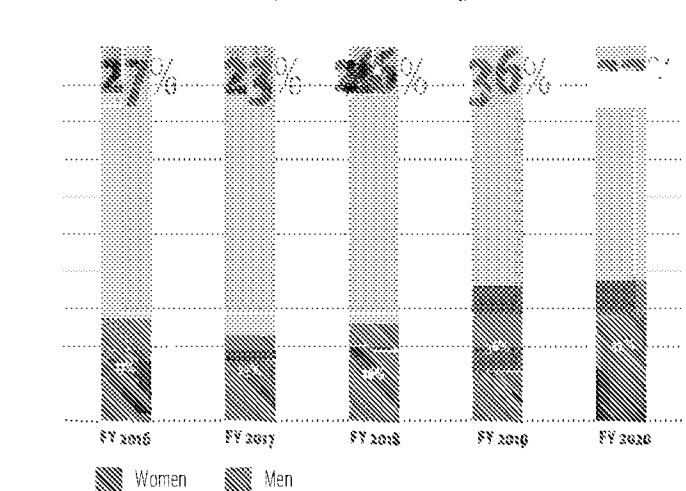
(U) HOW ARE WE DOING?

(U) The FBI has experienced a slight increase in the ethnic/gender diversity of special agent applicants during the past five years.

(U) Ethnic Diversity of Special Agent Applicants

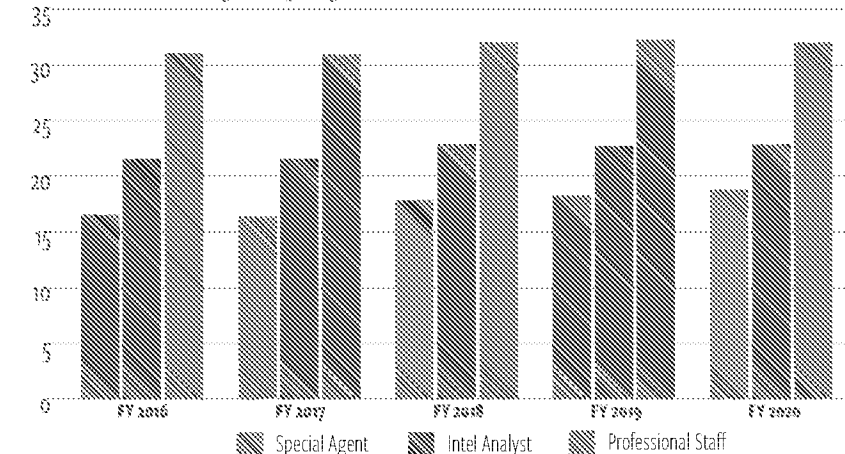


(U) Gender Diversity of Special Agent Applicants

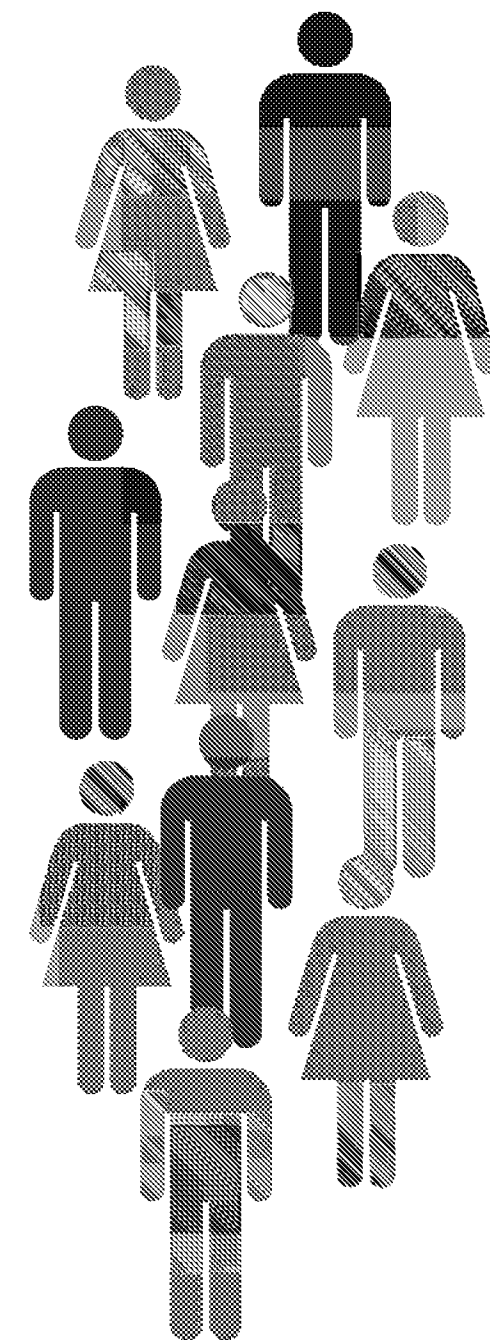
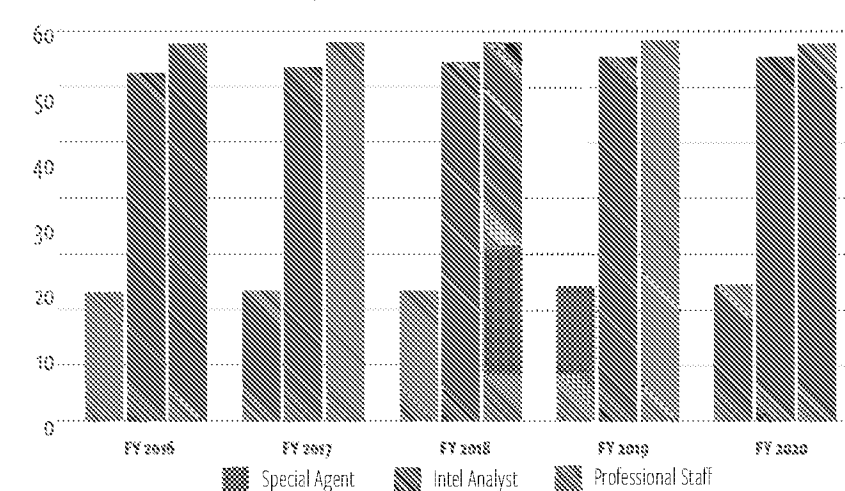


(U) We have more gender and ethnic diversity among professional staff and intelligence analysts.

(U) FBI Minority Employees



(U) FBI Women Employees



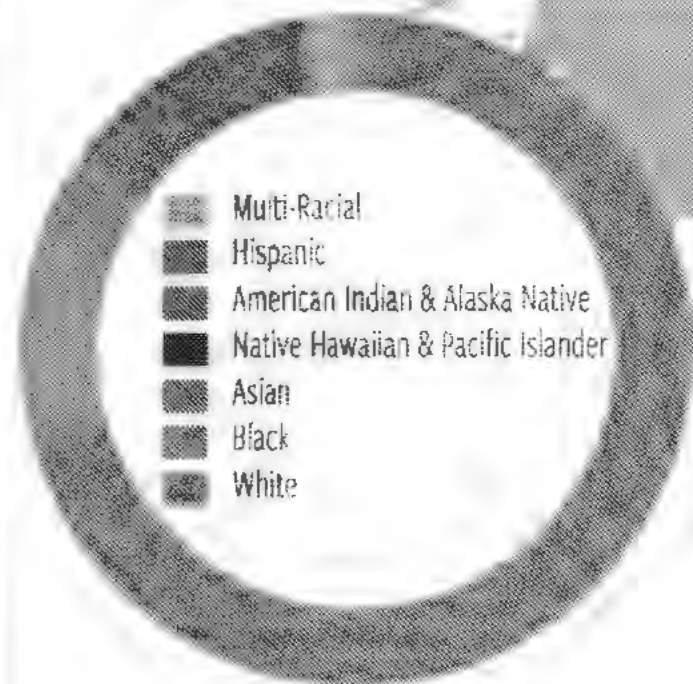
The FBI: Diversity At-a-Glance

FBI DIVERSITY EXECUTIVE COUNCIL

Diversity Advisory Committees

- (U) American Indian and Alaska Native Advisory Committee
- (U) Asian Pacific American Advisory Committee
- (U) Black Affairs Diversity Committee
- (U) Bureau Equality Committee
- (U) Hispanic Advisory Committee
- (U) Near and Middle East Advisory Committee
- (U) Persons with Disabilities Advisory Committee
- (U) Veterans Affairs Advisory Committee
- (U) Women's Advisory Committee

(U) ONBOARD OVERVIEW



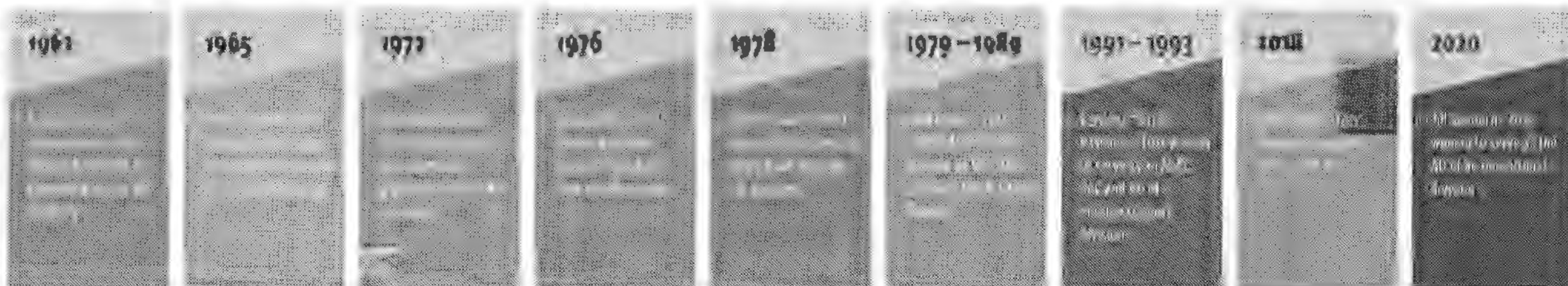
1.2

0.1

3.4

16.1

(U) SIGNIFICANT DIVERSITY EVENTS



(U) THREATS: 2020 AND BEYOND



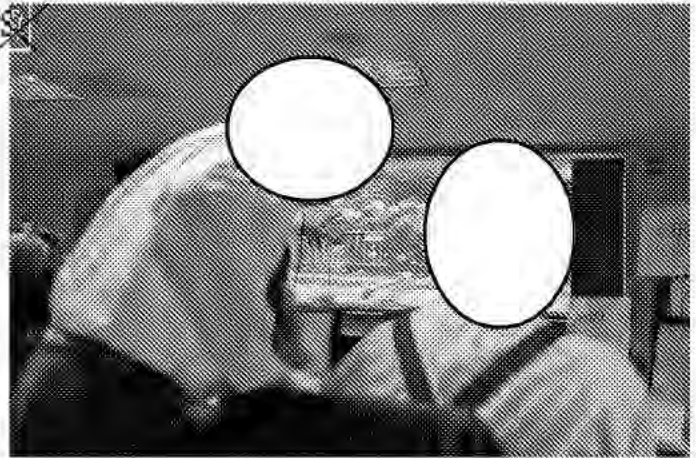
(U) THREATS: 2020 AND BEYOND

(U) OVERVIEW

(U)

UNCLASSIFIED

(U) Review of Boston Marathon Bombing Video

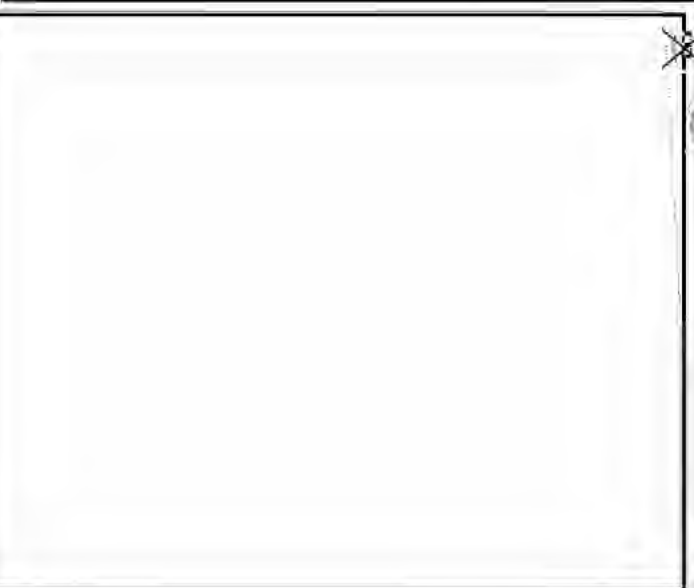
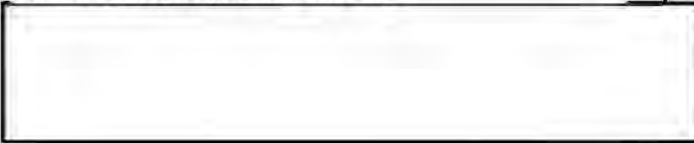


(U)

b1
b3
b5
b6
b7C
b7E

(U) TERRORISM

(U//~~FOUO~~) Preventing terrorist attacks remains the FBI's top priority. The terrorism threat has diversified in the post-9/11 environment to include



(U//~~FOUO~~) Racially or ethnically motivated violent extremists (RMVE) comprise the most lethal of the domestic violent extremist (DVE) threats in the United States. RMVEs conducted four of the five DVE attacks in 2019, resulting in 32 deaths. RMVEs are engaged in the unlawful use of threat of force or violence, in

violation of federal law, in furtherance of political or social agendas that are deemed to derive from bias, often related to race, held by the actor against others, including a given population group. DVEs demonstrate several indicators, some of which may be criminal. The FBI does not investigate, collect, or maintain information on U.S. persons solely for the purpose of monitoring activities the First Amendment protects.

(U) COUNTERINTELLIGENCE

UNCLASSIFIED

(U) FBI Bomb Tech



THREATS, 1020 AND 10210

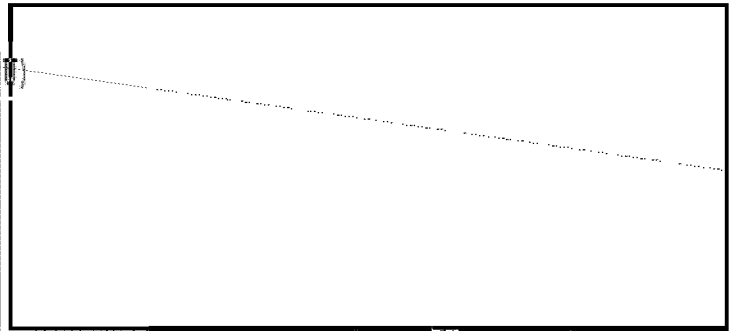
(U)

b1
b3
b5
b7E

(U) WEAPONS OF MASS DESTRUCTION

(U)

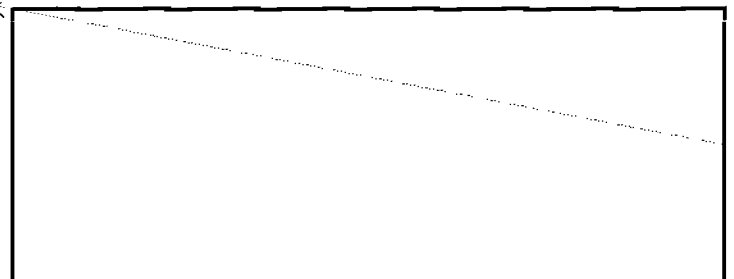
UNCLASSIFIED



(U//~~FOUO~~) Despite national and local disruption efforts, violent gangs continue to significantly impact U.S. communities, national interests, public safety, the U.S. economy, and the integrity of law enforcement and government operations. [REDACTED]

(U) CRIMINAL

(U//~~FOUO~~) The corruption of domestic public officials encompasses the corruption of legislative, executive, and judiciary officials and employees at all levels of government, including federal, state, local, and tribal. These employees exploit their official position for personal gain through bribes, quid pro quo arrangements, kickbacks, extortion, and misappropriation schemes. U.S. public officials and employees are vulnerable to individuals, businesses, foreign actors, and legitimate and criminal organizations who attempt to exploit the official's access and influence over policies, processes, and government spending. This corruption threatens U.S. national interests and public safety and is likely to cause the most severe damage to the integrity and operations of federal, state, and local governments, depending on the official's jurisdiction and range of influence. The corruption of domestic public officials impedes the ability for specific entities to function over time and causes lasting damage to the integrity and operations of a specific government entity. It is also likely to cause severe damage to U.S. critical infrastructure and key resources, all of which are potential targets for corrupt activity because of government regulation of the industries that service these sectors.

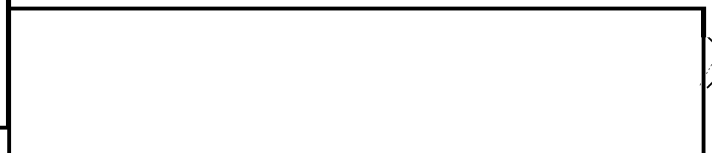
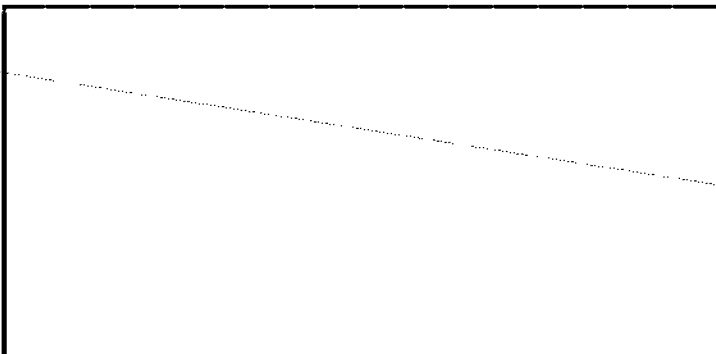


b1
b3
b5
b6
b7C
b7E

(U//~~FOUO~~) All children in the United States are at risk from crimes against children threat actors, particularly as the ease of access to online venues increases. The crimes against children threat — which includes abductions, sexual abuse and the production of child sexual abuse materials, sextortion, and child sex tourism — causes severe damage to national public safety and trust in law enforcement through loss of life and well-being.

(U//~~FOUO~~) The FBI is the primary agency investigating violations of federal civil rights statutes. These crimes, in particular allegations of color-of-law abuses, have the potential to cause civil disorder and damage to a city's economy and infrastructure; compromise integrity and operations of state, local, and federal agencies; and cause severe damage to public safety, health, and well-being. The impact of color-of-law violations is likely to remain significant in the near term.

(U) CYBER



(U)

UNCLASSIFIED



(U//~~FOUO~~) Cyber-criminal activity is having an observed substantial impact at the national level, which will likely continue given the ongoing use of cyber fraud schemes to target and profit from U.S. businesses and individuals.

THREATS 2020 AND BEYOND

b1
b3
b5
b6
b7C
b7E

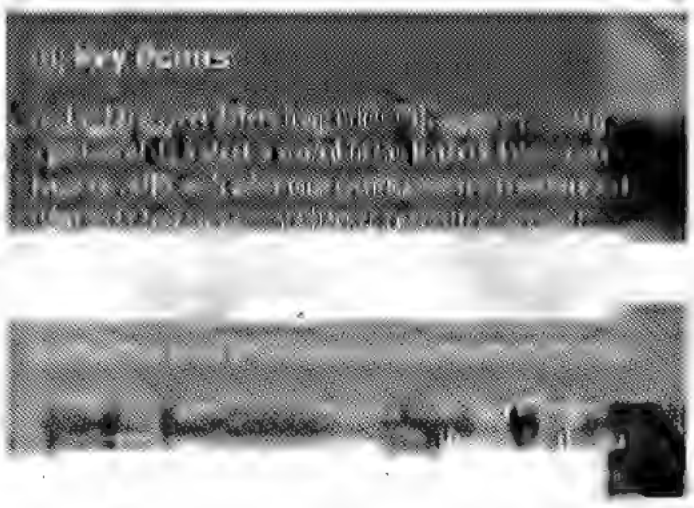
(U//~~FOUO~~) Illicit actors exploit cryptocurrency for a combination of reasons, including fast transactions with low fees, ability to avoid traditional banking structures, the perception of anonymity the technology provides and the disparate global regulatory environment. During the past decade, increased public awareness, improved ease of use, and greater merchant acceptance enabled less technically sophisticated actors to exploit this technology in a variety of ways.

(U) CHALLENGES

--

(U) FBI PROGRAM SPOTLIGHTS

(U) FBI BUDGET



CLASSIFICATION SPOTLIGHT

(U) INTERNAL OVERSIGHT AND THE OFFICE OF INSPECTOR GENERAL

(U) Key Points

(U) Because the FBI must ensure it maintains the trust of the people we serve, the FBI has rigorous internal and external oversight mechanisms to detect deficiencies within the FBI and safeguard accountability.

(U) The FBI takes seriously the recent DOJ Office of Inspector General's recommendations from the Crossfire Hurricane and FISA investigations.

(U) The FBI has made changes and will continue to make changes to strengthen our organization and ensure we exercise our authorities with objectivity and integrity.

(U) OVERVIEW

(U) The FBI has a long and robust relationship with the DOJ Office of the Inspector General (OIG). The FBI works closely with the various divisions within OIG to facilitate various inspections, reviews, audits, and investigations. The FBI has worked closely with the OIG to facilitate two recent, high-profile reviews regarding the Bureau's FISA authority: Crossfire Hurricane and FISA. Based on these reviews, the FBI has made changes to ensure it exercises its investigative authorities with objectivity and integrity.

(U) FISA Reviews

(U) In March 2018, the OIG began a review to examine certain FBI and DOJ actions during an FBI investigation opened on July 31, 2016, known as "Crossfire Hurricane." As part of this review, the OIG examined four FBI applications filed with the FISC to conduct FISA surveillance targeting Carter Page. On December 9, 2019, the OIG's Oversight and Review Division published the resulting report titled, "Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation" (Report), which provided nine recommendations to address deficiencies the OIG identified. In a December 6, 2019, letter, the FBI Director accepted the Report's findings and ordered more than 40 corrective actions to address the OIG Report's recommendations, including improvements beyond those the OIG recommended. The corrective actions include numerous updates to the forms used in the FISA application process and requirements for FISA approval and use; mandatory training related to the OIG Report findings; tighter controls over the FISA application process and the use of human source information; policy revisions

regarding the use of human source information and source validation; enhanced approval related to certain sensitive matters; and implementation of policies for defensive and transition briefings, among other items.

(U) In December 2019, following the public release of the Report, and because of its findings, the OIG commenced an audit of the FBI's process for verification of facts included in FISA applications. The audit's preliminary objective was to evaluate whether the FBI was in compliance with the Woods procedures requirements for applications related to U.S. persons. As part of this audit, the OIG reviewed 29 FISA applications from eight field offices and issued a Management Advisory Memorandum in March 2020, which included two recommendations. On July 29, 2020, the FBI submitted a declaration to the FISC stating that a further analysis by the DOJ National Security Division's Office of Intelligence (OI) and the FBI of the 29 dockets audited by the OIG confirmed "the overwhelming majority of the factual assertions in the applications were supported by documentation" and "[m]ore importantly, from a qualitative perspective, with two exceptions, the errors and unsupported facts [were] assessed by OI to be non-material, and the two material errors [were] not assessed to have invalidated any [FISC] authorization." The FBI continues to work closely with the OIG on the issues identified in the Management Advisory Memorandum.

(U) Oversight Process

(U) OIG's reviews typically go through several stages and culminate with a report. For audits and reviews, the OIG provides a memorandum to the FBI laying out its preliminary objectives. An entrance conference normally follows shortly thereafter, at which time the audit will enter the fieldwork phase. During this phase, the FBI works closely with OIG to satisfy all requests for information, including interviews with FBI personnel as well as documents.

(U) Once the OIG completes its fieldwork, the OIG produces a draft report and shares it with the FBI. The OIG then schedules an exit conference with the FBI to discuss factual or technical accuracy concerns. The FBI follows up with written comments regarding accuracy. The OIG then provides a final draft report at which time the FBI can comment formally. This formal comment, which will also include responses to any recommendations, is appended to the final report. After the OIG and FBI conduct classification and sensitivity reviews, the OIG releases the report to the public.

(U) The FBI then enters the report resolution phase, which consists of formal responses from the FBI to open recommendations. The OIG will provide periodic feedback memoranda, which would either close the recommendations or provide actions the FBI must take to close the recommendations.

(U) Throughout each stage of the process, the FBI has open channels of communication with the OIG. The FBI prides itself on the excellent rapport between the FBI and the OIG during the last several years. This great relationship allows the OIG to complete its work and the FBI to take corrective action, as necessary, to better fulfill its core mission.

(U) Some examples of actions the FBI has taken pursuant to OIG recommendations include the following:

- (U) Updates to the FBI's Home-to-Work Plan as part of a revised Government Vehicle Use Policy to have clear policy regarding task force officers and special agents taking government vehicles home.
- (U) Training related to Contractor Performance Assessment Reports (CPAR) to ensure contracting officers complete the CPARs uniformly and submit them in a timely manner.
- (U) Implementation of a technological mechanism to ensure the FBI identifies long-term confidential human sources to generate an automated response sent to the case agent, supervisor, and all those with a validation role.
- (U) Restrictions on access to its highly classified confidential human source shared system so that only those with a need to know could access said system.
- (U) Updates to Loose Media Kiosks at all the FBI's Regional Computer Forensic Laboratories to ensure users have taken the appropriate training before using the kiosks.
- (U) Revised procedures to ensure that software updates to Cell Phone Investigative Kiosks are properly communicated and documented.

(U) All of the aforementioned actions the FBI has taken in response to OIG recommendations have led to the closure of recommendations.

(U) The FBI also reviews matters concerning allegations of misconduct, whether or not such alleged misconduct may be considered criminal or administrative. The OIG maintains the statutory right of first refusal to investigate all misconduct matters. Before the FBI determines whether an allegation of misconduct requires an investigation, the OIG Investigative Division examines the allegation received and exercises a statutory right of first refusal to investigate the matter. OIG selects certain FBI investigations to monitor based on the type and severity of the allegation. Although the OIG may investigate any allegation of misconduct or criminality reported to the FBI, the OIG will most likely initiate an investigation of certain complaints:

- (U) An allegation of criminal conduct that if substantiated would likely result in criminal prosecution;
- (U) An allegation lodged against a senior FBI manager (GS-15 and Senior Executive Service);
- (U) Any matter the U.S. Attorney General, Director of the FBI, or the DOJ Inspector General determines would best be investigated by an entity outside the FBI;
- (U) A whistleblower retaliation allegation; or
- (U) A claim of whistleblower status based on potential retaliatory action.

(U) If the OIG determines an investigation is warranted, the FBI initiates a parallel investigation and coordinates with the OIG by responding to all requests for information, including interviews with FBI personnel, as well as obtaining requested documentation. The two entities within the OIG that conduct these investigations are the OIG Investigative Division and the Oversight and Review Division. In addition, the FBI coordinates with the OIG, Oversight and Review Division, as well as the DOJ Office of Professional Responsibility on allegations regarding whistleblower retaliation.

(U) For those matters that the OIG has deferred back to the FBI as a monitored referral, the FBI will keep the OIG apprised of pertinent information obtained either through the review of the initial allegation or administrative inquiry, if one was initiated.

(U) FBI BACKGROUND INVESTIGATIONS

(U) Key Points

(U) The FBI conducts interviews and gathers information through its background investigation process for use in the determination of eligibility for a security clearance.

(U) During an election year, the FBI receives requests to conduct background investigations from the Office of the Presidential Candidate of each political party and expedites investigations for key members of a newly elected or reelected Presidential administration.

(U) The FBI's background investigation process function is purely fact finding; the FBI does not adjudicate or render opinions on the background investigation results.

(U) OVERVIEW

(U) Forming a government after the election of a new or second-term President requires numerous background investigations for security clearances. In the lead up to the election, security clearances are also required for the Presidential candidates' advisors or senior staff. The FBI is responsible for conducting these investigations. Once election results are finalized, the Office of the White House Counsel (WHCO) or the Office of the President-Elect (OPE) requests background investigations for transition team members, along with other staff. Each investigation provides comprehensive information to the President or President-Elect and his or her staff to assess an individual's suitability, and may also be used to determine an individual's eligibility to access classified information or hold a sensitive position. The FBI does not adjudicate or render opinions on the results of a background investigation.

(U) BACKGROUND

(U) In support of Presidential administration transitions, the FBI conducts background investigations of potential Presidential appointees and White House staff. Our investigations are thorough and comprehensive inquiries designed to verify information the potential appointee or staff member provides, which may assist the WHCO or OPE with decision-making concerning an individual's suitability for federal employment, as well as access to classified materials.

(U) Executive Order 12968 requires an individual to undergo a background investigation before being granted access to classified information and to ascertain whether

the individual continues to meet the requirements for access. During election years, presidential transition teams may submit names of key personnel to initiate FBI background investigations in advance of Election Day. The Intelligence Reform and Terrorism Prevention Act of 2004 allows for temporary security clearances designed to allow for a smoother transition and to prevent lapses in national security coverage.

(U) FBI background investigations focus on character and conduct, emphasizing such factors as honesty, trustworthiness, reliability, financial responsibility, criminal activity, emotional stability, foreign influences, and other pertinent areas. Field agents gather information, which includes checks of national records and credit checks, as well as verification of education, residences, employment, and military service. The FBI makes inquiries with appropriate federal, state, and local law enforcement and regulatory agencies and licensing authorities. It also may report any information or circumstances that may develop during the background investigation and could have a bearing on the candidate's suitability for the position and/or access to national security information.

(U) Through our extensive investigative process, the FBI interviews persons who are knowledgeable of the candidate. Sometimes we conduct interviews of individuals the candidate identifies: references, associates, superiors, supervisors, colleagues, coworkers, and neighbors. Information obtained through interviews may be the opinion, hearsay, or personal knowledge of the person interviewed. Agents also may identify other individuals whom they wish to interview.

(U) If the background investigation develops information of alleged misconduct or any other type of unfavorable information or issues that may be pertinent to the candidate, all aspects of the allegation or issue are thoroughly explored. Every effort is made to substantiate or refute the information. The FBI does not render an opinion on the allegation and reports all information gathered.

(U) The FBI's role is to deliver a report of accurate and complete information. The prioritization and extent of each background investigation is based on the position for which the individual is being considered and whether the candidate has been the subject of a prior background investigation. For example, the relative importance and scope of an investigation for a Presidential appointment or judicial nomination is higher and more expansive than that of a staffer being considered to work in the Executive Office

of the President. Whereas the expanse of the former may refer back to the individual's 18th birthday, the latter may consist only of limited inquiries and interviews concerning the past five years of the candidate's life.

(U) Following the certification of election results, the Presidential transition period begins. Although it may seem as if the reelection of a President would result in limited transition background investigations, it historically has not been the case. For the last three second-term Presidents, an average of 43 percent of their Cabinet secretaries, deputy secretaries, and undersecretaries left their positions following the President's election to a second term, resulting in new appointments.

(U) If a new President is elected, the OPE identifies approximately 100 key positions in the President-Elect's administration, all of which must undergo a background investigation to be ready to assume their new positions following Inauguration. Those positions include the President-Elect's Cabinet, other positions with Cabinet-

level status, and high-ranking members of the White House staff, such as the counsels, chiefs of staff, and national security advisors to the President and Vice President. By the end of the process, the FBI will have completed more than 1,200 background investigations for positions within a new administration, with more than half being for Presidential appointments that require Senate confirmation.

(U) After field agents complete the investigations, they provide the results to FBI Headquarters where they are reviewed for thoroughness. FBI Headquarters provides an investigative report to WHCO or OPE for use as it deems appropriate. As previously stated, this information also may be used to assess an individual's eligibility to access classified information or hold a sensitive federal government position. Once the FBI presents this report, our involvement ends. WHCO or OPE then adjudicates security clearances for potential White House personnel and appointees.

(U) FBI FACILITIES



(U) Key Points

(U) The FBI strives to create unmatched facilities that provide our agents and professional staff with the tools and training required to meet evolving threats.

(U) The Bureau is now rapidly expanding its footprint across 1,600 acres at Redstone Arsenal in Huntsville, Alabama, to drive a new era of innovation alongside the nation's top defense, law enforcement, and technology organizations.

(U) The FBI will continue to innovate within the J. Edgar Hoover Building to find efficiencies to sustain its critical operations despite the building's failing infrastructure, as we engage in further discussions on a potential replacement of the current facility.

(U) OVERVIEW

(U) As America's adversaries equip themselves with advanced technology and new methods for conducting espionage, the FBI strives to create unmatched facilities that provide our agents and professional staff with the tools and training required to meet these evolving threats. The FBI's commitment to modernizing and expanding its facilities portfolio is being realized today. Whether through the centralized cost-efficient data centers powering the FBI's networks, or the futuristic, robot-controlled Central Records Complex in Winchester, Virginia, the Bureau's larger campuses have all seen multiple construction efforts designed to accommodate and train one of the nation's most resilient workforces. State-of-art facilities are essential if we are to outpace increasingly complex global threats.

(U) BACKGROUND

(U) Redstone Arsenal

(U) Within the next five years, the Bureau plans to construct sophisticated research facilities at Redstone Arsenal in Huntsville, Alabama, and rapidly expand the FBI's capabilities to analyze case data in record time for use by our agents and law enforcement partners. Our Redstone complex will also give our agents access to on-site training facilities that mimic real-world scenarios, replete with neighborhoods and rural environs for unmatched field instruction for the FBI and its law enforcement partners.

(U) Although FBI has maintained a presence at Redstone Arsenal for almost 50 years, the Bureau is now rapidly expanding its footprint across 1,600 acres positioned

among some of the nation's top defense, law enforcement, and technology organizations. These new facilities will drive a new era of innovation in Huntsville, a city becoming the Silicon Valley of the South, where the lower cost of living and modern amenities are among the many highlights for FBI employees relocated there.

(U) Counter-IED Center of Excellence: With the presence of Hazardous Devices School and Terrorist Explosive Device Analytical Center (TEDAC), the FBI has identified Huntsville as its Counter-IED Center of Excellence. The Hazardous Devices School has provided training for more than 20,000 local, state, and federal first responders and bomb techs and is the nation's only facility that trains and certifies public safety bomb technicians. The school features classrooms, explosive ranges, and mock villages. Joining the Hazardous Devices School is TEDAC, a multi-agency organization that coordinates the efforts of the entire government to gather and share forensic data and intelligence about tactics, techniques, and procedures. TEDAC has received more than 100,000 IED submissions from more than 50 countries and has called Huntsville home since 2016.

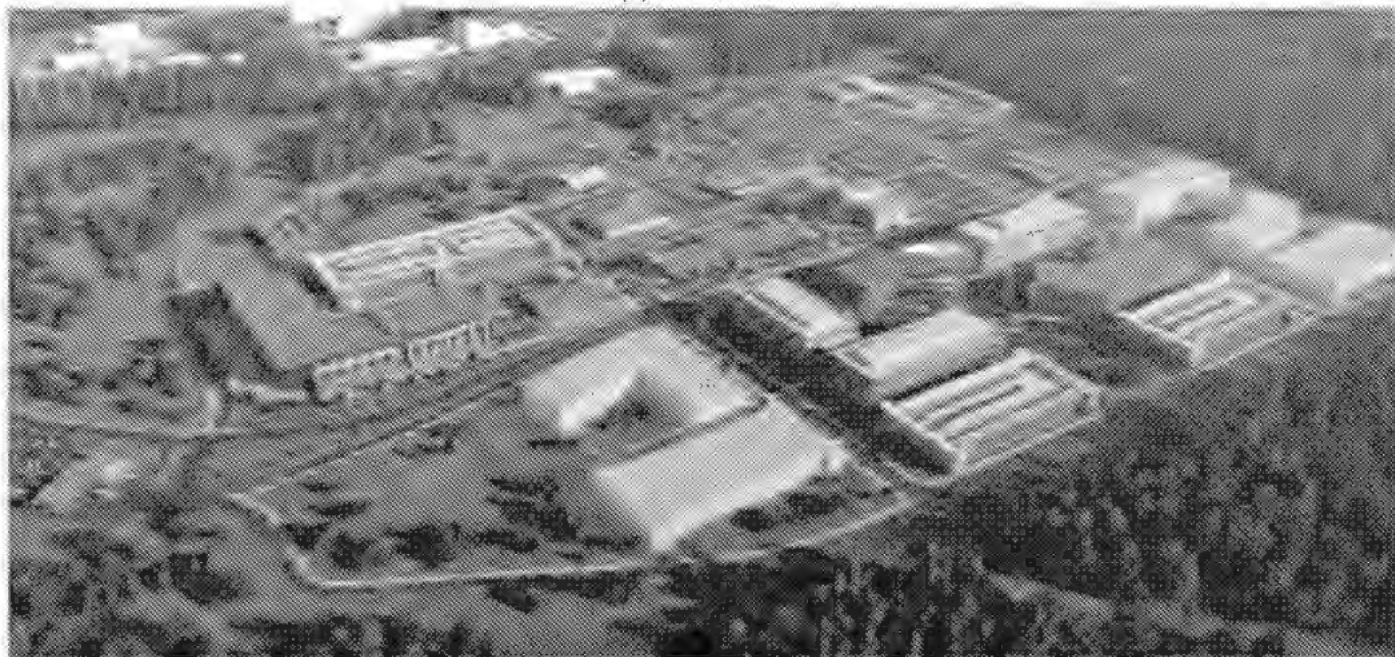
(U) Strategic Realignment: The FBI recognizes it is not required to perform all its mission functions in one central location. Realigning certain functions to Huntsville allows the FBI to strategically grow its workforce both operationally and professionally. The realigned functions were carefully identified to support the goal to enhance our analytics and resiliency. By August 2021, the FBI anticipates the relocation of 1,400 personnel to Redstone, with additional positions expected to relocate in subsequent years.

(U) Advanced and Specialized Training: Redstone's South campus offers opportunities to collaborate with other government agencies to hone specialized skills required to meet the mission and enhance law enforcement capabilities. Specialized training facilities will offer dedicated classrooms, labs, and workbenches to develop tradecraft under real-world simulation in the campus's innovative Smart City. This new capability creates diverse realistic environments — urban, suburban, and rural — for unique training that mimics real-world scenarios the FBI's operational workforce encounters.

(U) Enterprise and Applied Technology: The FBI is growing its enterprise and applied technology capabilities in data analytics, research and development, testing, and training. One of the major developments opening in 2024 is the

UNCLASSIFIED

(U) FBI Redstone



highly innovative Science and Technology District. These facilities have been strategically designed and configured to equip FBI personnel with the technological capabilities to sift through voluminous amounts of case data. The district's Innovation Center will generate technical experimentation and development capability on never-before-seen levels for law enforcement.

(U) These world-class facilities make up just a handful of the Redstone facilities designed to ensure FBI personnel and its partners are well-equipped to overcome increasingly sophisticated threats in the coming years.

(U) NATIONAL CAPITAL REGION FACILITIES

(U) The FBI manages more than 40 lease agreements in the National Capital Region (NCR) (both direct and in partnership with GSA), totaling more than 5.7 million in rentable square footage with an annual rent of \$167 million. Although most sites are located in the immediate vicinity to Washington DC regional locations range as far as Richmond, Virginia, to the south, Linthicum, Maryland, to the north, and Winchester, Virginia, to the west. These locations house key operational personnel and storage facilities for equipment, supplies, and records. In addition, a few locations provide specialized capabilities vital to the FBI's mission, including national security, cyber, and crisis response.

(U) STATUS OF FBI HEADQUARTERS

(U) Built in 1975 to support 2,000 personnel, the FBI Headquarters infrastructure, including mechanical, electrical, and life safety systems requires critical repairs

or replacement to safely support the current capacity of 5,500 FBI personnel. In lieu of a new FBI Headquarters building, upgrades are required to replace failing plumbing and piping, mechanical system supply, and main electrical system switchgear that have exceeded their useful life.

(U) In pursuit of a new FBI Headquarters building, GSA announced in 2014 a procurement strategy to construct a new facility in one of three potential NCR locations in Maryland and Virginia. The administration canceled this project in 2017 because of a lack of funding. The FBI and GSA have recently proposed new NCR locations to the Office of Management and Budget and await further action.

(U) The FBI continues to plan and innovate within the J. Edgar Hoover Building to find efficiencies to sustain its critical operations despite the building's failing infrastructure as the FBI continues to engage with oversight entities about the potential for a new facility located on the existing Pennsylvania Avenue footprint.

(U) CENTRAL RECORDS COMPLEX

(U) The FBI's new Central Records Complex in Winchester, Virginia, will house more than two billion pages of records by 2022. The 256,000 square-foot facility uses robots to help manage the storage of truckloads of archived records now housed at each of the FBI's 56 field offices and other sites. Construction of the facility began in late 2017 and was completed in August 2020, when employees loaded the first records into custom-designed bins to be shuttled away by robots into darkened, climate-controlled confines for safe keeping and easy retrieval.

(U) Built for nearly 500 employees, the facility also includes an office support building, visitor screening facility, and surface parking lot. The Central Records Complex houses an automated storage and retrieval system used to store and retrieve records quickly and efficiently, leveraging innovative technologies never before used in the federal government. The system manages more than 361,000 records storage bins with lids (specifically designed for this system) using an overhead grid of frameworks, allowing robots to retrieve the desired records.

(U) THE NEW DATA CENTER ON THE POCATELLO CAMPUS

(U) Maintained for more than 30 years, the FBI's campus in Pocatello, Idaho, is home to a newly completed data center that is part of the Bureau's data consolidation strategy. The data center will provide DOJ agencies with both classified and unclassified data processing capabilities for the foreseeable future.

(U) The data center has evolved from a continuity of operations facility for a single data center into a consolidated campus of four main buildings and a number of smaller facilities (more than 245,000 sq. ft.) serving about 330 employees. As part of the DOJ-wide data center consolidation project, the facility — along with a handful of other FBI data centers — consolidates leased data centers across DOJ in Northern Virginia, Texas, Maryland, and other areas. Completed in 2020 at a cost of \$170 million, the data centers allow the FBI to realize an average annual cost offset of \$15 million per year, create efficiencies (most notably through energy reduction), and provide modern technological architecture. This consolidation strengthens the cybersecurity posture for all DOJ components using the facility and provides the flexibility needed to focus on and rapidly respond to mission requirements.

(U) FACILITIES UPDATES ACROSS THE FBI

(U) *Criminal Justice Information Service:* Established in 1992, Criminal Justice Information Services (CJIS) serves as a high-tech hub and provides state-of-the-art tools and services to law enforcement, national security/intelligence community partners, and the general public. Currently, we are updating the main entrance to the CJIS campus, lobby, and constructing a new Clarksburg Resident Agency.

(U) *The FBI Academy (Quantico):* The FBI Academy is the FBI's law enforcement training and research center in Quantico, Virginia. In January 2021, major renovations will include new security features at the East and West gates and a new FBI Police Command Center. A newly constructed visitor's center will feature a modern design for the prestigious campus. To improve the academy experience, the FBI has renovated the cafeteria and dormitory and revitalized the academy's courtyard to ease pedestrian traffic. The FBI's new Reflection Garden houses one of the FBI's 9/11 memorials and several granite sculptures, including one that honors the valued relationship between the FBI, the National Academy, and its law enforcement partners worldwide.

(U) *San Juan Field Office:* Completed January 2020, just three years after the devastation of Hurricane Maria, the new San Juan Field Office offers employees modern workspaces and creates a communications hub that can be sustained during hurricanes, seismic activity, or other natural disasters.

(U) *Legat Network Enhancement:* The FBI has 63 Legat locations and 30 sub-Legat locations throughout the world. During the past five years, the FBI has enhanced network connectivity specifically focused on the national security mission for these offices. We have nine current projects that will provide that enhanced connectivity to the remaining offices by the close of FY 2021.

(U) FBI CYBER STRATEGY



(U) Key Points

(U) FBI authorities, capabilities, and partnerships enable unique opportunities for the USA to impose risk and consequences on cyber adversaries.

(U) Public-Private Partnerships across government and public sectors are essential to countering cyber threat and defending the nation's national and economic security.

(U) The FBI, through the National Cyber Investigative Joint Task Force, is the lead agency for cyber threat response activities.

UNCLASSIFIED



(U) OVERVIEW

(U) Malicious cyber activity threatens Americans' public health and safety, national security, and economic security. No single agency can address these threats alone. Criminals and foreign states use cyber capabilities to exploit the gaps they perceive in the U.S. system between foreign and domestic authorities; national security and criminal threats; and government and private sector lanes for defending critical networks. In this complex environment, the FBI is the indispensable partner uniquely positioned to bridge these gaps.

(U) BACKGROUND

(U) *The FBI's Strategy to Impose Risk and Consequences on the Adversary*

(U) The FBI adopted a new cyber strategy in FY 2020 to change the cost-benefit calculus of criminals and foreign state actors who believe they can compromise U.S. networks, steal U.S. financial and intellectual property, and hold U.S. critical infrastructure at risk, all without incurring any risk themselves. Under this strategy, the FBI uses its unique role as the lead federal agency with law enforcement and intelligence responsibilities to not only pursue its own actions but also enable partners to defend networks, attribute malicious activity, sanction bad behavior, and take the fight to adversaries overseas.

(U) As the world's premier cyber investigative agency, the FBI uses domestic collection capabilities, its global footprint, and partner engagement to attribute cyber crimes and attacks. This is the first step toward holding adversaries accountable.

(U)

(U) *Sharing Information and Enabling the Private Sector Ahead of the Threat*

(U//~~FOUO~~) The FBI's global presence uses dual law enforcement and intelligence authorities to pursue legal actions (e.g., shutting down dark markets, arresting criminals, and seizing virtual infrastructure) and to enable the actions of other partners through use of their own authorities (e.g., sanctions, demarches, and cyber effects operations).

b1
b3
b5
b6
b7C
b7E

(U)

(U)

(U) The FBI operationalizes this team approach through unique hubs where government, industry, and academia can work alongside each other in long-term, trusted relationships to combine efforts against cyber threats. Within government, that hub is the NCIJTF, which the FBI leads with more than 30 colocated agencies from the USIC and law enforcement.

(U//~~FOUO~~) Through its capabilities and blended authorities, the NCIJTF directs and supports whole-of-government campaigns to protect the United States from adversaries, criminal groups, and malicious actors in cyberspace, and assist U.S. allies to do the same. PPD-41, U.S. Cyber Incident Coordination, designated DOJ, acting through the FBI and NCIJTF, as the lead agency for cyber threat response activities, including investigation, attribution, and threat pursuit, accomplished by each of the NCIJTF's mission centers. With senior executives from partner agencies as leads, the NCIJTF mission centers spearhead integrated whole-of-government campaigns in line with the National Security Council's National Cyber Strategy, sequence whole-of-government campaigns to maximize impact against adversaries, operationalize intelligence to provide investigative analysis and tactical targeting to counter malicious cyber activities, and represent the interagency when briefing the campaign status to the National Security Council.

(U) The FBI also leads the National Defense Cyber Alliance, where experts from the government and cleared defense contractors share threat intelligence in real time, leading to notifications of 292 observations of suspected activity in its first year of operation.

(U) As the largest law enforcement partner in another such hub, the National Cyber Forensics and Training Alliance, the FBI has enabled alliance members to prevent more than \$1 billion in potential losses, identify critical threats impacting private industry, and support global law enforcement through identification of current threats most impactful to industry.

(U) Information gained through investigations and intelligence is quickly shared with the private sector across these formalized mechanisms and others to aid in the defense of critical infrastructure networks. The FBI reviews and analyzes suspected internet-facilitated criminal activity received through the Internet Crime Complaint Center (IC3) and generates leads to FBI field offices for investigation. IC3's website contains public service announcements outlining specific scams identified from this analyses and the FBI prepares an annual report to aggregate and highlight the data the general public provide.

The FBI's crosscutting roles and expansive private sector engagement inform the defense of U.S. critical infrastructure as well as the offensive and defensive missions of other U.S. and allied government agencies.

FBI PROGRAM SPOTLIGHTS

b1
b3
b5
b7E

(U) FBI CRITICAL INCIDENT NATIONAL ASSETS

FBI PROGRAM SPOTLIGHTS

(U) Key Points

(U//FOUO) The FBI maintains unique tactical, technical, and aviation assets trained and equipped to rapidly execute specialized tactics, techniques, and procedures to respond to critical incidents and threats worldwide.

(U//FOUO)

(U//FOUO) The FBI, through the Hazardous Devices School, is responsible for delivering certification, re-certification and advanced courses of instruction for all public safety bomb technicians throughout the United States. This school serves as the single source of bomb technician certification training to ensure common standards and training for bomb technicians nationwide.

(U) OVERVIEW

(U//FOUO) The FBI maintains specialized, standing tactical, technical, and aviation teams to provide rapid response to national security, criminal, critical incidents and threats. These specialized personnel and resources tackle the FBI's most complex missions from rendering safe an improvised explosive device (IED) or WMD to countering an attack or hostage taking. The mission of these specialized teams is accomplished through a layering of phased capabilities and standards across the FBI enterprise and through collaboration with federal, state, local, and international partners.

(U//FOUO) The FBI has approximately [] special agent bomb technicians in locations throughout the FBI's domestic and global offices. These technicians conduct a range of operations from rendering IEDs safe to major case support, from conducting WMD diagnostics to gathering intelligence overseas. The bomb technicians support FBI investigations through post-blast evidence collection, interviews of bomb makers, and assessing the technical feasibility of a terrorist or criminal device. In addition, the bomb technicians work closely with their public safety bomb squad partners.

b1
b3
b5
b7E

(U) BACKGROUND

(U) Countering IED and WMD Capabilities

(U//FOUO) On behalf of the Attorney General, the FBI leads the Joint Program Office (JPO) for Countering Improvised Explosive Devices (C-IED), established through PPD-17, Countering Improvised Explosive Devices, to coordinate United States C-IED policy in support of the National Security Council process. The JPO C-IED facilitates the integration and alignment of necessary domestic, transborder, and international activities across the USG to counter IEDs in accordance with national policy. []

b1
b3
b5
b6
b7C
b7E

response, and law enforcement assistance. To enhance field office SWAT teams during large scale multi-office operations and critical incidents, the FBI established a tactical task force model. Under this model, the task force forward deploys to the field office and provides full mission planning, target intelligence, resource recruitment and allocation, communications support, medical support, and logistics. The task force also stringently selects and trains personnel in all field offices able to surge in response to a critical incident.

(U) Aviation

(U//FOUO) In addition to the dedicated alert aircraft, the FBI maintains and operates a fleet of aircraft located across various field offices to conduct aerial surveillance and photography in support the FBI's mission. The FBI also maintains and operates aircraft to transport personnel and equipment to crisis sites worldwide; evidence in sensitive matters; and terrorism and criminal subjects as part of a foreign transfer of custody. In addition to supporting the aviation needs of the Attorney General and FBI Director, these aircraft provide a 24/7 response capability worldwide for all facets of FBI's intelligence and law enforcement operations.

(U) Specialized Tactical Capabilities

(U//FOUO) All 56 FBI field offices also maintain SWAT teams to deliver effective tactical operations for all facets of FBI investigative and intelligence activities, crisis

(U//~~FOUO~~) NATIONAL SECURITY THREAT ACTOR GLOBAL DETECTION PROGRAM

(U) Key Points

(U//~~FOUO~~)(U//~~FOUO~~)

(U//~~FOUO~~) TSC's watchlisting architecture has demonstrated success in creating a common operating picture across the USG for threat actors beyond known or suspected terrorists.

(U) OVERVIEW

(U//~~FOUO~~) Through DOJ, the FBI is heading the Executive Branch's efforts to create identity intelligence systems for both TOC and cyber actors, helping create a common operating picture for the USIC as well as federal, state, local, and tribal law enforcement.

(U//~~FOUO~~)(U//~~FOUO~~)(U//~~FOUO~~)

(U) BACKGROUND

(U//~~LES~~) As the threat environment evolved and national security threats increasingly converged,

With 17 years of experience providing

b1
b3
b5
b7E

(S)

(U)

(S)

(U) 75

~~(U//FOUO)~~ INFORMATION TECHNOLOGY MODERNIZATION INITIATIVE~~(U)~~ Key Points

~~(U//FOUO)~~ The FBI is investing \$225 million to transform presently available IT capabilities and infrastructure to meet the demands of current and future investigations.

~~(U//FOUO)~~ The networking, storage, and data analysis requirements across the FBI outpace the ability to meet mission demands.

~~(U)~~ Modernizing the FBI's IT enterprise will require substantial, sustained investment across three critical areas: network infrastructure, core data management for advanced analytics, and cybersecurity.

UNCLASSIFIED

~~(U)~~ Pocatello Data Center~~(U)~~ OVERVIEW

~~(U//FOUO)~~ The FBI is in the process of transforming presently available IT capabilities and infrastructure to meet the demands of current and future investigations. The networking, storage, and data analysis requirements across the FBI's criminal and national security programs outpace the ability to meet mission demands. Investments to transform IT infrastructure and provide adequate analytical capabilities are critical to accomplishing the FBI's mission today and in the future.

~~(U//FOUO)~~ Modernizing the FBI's IT enterprise will require substantial, sustained investment across three critical areas: network infrastructure, core data management for advanced analytics, and cybersecurity. Network infrastructure improvements will require upgrading network bandwidth between data centers, field offices, and resident agencies. [REDACTED]

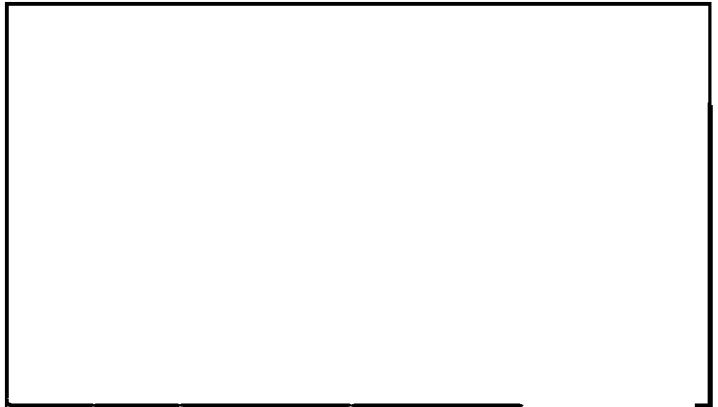
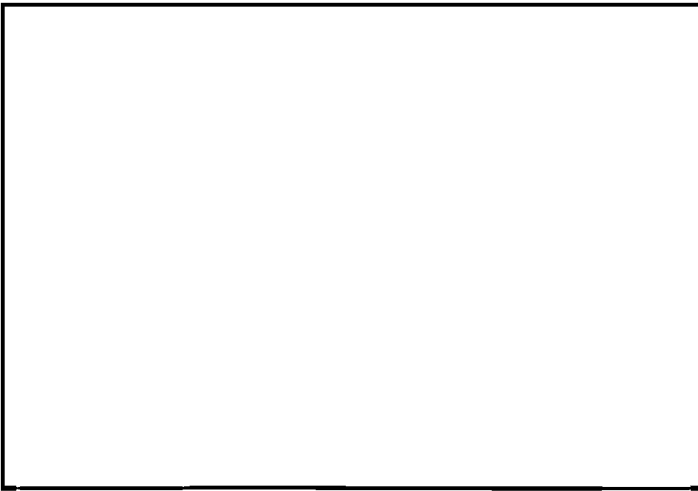
~~(U)~~ BACKGROUND

~~(U//FOUO)~~ To modernize investigative data analysis and keep pace with investigations, the FBI requires networks able to transport bulk data and reduce reliance on standalone, *ad hoc* systems that may lack adequate security protections. In addition to investments in networks and investigative tools, the FBI is also building facilities in Huntsville, Alabama, that will provide modern, collaborative space to develop advanced analytical tools and data management platforms to advance investigations.

~~(U//FOUO)~~ The FBI's ability to communicate securely and covertly with human sources is essential to collecting intelligence. The rapidly evolving digital environment, in which all manner of data produced by common day-to-day activities are captured, processed, and sold, has introduced new challenges in preventing adversaries from [REDACTED]

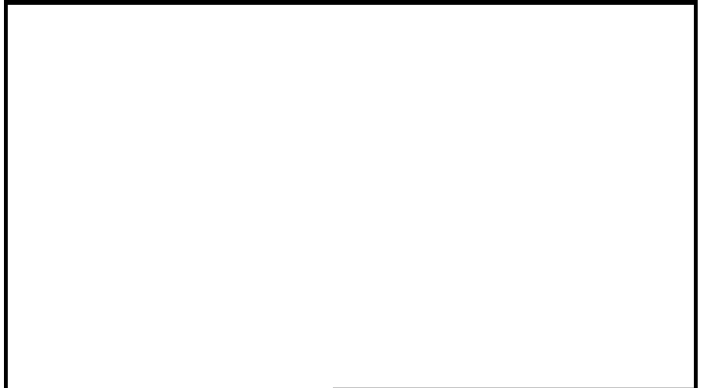
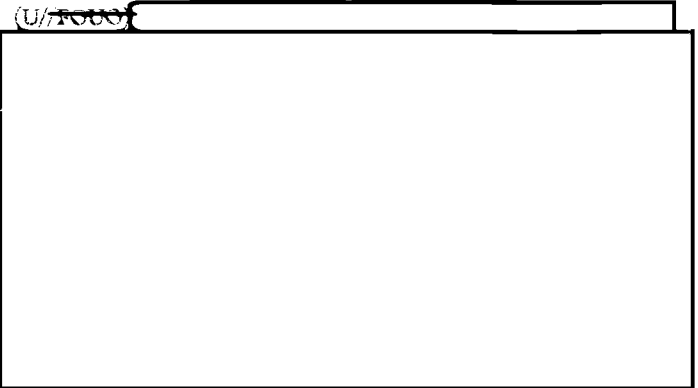
~~(U//FOUO)~~ Bandwidth and data challenges are not limited to major cases or large offices. [REDACTED]

~~(U//FOUO)~~ In addition to network infrastructure, the FBI is also enhancing its core data management for advanced analytics. The volume of data collected during investigations continues to rapidly expand. [REDACTED]



(U//~~FOUO~~) Investment in IT modernization also will support efforts to improve FBI cybersecurity through reduced reliance on standalone and *ad hoc* systems.

b5
b7E



(U) VIOLENT CRIME



FBI PROGRAM 5
b6
b7C
b7D

(U) Key Points

(U//~~FOUO~~) The FBI uses an intelligence-driven approach to identify the most prolific criminal organizations, violent offenders, and geographic area — combined with enterprise-level and targeted investigation — to dismantle criminal organizations and arrest the most violent offenders.

(U//~~FOUO~~) The FBI denies access of would-be criminals to the tools and places necessary to commit crimes, brings to justice perpetrators who carry out violent crimes, and provides support to the victims of those crimes.

(U//~~FOUO~~) Through its strategic initiatives and global footprint and partnerships, the FBI collaborated with federal, state and local partners to combat violent crime and provided unique technical resource capabilities, surged intelligence and operational assets, and increased prosecutions of violent actors.

(U) OVERVIEW

(U//~~FOUO~~) Violent crime continues to remain a persistent and significant threat both throughout the United States and across the globe. The FBI's expansive international footprint allows the FBI to lead efforts to address violent crime. In 2020, the FBI undertook a number of strategic initiatives aimed at addressing a myriad of crimes against children and gang-related violence. A key component of the FBI's ability to advance these initiatives is national and, in some cases, international task forces, which bring together state, local, tribal, and international resources to leverage law enforcement and intelligence capabilities. The FBI denies access of would-be criminals to the tools and places necessary to commit crimes, brings to justice perpetrators who carry out violent crimes, and provides support to the victims of those crimes.

(U) BACKGROUND

(U//~~LES~~) Major violent crime incidents can paralyze whole communities and stretch state and local law enforcement resources to their limits. The FBI can support these departments not only with a surge of personnel, but also by bringing assets not available at the state and local level. These assets include source development assistance, critical incident response support, implementation of enterprise investigations, prosecutorial support at the federal level, and technical support to address crimes using sophisticated internet platforms and networks. Intelligence supports all domestic and international violent crime cases to maintain a comprehensive understanding of the threat.

UNCLASSIFIED

89 Operation Cross Country



(U) An FBI agent interviews a young woman in a hotel room during a human trafficking operation in Denver.

The FBI continues to mitigate violent crime threats by developing an understanding of criminal tradecraft and vulnerabilities through analysis that is also disseminated to the FBI's domestic and global partners.

(U//~~FOUO~~) Crimes Against Children and Human Trafficking

(U//~~FOUO~~) The FBI provides a rapid, proactive, and intelligence-driven investigative response to the sexual victimization of children, other crimes against children, and human trafficking within the FBI's jurisdiction. The FBI currently leads 86 Child Exploitation and Human Trafficking Task Forces throughout the United States with representation from more than 400 state and local law enforcement agencies as well as more than 850 task force officers. In 2004, the FBI initiated the Violent Crimes Against Children International Task Force (VCACITF) to promote and develop a select cadre of international law enforcement experts to formulate and deliver a unified global response against child sexual exploitation matters. This task force, which is currently composed of more than 64 active task force officers from 46 countries, allows for real-time global collaboration between the FBI and its partners to recover children and bring perpetrators to justice. Since its inception, the VCACITF has been instrumental in the successful initiation and resolution of several high-profile, extremely complex investigations with a true global footprint. In 2005, the FBI created the Child Abduction Rapid Deployment (CARD) Team to provide a nationwide resource to support investigations of child abductions and critically missing children. The CARD Team is a nationwide resource for law enforcement at no cost to the requesting agency. CARD Team members attend specialized training on child abduction investigative

search techniques and technology and develop best practices through operational experience. The CARD Team has deployed 177 times since its inception, which has resulted in the recovery of 84 live children and 86 deceased children as well as the arrest of numerous offenders. The FBI also employs a team of child and adolescent forensic interviewers and victim specialists who engage with these victims and provide trauma-informed interviews and support services.

~~(U//FOUO)~~ Indian Country Crimes

~~(U//FOUO)~~ The FBI has been helping to ensure safety and security in Indian Country since our founding in 1908. Protecting tribal communities is a highly important responsibility. The FBI has the jurisdiction to investigate certain serious crimes committed on Indian reservations, and also works closely with tribal law enforcement partners to provide resources and assistance to maintain safety in Indian Country communities. The FBI provides guidance, training, program management and operational support to FBI field offices with respect to Indian Country. Through enhanced outreach, the FBI enriches its partnerships with federal, local, state, tribal law enforcement, nongovernmental organizations, private industry, and the public to aid in the decrease of violent crimes in Indian Country. The FBI created Safe Trails Task Forces to aid the FBI's mission. The USG recognizes 574 Indian tribes in the United States, with the FBI having investigative responsibility for federal crimes committed on approximately 200 Indian reservations. Through the development of confidential human sources, subject proffers and interviews, liaison contacts, and tripwires, the FBI increases intelligence reporting to address known gaps to better understand the Indian Country threat.

~~(U//FOUO)~~ Violent Incidents and Gangs

~~(U//LES)~~ Violent incident crimes and violent gangs pose a major threat to the American public, and this threat is significant and worldwide in scope. The FBI identifies, prioritizes, and targets the most violent and organized threat actors who pose an immediate threat to the safety of communities within their area. Using sophisticated investigative techniques, the FBI directs resources toward intelligence-driven investigations to positively impact the community. The FBI continues to develop collaborative partnerships to coordinate multi-jurisdictional investigations with federal, state, and local law enforcement and pursue federal prosecution so, when appropriate, significant prison sentences can be levied. The FBI works with federal, state, and local partners to identify the most violent offenders. Once identified, the FBI targets these offenders proactively and aggressively and proposes them for criminal prosecution. The FBI also focuses on Hobbs Act cases, including the robbery of

~~SECRET//NOFORN~~

~~(U)~~ FBI in Indian Country



commercial institutions, and armored carriers, as well as coordinates identification of additional Top Ten Fugitives. Through charges, arrests, and convictions, the FBI reduces the number of threat actors and protects the public's safety, health, and overall well-being. Through the development of human sources, subject proffers and interviews, liaison contacts, and tripwires, the FBI increases intelligence reporting to address known gaps to better understand the threat issue at a national level.

~~(U//LES)~~ The FBI also focuses on neighborhoods impacted by violent gangs and crimes of violence through the use of the Enterprise Theory of Investigations (ETI) concept. The National Gang Intelligence Center (NGIC) promotes multiagency collaboration efforts through intelligence-sharing initiatives and provides analytic support to our task forces. Ultimately, successful mitigation of gang activity in each field office territory leads to a decline in the overall threat gangs pose at a national level. By providing a strategic approach to coordinating violent gang investigations, intelligence-gathering activity, and victim support, and by supplementing liaison efforts, the FBI seeks to promote an integrated approach to mitigation across the nation. The ETI has proven successful to disrupt and dismantle the most violent offenders across the country.

~~(U//FOUO)~~ These initiatives have enabled the FBI's task forces to make progress addressing violent crime perpetrated by some of the nation's most violent offenders, gangs, and criminal enterprises nationwide. The FBI's 52 Violent Crime Task Forces and 172 Safe Streets Task Forces are responsible for the seizure of thousands of illegal firearms, the dismantlement of multiple criminal enterprises and the arrest, indictment, and conviction of thousands of criminals in 2020 alone.

(U//~~FOUO~~) Gang violence does not always originate in the United States. Therefore, the FBI, which has a robust investigative footprint in affected countries, continues to lead the effort to disrupt and dismantle transnational gangs, including MS-13, from their points of origin. DOJ-initiated Task Force Vulcan, an FBI-led multiagency effort to combat MS-13 violence across the hemisphere by targeting violent gang cliques in the United States and Central America. The Transnational Anti-Gang Task Force, established in 2007, now has [] task force officers ([] in El Salvador, [] in Guatemala, and [] in Honduras) responsible for the investigation of MS-13 members operating in the northern triangle of Central America. These officers provide intelligence for U.S.-based FBI investigations.

(U//~~LES~~) In July 2020, DOJ announced Operation LeGend, a response to a local request for assistance to address an

increase of violent crimes in Kansas City, Missouri. As a result, and in response to recurring violence in other cities (see chart below), DOJ directed the FBI, ATF, DEA, and the U.S. Marshals Service to surge resources to the affected areas. The operation focuses on homicide, robbery, gang, and nonfatal shooting investigations, as well as the execution of violent fugitive warrants. The FBI quickly and efficiently surged resources to provide a mix of assistance across job families to accomplish the operation's goals. Additionally, the surge was strategically planned to include necessary technical assets, training for deployed personnel, and employees with skills and experience in violent crime investigations. These surges can also require significant financial resources to fund travel for investigators, victims, and their families, as well as the transportation of evidence, subjects and witnesses.

(U//~~LES~~) Violent Crime and Safe Streets Gang Task Force Statistics for FY 2020 (through August 2020)



(U//~~LES~~) Operation LeGend Statistics Since Inception (through September 30, 2020)

	Inception Date	New Cases Opened	Federal Arrests	State Arrests	Weapons Recovered	Search Warrants
Albuquerque	07/15/2020	54	27	26	65	34
Chicago	07/27/2020	124	71	55	49	14
Cleveland	07/15/2020	23	17	17	26	34
Detroit	07/15/2020	44	25	19	26	82
Indianapolis	08/18/2020	19	21	20	13	5
Kansas City	07/20/2020	75	57	66	66	41
Memphis	07/15/2020	27	11	8	43	21
Milwaukee	07/15/2020	44	15	99	65	49
St. Louis	08/10/2020	53	24	59	45	26
TOTAL		463	268	369	398	306

(U) PUBLIC CORRUPTION



(U) Key Points

(U//~~FOUO~~) Public corruption directly affects our national security, our freedom, our way of life and can undermine democracy by diminishing confidence in government institutions.

(U//~~FOUO~~) The top criminal priority of the FBI, public corruption causes severe damage to the integrity of federal, state, and local governments and to U.S. economic and critical infrastructures.

(U//~~FOUO~~) The FBI is the primary federal agency investigating all types of public corruption — these are among the FBI's most sensitive investigations because of the intense media attention and the potential to adversely, and irreparably, impact the reputations of public officials.

(U) OVERVIEW

(U//~~FOUO~~) Combating public corruption is the FBI's top criminal priority. It encompasses corruption of legislative, executive, and judiciary officials and employees at all levels of government who exploit their official position for personal gain through bribes, quid pro quo arrangements, kickbacks, extortion, and misappropriation schemes. The more than 22 million public officials — including federal, state, local, and tribal officials — across the United States make corruption a formidable threat throughout the country. U.S. public officials and employees are vulnerable to individuals, businesses, foreign actors, and legitimate and criminal organizations that attempt to exploit the officials' access and influence over policies, processes, and government spending. Foreign governments influence domestic public officials and endeavor to recruit them to buy influence, exploit social rifts, and degrade faith in democracy.

(U) BACKGROUND

(U//~~FOUO~~) The FBI is uniquely positioned to investigate public corruption relating to state and local officials because of our presence throughout the United States, its territories, and the world. The United State has more than 22 million public officials, with approximately 19 million state, local, and tribal government employees who obtain public office through elections, appointments, direct hire methods, and contracts. The threat to each government entity changes regularly as each government

adapts priorities to address the needs of its constituents. When unchecked, state and local corruption can result in increased federal corruption, as state and local public officials pursue more prominent roles in federal offices.

(U//~~FOUO~~) Foreign Influence

(U//~~FOUO~~) Foreign influence is any effort from foreign governments to influence U.S. public officials, at all levels, through illegal means — typically facilitated through bribes and illegal campaign contributions. Through foreign influence campaigns, other nations can impact U.S. elections and interfere with U.S. policy at home and abroad. Compromised public officials erode domestic and international confidence in the USG, and weaken the nation's security.

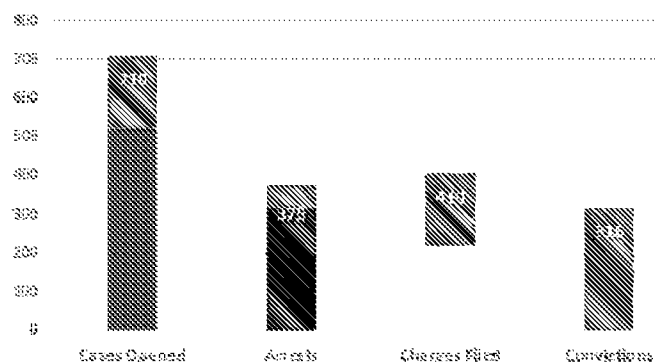
The FBI's Foreign Influence Task Force brings together criminal, counterintelligence, and cyber efforts to combat foreign influence.

(U//~~FOUO~~) Campaign Fraud and Election Crimes

(U//~~FOUO~~) Campaign finance violations and election fraud threaten the U.S. system of representative government by corrupting the democratic process. Election crimes

AMERICAN OVERSIGHT

(U) Public Corruption Statistics FY 2020



b5
b7E

include vote buying, absentee ballot fraud, illegally stuffing ballot boxes, or falsely registering to vote. During the 2016 election, the FBI developed intelligence related to potential voter suppression by foreign countries through social media, a newer tactic requiring continued attention. The FBI has identified violations through dark money and cryptocurrency because of a new reporting requirement for nonprofit organizations.

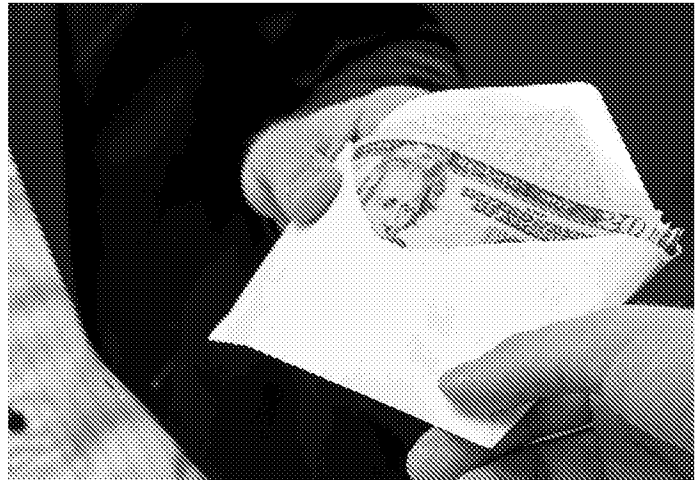
(U//~~FOUO~~) Prison Corruption

(U//~~FOUO~~) Corruption in federal, state, and local correctional facilities remains an issue, with more than 1.4 million individuals incarcerated in federal and state prisons and another 600,000 held in local jails. Corrupt prison staff compromise their official positions and personal integrity by performing illegal acts on behalf of prisoners in exchange for some form of remuneration. The FBI's prison corruption initiative, which began in June 2014, addresses contraband smuggling by local, state, and federal prison officials in exchange for bribe payments. Through this initiative, we work to develop and strengthen collaborative relationships with state and local corrections departments and the DOJ OIG to help identify prison facilities plagued with systemic corruption and to employ appropriate criminal investigative techniques to combat this threat. Increased advances in technology continue to present challenges to mitigating corruption within correctional facilities.]

(U//~~FOUO~~) Border Corruption

(U//~~FOUO~~) The U.S. land border is more than 7,000 miles with an additional 95,000 miles of shoreline the federal government must protect. Corruption at the U.S. borders

UNCLASSIFIED



and ports of entry presents a significant threat by allowing violent drug cartel members, foreign intelligence services, terrorism subjects, and weapons smugglers to enter the United States. The continued emergence of large-scale infrastructure projects and the accompanying staffing increases presents significant opportunities for additional corruption. The large volume of cargo entering maritime ports, government contract opportunities, and turnover of public officials also creates vulnerabilities individuals may exploits.]

(U//~~FOUO~~) Contract Corruption

(U//~~FOUO~~) Contract corruption involves all stages of the contracting process, and often also involves fraud against the government. Contract corruption causes continuing damage to U.S. economic and critical infrastructures. The FBI disrupts corruption related to negotiation and award of contracts by identifying key infrastructure projects across the United States and ensures coordination with the OIGs across the United States.

FBI-JTTF

(U) FBI SUCCESSES

b6
b7c

(U) DISRUPTING FOREIGN INTELLIGENCE ACTIVITIES

(U) Key Points:

(U//FOUO) The FBI is going beyond collaboration to actually integrating efforts with other intelligence and law enforcement agencies. We are using all available tools to bring the fight to our adversaries' doorsteps, including [REDACTED]

(U//FOUO)



(U) The San Francisco Russian Consulate begins burning materials after receiving a 48-hour notice to vacate.

(U) OVERVIEW

(U//FOUO) The FBI is going beyond collaboration to actually integrating efforts with other intelligence and law enforcement agencies. We are using all available tools to bring the fight to our adversaries' doorsteps, including [REDACTED]

(U) BACKGROUND

(U//FOUO) The threats to U.S. national security are persistent, multifaceted, and increasing. China is determined to supplant the United States as the dominant military and economic superpower by stealing cutting-edge U.S. technology and intellectual property. Russia has become more sophisticated in its illicit attempts to influence our elections and foreign policy. Foreign adversaries are conducting complex campaigns to steal U.S. technology and destabilize our system of government by fueling mistrust in the security of our democratic process.

(U) REDUCING RUSSIAN COLLECTION PRESENCE IN THE UNITED STATES

FM/SUSC/SEC

b1
b3
b6
b7C

~~(S)~~ (U)

FBI SUCCESSIONS

(U) REDUCING CHINESE COLLECTION PRESENCE IN THE UNITED STATES

(U//~~FOUO~~) Nontraditional Collector Mitigation / Visa Denial Proclamation

(U//~~FOUO~~) Disrupting China's Cyberattacks

b1
b3
b5
b7E

~~(S)~~
(U)

UNCLASSIFIED

FBI SUCCESSSES

(U) China's Approach to Technology Transfer



(U) In August 2019 and August 2020, a federal grand jury returned two separate indictments charging five cyber actors, all of whom were residents and nationals of China. These actors were members of a hacking group in China known as APT41, with computer intrusions affecting more than 100 victim companies in the United States and abroad. The same federal grand jury returned a third indictment in August 2020 charging two Malaysian businessmen who conspired with two of the Chinese hackers to profit from computer intrusions targeting the video game industry in the United States and abroad. In addition to arrest warrants for all of the charged defendants, in September 2020, seizure warrants were issued resulting in the recent seizure of hundreds of accounts, servers, domain names, and command-and-control web pages the defendants used to conduct their computer intrusion offenses.

(U) FOREIGN INTERFERENCE IN U.S. ELECTIONS

(U) FITF does this is by establishing relationships: at the federal level with other government agencies, at the state and local levels with election officials, and in the private sector with campaign staffs and social media companies. FITF also exchanges intelligence with governments and law enforcement entities abroad that are working to counter the same types of operations targeting their elections.

(U) FITF partners with the private sector by sharing threat indicators with U.S. technology companies and, in partnership with DHS and ODNI, by making publicly available online the FBI's Protected Voices initiative. Protected Voices helps campaigns, companies, and individuals better understand the malign foreign influence threat, practice good cyber hygiene, and recognize threat indicators.

(U) Dismantling Election Interference Social Media Accounts

b1
b3
b5
b7E

FBI

~~(S)~~ (U)

FBI SUCCESSES

(U//~~FOUO~~) Previous whole-of-government efforts and task forces functioned on an *ad hoc* basis and lacked centralized guidance, resources, and infrastructure. The NCITF is a true partnership, co-chaired by the FBI, DoD, and CIA, with multiple leadership positions open to all participating agencies. The NCITF is moving forward as one counterintelligence team, integrating members' missions and authorities, and is proving to be a formidable front line against foreign actors seeking to harm the United States.

(U//~~FOUO~~) *Tactical Analytical Cell*

(U) INTERAGENCY AND INTERNATIONAL
COLLABORATION

b1
b3
b5
b7E

(U) The investigative challenges and threats to our national security are growing in both volume and sophistication. The NCITF and [] are examples of FBI innovations to meet the threats. We are proactively taking the fight to our nation's adversaries, both domestically and internationally.

(U//~~FOUO~~) IMPROVED INTELLIGENCE PRODUCTION FOR POLICYMAKERS

FBI SUCCESS

(U) Key Points

Through FBI intelligence efforts, the unique perspective of the FBI — based in part on the bureau's collection capabilities, and its domestic law enforcement partnerships — is presented in a

(U//~~FOUO~~) The FBI produces an array of products and continues to USIC products, including the PDB, to provide timely and relevant intelligence to customers.

(U//~~FOUO~~)

(U) OVERVIEW

(U//~~FOUO~~) To offer policymakers intelligence vital for their decision-making, the FBI has developed a plethora of intelligence products.

(U) BACKGROUND

(U//~~FOUO~~)

(U//~~FOUO~~)

(U) Policy-level Impact

b1
b3
b5
b7E

(U)

~~(S)~~



(U//FOUO)



(U) Congressional Sharing

(U//FOUO)



the FBI updated its internal processes in 2020 to address progress in the production of external intelligence products and improve dissemination of those products to the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. The FBI reviewed existing guidance, in coordination with the DOJ Office of Legal Affairs, to ensure the FBI was maximizing dissemination of finished intelligence products to the House and Senate intelligence committees related to the

FBI's national security mission. Those changes increase the FBI's opportunity to share analytic products with these committees on counterintelligence and cyber threats, among other intelligence the FBI already provides.

b1
b3
b5
b7E

(U) GLOBAL BIOMETRICS INITIATIVE

(U) Key Points

(U) As a result of the Global Biometrics Initiative, the FBI has shared tens of thousands of latent prints and DNA profiles of terrorism suspects with trusted foreign partners.

(U) The FBI is designing global collection efforts to obtain biometrics from foreign law enforcement partners for high-value suspects of terrorist activity, egregious crimes, or transnational criminal activity.

(U) Partner nations have made more than 100 identifications from FBI collected latent prints from employee devices resulting in two successful prosecutions, as well as multiple arrests and entry denial.

(U) OVERVIEW

(U) Following the September 11, 2001, terrorist attacks against the United States, the U.S. Attorney General directed the FBI, through its Legats, to obtain fingerprints and biographic information for known or suspected terrorists processed by foreign law enforcement agencies.

(U) In response, the FBI established an initiative to conduct global biometric and biographic information collecting and sharing. The initiative is extremely successful in biometric collection efforts. The FBI has acquired more than three million fingerprint records from 92 foreign partners and made those fingerprint records available to domestic law enforcement, criminal justice, and intelligence agencies, as well as trusted foreign partners.

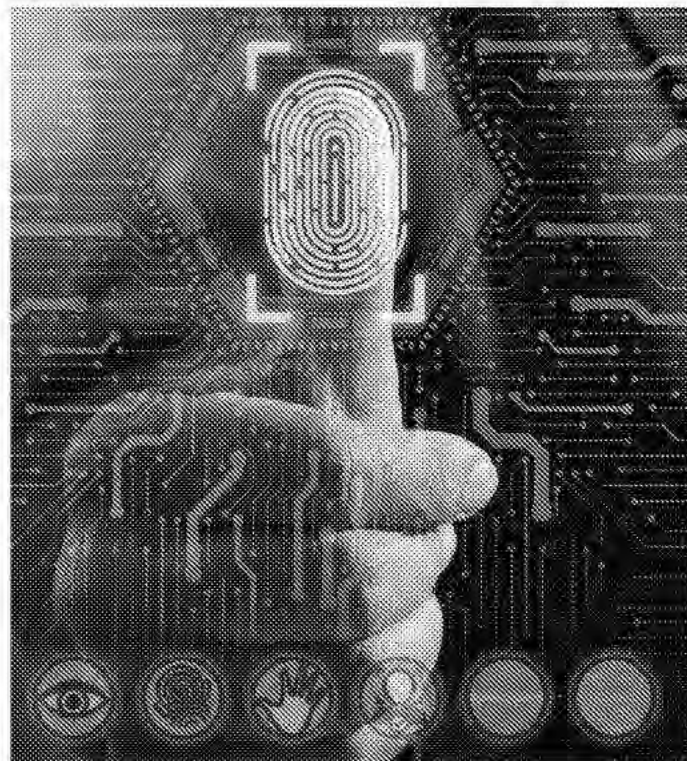
(U) In addition, the FBI has shared tens of thousands of latent prints and DNA profiles associated with terrorism with trusted foreign partners. To date, partner nations have made more than 100 identifications by searching these latent prints.

(U) BACKGROUND

(U) The FBI collaborates with the DHS to secure the signing and implementation of Preventing and Combating Serious Crime (PCSC) Agreements as part of the Visa Waiver Program with foreign countries. The FBI acts as the technical implementer for the DOJ to provide connectivity between United States and partner nation biometric systems for biometric exchange.

(U) In addition to acquiring and sharing biometrics through PCSC agreements, the FBI coordinates additional global collections efforts to obtain high-value biometrics

UNCLASSIFIED



from foreign law enforcement partners. Targeted biometric records pertain to individuals of interest to partner countries, the United States, the international law enforcement community, and U.S. military allies, and include individuals associated with or appropriately suspected of terrorist activity, egregious crimes, or transnational criminal activity.

(U)

(U) TEDAC serves as a single interagency organization to receive, analyze, and exploit all terrorist IEDs of interest to the United States. TEDAC coordinates the efforts of the entire government, from law enforcement to intelligence to military, to gather and share forensic data and intelligence about devices, tactics, techniques, and procedures — helping to disarm and disrupt IEDs, link them to their makers, and prevent future attacks. To date, TEDAC has received more than 100,000 IED submissions from more than 50 countries.

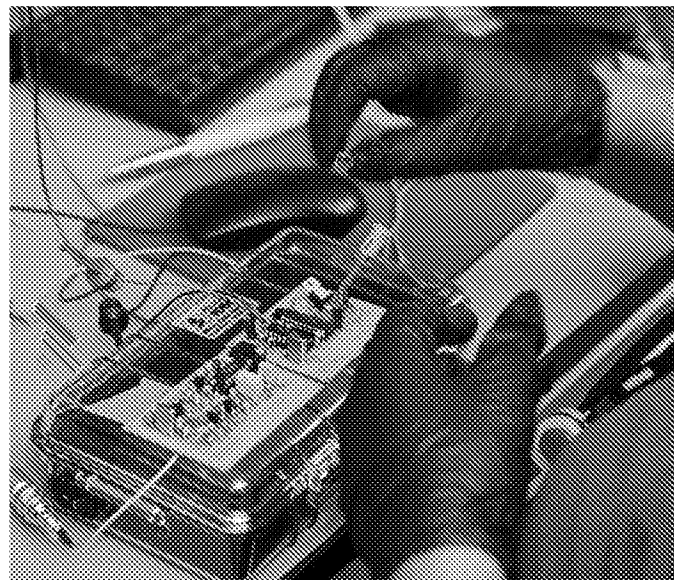
(U) TEDAC's organizational structure includes representatives from the DOJ, DoD, and international partner agencies that work collaboratively to address

IED-related issues and develop solutions in support of the counter-improvised explosive device fight.

(U) In addition, TEDAC uses the authorities within PCSC agreements to share appropriate latent prints and biometric information developed from IEDs and associated with terrorism, often in near-real-time, through the Law Enforcement Enterprise Portal. The FBI has been sharing terrorism-related prints with trusted foreign partners through this mechanism since 2016. To date, partner nations have made more than 100 identifications to FBI-developed latent prints resulting in two successful prosecutions and multiple citizenship and entry denials, as well as increased cooperation with allies of the United States.

(U) OPERATIONAL SUCCESSES

UNCLASSIFIED



(U//FOUO) In October 2019, the Canadian authorities apprehended an individual suspected of material support to terrorism — traveling from the United Arab Emirates to Toronto, Canada, with the intent to enter the United States — at the request of the FBI. Following biometric screening of the individual's fingerprint record, the individual was extradited to the United States to face charges.

b1
b3
b5
b7E

(U) VICTIM SERVICES PROGRAM

(U) Key Points

(U) Victim services plays a critical role in providing support and resources to the victims of crime and their families.

(U) For crisis response, the program has a special response team that provides victim services during mass causality events.

(U) Because of the program's extensive work with victim populations and community engagement, it is uniquely postured to share valuable subject matter expertise with FBI operational programs and our USIC, state, and local partners.

(U) In 2018, the FBI launched the Excellence in Law Enforcement-based Victim Assistance Training and Enrichment (ELEVATE) with our state, local, and tribal partners to assist with establishing or enhancing victim service programs within their agencies.

not only for the health and well-being of victims, but also the success of the investigations.

UNCLASSIFIED

Victim Services Program

Provided

200,783

services to victims and their families

And conducted

1,669

child/adolescent forensic interviews

(U) OVERVIEW

(U//~~FOUO~~) Across the United States, only 15 percent of law enforcement agencies have a victim services program. Providing such services to victims of crime not only supports their recovery and well-being, but also enhances investigative efforts and leads to more positive prosecutorial outcomes. Although the FBI has always prioritized support of victims, the FBI did not recognize the need for a large, professional, and mission-focused program until 9/11 — to respond to the thousands of victims associated with 9/11 and the victims of all criminal and national security investigations. Since then, the program has grown to include victim specialists within all 56 field offices, child and adolescent forensic interviewers stationed across the country, victim service coordinators, and the family engagement coordinator within the Hostage Recovery Fusion Cell. In addition, the program also has a crisis response team to provide victim services during mass casualty events, to share valuable subject matter expertise FBI-wide and with our partners, and to provide training to the law enforcement community to assist with establishing or enhancing victim service programs.

(U) BACKGROUND

(U//~~FOUO~~) The FBI's victim services program plays a critical role in providing support and resources to victims of crime and their families. The program assists victims in navigating the physical and emotional aftermath of a crime and the criminal justice system. This assistance is critical,

(U//~~FOUO~~) In addition, the program has a special response team that provides victim services during mass causality events. The team is composed of victim specialists, special agents, and intelligence analysts who provide on-scene support, death notifications, and coordination of support services to hospitalized victims and families of deceased victims. The team also collects, cleans, and returns personal effects for victims and their families. Since 2005, this specialty team has responded to 28 mass casualty events throughout the United States, including the shootings in Las Vegas (the deadliest mass shooting committed by an individual in the Western Hemisphere); Marjory Stoneman Douglas High School (the largest school shooting in U.S. history); the Tree of Life Synagogue in Pittsburgh (the deadliest attack on the Jewish community in the United States); and the recent WalMart shooting in El Paso (the deadliest attack on Latinos in modern American history).

(U) In addition to providing services to victims of crime, victim specialists, child and adolescent forensic interviewers, and victim specialist coordinators are uniquely postured to provide valuable subject-matter expertise because of their extensive work with victim populations and community engagement. The FBI is ensuring this expertise is being fully leveraged through the production of informative products shared across the FBI and with our USIC, state, and local partners.

(U) In 2018, the FBI launched ELEVATE with our state, local, and tribal partners to assist with establishing or enhancing victim service programs within their agencies.

(U) This program has three main tenets:

1. (U) *Specialized Training*: includes 9 weeks of classes that are accredited by the University of Virginia and a one-week residency at the FBI Academy in Quantico for practical exercises

2. (U) *Program Standards*: establishes program standards for direct services

3. (U) *Mentorship*: pairs participants with mentors from model programs for a year to assist in the building or enhancing of the participant's victim services program

DECLASSIFIED

(U) Pulse Nightclub Memorial



(U) The Pulse nightclub and memorial in Orlando, Florida, site of a tragic mass shooting on June 12, 2016

This page was automatically left blank.

~~RESTRICTED DATA~~ ~~RESTRICTED DATA~~

(U) ADDENDUM

~~RESTRICTED DATA~~ ~~RESTRICTED DATA~~

(U) FBI.gov RESOURCES

CATEGORY	TOPIC	FBI.gov LINK
RESOURCES	Mission & Priorities	https://www.fbi.gov/about/mission
	Leadership	https://www.fbi.gov/about/leadership-and-structure
	FAQs	https://www.fbi.gov/about/faqs
	Partnerships- operational, investigative, public, private sector	https://www.fbi.gov/about/partnerships
	Community Outreach	https://www.fbi.gov/about/community-outreach
	Law Enforcement	https://www.fbi.gov/resources/law-enforcement
	Businesses - full site	https://www.fbi.gov/resources/businesses
	Businesses: Private Sector partnerships	https://www.fbi.gov/about/partnerships/office-of-private-sector
	Victims	https://www.fbi.gov/resources/victim-services
	Reports and Publications	https://www.fbi.gov/resources/library
SERVICES	Criminal Justice Information Services	https://www.fbi.gov/services/cjis
	Critical Incident Response Group	https://www.fbi.gov/services/cirg
	CIRG: Strategic Information & Operations Center	https://www.fbi.gov/services/cirg/sioc
	Laboratory - full site	https://www.fbi.gov/services/laboratory
	Training Academy - full site	https://www.fbi.gov/services/training-academy
CRISIS RESPONSE	Training Academy: National Academy	https://www.fbi.gov/services/training-academy/national-academy
	Active Shooter & Resources	https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-resources
	CIRG	https://www.fbi.gov/services/cirg
NATIONAL SECURITY	Intelligence Guide for First Responders	https://www.dni.gov/nctc/jcat/jcat_ctguide/intel_guide.html
	Overview	https://www.fbi.gov/about/leadership-and-structure/national-security-branch
	Terrorist Screening Center	https://www.fbi.gov/about/leadership-and-structure/national-security-branch/tsc
	High-Value Detainee Interrogation Group	https://www.fbi.gov/about/leadership-and-structure/national-security-branch/high-value-detainee-interrogation-group

(U) FBI.gov RESOURCES

CATEGORY	TOPIC	FBI.gov LINK
CYBER	Cyber crime	https://www.fbi.gov/investigate/cyber
	Internet Crime Complaint Center (IC3)	https://www.ic3.gov/default.aspx
CRIMINAL	Public Corruption	https://www.fbi.gov/investigate/public-corruption
	Civil Rights	https://www.fbi.gov/investigate/civil-rights
	Organized Crime	https://www.fbi.gov/investigate/organized-crime
	White Collar Crime	https://www.fbi.gov/investigate/white-collar-crime
	Violent Crime	https://www.fbi.gov/investigate/violent-crime
	Surge in Violent Crime	https://www.fbi.gov/wanted/operation-legend
	Gangs	https://www.fbi.gov/investigate/violent-crime/gangs
	Opioids	https://www.fbi.gov/news/stories/raising-awareness-of-opioid-addiction
	Crimes Against Children	https://www.fbi.gov/investigate/violent-crime/cac
	Sextortion campaign	https://www.fbi.gov/news/stories/stop-sextortion-youth-face-risk-online-090319
SOCIAL MEDIA	Indian Country	https://www.fbi.gov/investigate/violent-crime/indian-country-crime
	Human Trafficking	https://www.fbi.gov/investigate/violent-crime/human-trafficking
	Facebook	https://www.facebook.com/FBI/
	Twitter	https://twitter.com/FBI?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor
	Instagram	https://www.instagram.com/fbi/?hi=en
	FBI Podcasts	https://www.fbi.gov/news/podcasts
	You Tube	https://www.youtube.com/user/fbi

(U) ACRONYMS

AD	Assistant Director
ADIC	Assistant Director in Charge
AEAD	Associate Executive Assistant Director
AO	Administrative Officer
AOR	Area of Responsibility
ASAC	Assistant Special Agent in Charge
ASCE	Academic Security & Counter Exploitation program
ATB	Adjustments to Base
BFTC	Basic Field Training Courses
CALEA	Communications Assistance for Law Enforcement Act
CARD	Child Abduction Rapid Deployment
CAT	Cyber Action Team
CBJB	Congressional Budget Justification Book
CBRE	Chemical, Biological, Radiological, or Explosive
CBRN	Chemical, Biological, Radiological, or Nuclear
CFIUS	Committee on Foreign Investment in the United States
CIA	Central Intelligence Agency
CIRG	Critical Incident Response Group
CISA	Cybersecurity and Infrastructure Security Agency
CITAC	Counterintelligence Tactical Analytical Cell
CITF	Counterintelligence Task Force
CJIS	Criminal Justice Information Services
CJS	Commerce, Justice, Science, and Related Agencies
CNE	Computer Network Exploitation
CPAR	Contractor Performance Assessment Reports
CR	Continuing Resolution
CRC	Central Records Complex
DAR	Diversity Agent Recruitment
DD	Deputy Director
DDD	Director's Decision Documents
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense

(U) ACRONYMS

DOJ Department of Justice
DPI Director's Priority Initiative
EAD Executive Assistant Director
ETI Enterprise Theory of Investigations
FBI Federal Bureau of Investigation
FFLs Federal Firearms Licensees

[REDACTED]

FIRRMA Foreign Investment Risk Review Modernization Act
FISA Foreign Intelligence Surveillance Act
FISC Foreign Intelligence Surveillance Court

[REDACTED]

FOIA Freedom of Information Act

[REDACTED]

GSA General Services Administration

[REDACTED]

HIG High-Value Detainee Interrogation Group
HPSCI House Permanent Select Committee on Intelligence
HRFC Hostage Recovery Fusion Cell
HUMINT Human Intelligence
IA Intelligence Analyst

[REDACTED]

IC3 Internet Crime Complaint Center
IED Improvised Explosive Device
IEP International Executive Program

[REDACTED]

IT Information Technology

[REDACTED]

LEEP Law Enforcement Enterprise Portal

b3
b7E

(U) ACRONYMS

Legat	Legal Attaché
MLAT	Mutual Legal Assistance Treaty
MOU	Memorandum of Understanding
MS-13	Mara Salvatrucha
NCIC	National Crime Information Center
NCIJTF	National Cyber Investigative Joint Task Force
NCITF	National Counterintelligence Task Force
NCR	National Capital Region
NCTC	National Counterterrorism Center
N-DEx	National Data Exchange
NGI	Next Generation Identification
NGIC	National Gang Intelligence Center
NICS	National Instant Criminal Background Check System
NIP	National Intelligence Program
NJTTF	National Joint Terrorism Task Force
NSA	National Security Agency
NSC	National Security Council
NSPM	National Security Presidential Memorandum
NTOC	National Threat Operations Center
OCP	Office of the Counsel to the President
ODNI	Office of the Director of National Intelligence
OI	Office of Intelligence
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPE	Office of the President-Elect
PCSC	Preventing and Combating Serious Crime
PDB	President's Daily Brief

PPD	Presidential Policy Directive
-----	-------------------------------

QFRs	Questions for the record
------	--------------------------

R&D	Research and Development
-----	--------------------------

b7E

(U) ACRONYMS

RCFL Regional Computer Forensic Laboratory

[REDACTED]

SA Special Agent

SAC Special Agent in Charge

SARs Suspicious Activity Reports

SIA Supervisory Intelligence Analyst

[REDACTED]

SSA Supervisory Special Agent

SSCI Senate Select Committee on Intelligence

SSIA Senior Supervisory Intelligence Analyst

SSTF Safe Streets Task Force

[REDACTED]

TCO Transnational Criminal Organization

TEDAC Terrorist Explosive Device Analytical Center

TOC Transnational Organized Crime

TRP Threat Review and Prioritization

TSC Terrorist Screening Center

UAS Unmanned Aerial Systems

UCR Uniform Crime Reporting

[REDACTED]

USG U.S. Government

USIC U.S. Intelligence Community

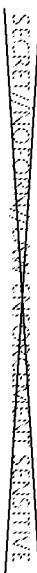
[REDACTED]

VCACITF Violent Crimes Against Children International Task Force

VCTF Violent Crime Task Force

WMD Weapons of Mass Destruction

b7E





FIDELITY BRAVERY INTEGRITY

Federal Bureau of Investigation
935 Pennsylvania Ave., NW
Washington, DC 20535
www.fbi.gov