Federal Bureau of Investigation

Addressing Threats to the Nation's Cybersecurity

As the primary investigative agency of the federal government for more than a hundred years, the responsibilities of the Federal Bureau of Investigation (FBI) have kept pace with ever-emerging threats and crime trends affecting the United States. From the notorious gangsters of the early 20th century, to espionage and sabotage during World War II, through the Cold War years and the global war on terrorism, the FBI has protected our nation. The 21st century brings with it entirely new challenges, in which criminal and national security threats strike from afar through computer networks, with potentially devastating consequences. While the FBI must adapt to meet these challenges, addressing the broad range of threats to the nation's cybersecurity is squarely within its mandate. *Why the FBI?*

It's our job.

The FBI has a unique dual responsibility, to prevent harm to national security as the nation's domestic intelligence agency and to enforce federal laws as the nation's principal law enforcement agency. These roles are complementary, as threats to the nation's cybersecurity can emanate from nation-states, terrorist organizations, and transnational criminal enterprises; with the lines between sometimes blurred.

The FBI's unified mission brings all lawful investigative techniques and legal tools together in combating these threats. This approach facilitates information sharing and ensures responsible stewardship of resources by collocating talent, tools, and institutional knowledge in a single organization.

- **Domestic Coordination within the U.S. Intelligence Community**

  As a member of the U.S. Intelligence Community (USIC), the FBI leads the National Cyber Investigative Joint Task Force (NCIJTF). Located in the Washington, D.C. metro area, the NCIJTF serves by Presidential Directive as the national focal point for coordinating cyber threat investigations. Representatives from the USIC member agencies, as well as select federal law enforcement partners, are present at the center and collaborate in identifying, mitigating, and disrupting cybersecurity threats.

- **Support to the Homeland Security Enterprise**

  As part of the homeland security enterprise, the FBI supports the Department of Homeland Security's (DHS) mission by investigating threats and incidents which affect the security of protected computers and networks. The results of these investigations increase collective knowledge which can be leveraged to improve the nation's security posture, such as providing effective mitigation strategies to potential victims. Additionally, actions taken by the FBI have succeeded in disrupting and dismantling threats. With the entire homeland security enterprise working together, and through a balanced approach employing both defensive measures and directed action against adversaries, our nation is safer.

Roles and Authorities in Brief

The FBI has the authority and responsibility to investigate and enforce all violations of federal law that are not exclusively assigned to another federal agency.
- Title 28, USC Section 533 & 28 CFR 0.85

"The Department of Justice and the FBI lead the national effort to investigate and prosecute cybercrime."
- The President's National Strategy to Secure Cyberspace, 2003

"The FBI is vested by law with the primary role in carrying out investigations within the United States of threats to the nation's security. This includes the lead domestic role in the investigation of international terrorist threats…and in the conduction of counterintelligence activities against foreign espionage and intelligence efforts directed against the U.S."
- Attorney General Guidelines for Domestic FBI Operations

"Intelligence elements of the FBI…shall collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence…"
- Executive Order 12333 and pursuant to Title 50, USC Section 401

- **Leadership within U.S. Law Enforcement**

  The FBI's capacity to respond to cyber incidents and emergencies in communities nationwide is enhanced through task force partnerships with other law enforcement agencies. Key federal, state, and local cyber investigative and forensic personnel, sworn and civilian, are teamed together in this endeavor. The FBI is enhancing the capabilities of each of its cyber task forces to address the full range of cybersecurity threats and function as extensions of the NCIJTF. No other agency can match this broad and robust presence, which is crucial for timely and effective incident response.

In the U.S. and abroad, we are where you need us.

Domestic — Whether you live and work in a large city or small town, chances are that the FBI has an office nearby. FBI field offices are located in 56 cities, with satellite offices in some 380 additional locations. Cyber agents at each field office are equipped to respond to events ranging from a significant data breach to a national cyber emergency. And, to supplement this standing capability, the FBI also maintains a rapid deployment team of highly specialized cyber agents.

International — Not only does 21st century technology enable global communication and commerce, it enables threat actors to apply their craft from anywhere in the world. For nearly 70 years, the FBI has stationed personnel overseas to build relationships that protect Americans at home. Today, the FBI maintains legal attaché offices within 75 U.S. Embassies globally, covering over 200 countries. Additionally, cyber agents have been embedded with foreign law enforcement partners in several key countries, fulfilling a liaison role to foster cooperation and mutual legal assistance.

We acknowledge the unique capabilities of private industry and academia, and the need for constant collaboration.

The U.S. Government cannot address cybersecurity threats alone. Ongoing collaboration with affected industries, security researchers, and academia is indispensible. The FBI maintains a presence and close partnership with the National Cyber Forensics and Training Alliance (NCFTA), and shares intelligence with the private sector through FBI-led InfraGard chapters and through various industry-specific Information Sharing and Analysis Centers (ISACs). In partnership with the National White Collar Crime Center (NW3C), the FBI offers the Internet Crime Complaint Center (IC3) as a means to receive cyber crime complaints from consumers and businesses for action by authorities, and to disseminate fraud alerts to the public.

FBI Headquarters, J. Edgar Hoover Building

We defend the Constitution by upholding the law, while protecting privacy and civil liberties.

Roles and responsibilities within the Executive Branch agencies are divided to ensure mission focus and clarity in regard to authorities. As a component of the Department of Justice, the FBI is responsible for investigations and intelligence collection within the territorial jurisdiction of the United States and relating to U.S. persons overseas.

Bound by the U.S. Constitution, relevant laws, and guidelines provided by the Attorney General, the FBI is governed by the principle of employing the least intrusive method necessary to further an investigation. When an investigative method would infringe upon an individual's reasonable expectation of privacy, approval and oversight by a U.S. District Court or the Foreign Intelligence Surveillance Court is required.

In its role as a protector and defender of the U.S. Constitution and enforcer of federal law, the FBI regularly takes action on behalf of victims whose privacy has been violated, such as through a computer intrusion or identity theft.

We care.

In the last decade, the FBI has assembled a team of hundreds of cyber experts with diverse and highly skilled information technology backgrounds. Our people are committed to serving the public by meeting cyber challenges head on and imposing consequences on those who victimize the American people through the misuse of computers and networks.