FBI CYBER Strategy

OUR VISION

For over a century, the FBI has been investigating crimes and collecting intelligence to protect the American public. As threats have evolved, so has our strategy. The FBI's new cyber strategy not only focuses on how we will confront the unique challenges faced in cyberspace, but also why we pursue our cyber mission: so the American people have safety, security, and confidence in a digitally connected world.

Safety is knowing that criminal and nation state actors are being held to account for targeting and compromising U.S. citizens, companies, and organizations. Accountability may come in a variety of forms ranging from indictments and red notices to sanctions, diplomatic pressure, or cyber operations.

Security is receiving actionable alerts about system and network vulnerabilities, derived from intelligence that only the FBI and its partners can provide. It means notifying targeted entities before they experience a breach and providing them with the tools and information necessary to defend themselves. We are committed to sharing as much as possible as quickly as possible so the public is alerted and prepared.

Confidence is knowing that the federal government is combatting these threats with fierce urgency and that if you become a victim, you will receive the attention you deserve. The FBI is working 24/7 and in tandem with the rest of the federal government and industry to break down walls and attack the cyber threat as a united front.

Our strategy drives us, but our vision inspires us. Together we'll fight to make it our reality.

OUR MISSION

Our Focus – what we do every day

To impose risk and consequences on cyber adversaries through unique authorities, world-class capabilities, and enduring partnerships, building on a century of innovation

OUR PLEDGE TO CYBER VICTIMS

Our Promise – compassion as we seek justice

In pursuing our mission, we recognize that we will encounter unique and novel issues related to privacy and handling of sensitive data. We will always treat victims with dignity and respect, protecting their privacy and data, and rigorously adhering to the U.S. Constitution, applicable laws, regulations, and policies, and the FBI's Core Values.

"Whether you're the corporate victim of a massive data breach or your personal life's been turned upside down by fraud, we're here for you." *— FBI Director Wray*

Our Mission Space

Unique Authorities

The FBI uses criminal and counterintelligence authorities to combat cyber criminals and foreign actors who use global infrastructure to compromise US networks.

LEADING CYBER THREAT RESPONSE

The FBI leads the U.S. Government's response to significant cyber incidents by investigating, collecting evidence and intelligence, identifying additional victims, and pursuing disruption opportunities.

USING LAW ENFORCEMENT AUTHORITIES TO HAVE BROAD IMPACT

Computer intrusion is a crime, whether it's done for personal profit or on behalf of a foreign government. The FBI uses legal process to obtain evidence that enables FBI and partner agencies to identify virtual infrastructure, shut down dark markets, expose adversaries' tools, and disrupt malicious activity.

ASSEMBLING THE DOMESTIC INTELLIGENCE PICTURE

The FBI is the nation's lead domestic intelligence agency. FBI intelligence on cyber threats and intrusions into US networks helps identify those responsible—the first step towards holding them accountable.

COORDINATING THROUGH THE NATIONAL CYBER INVESTIGATIVE JOINT TASK FORCE (NCIJTF)

Led by the FBI, the NCIJTF brings together more than 30 co-located agencies from the Intelligence Community and law enforcement in threat-focused mission centers to synchronize actions against cyber adversaries for maximum impact.

World-Class Capabilities

The FBI adapts to cyber threats by using innovative investigative techniques, developing cutting-edge analytic tools, and recruiting the next generation of the cyber workforce.

RECOVERING ASSETS TO ASSIST VICTIMS

The Internet Crime Complaint Center (IC3)'s Recovery Asset Team culls through thousands of public complaints to assist victims in recovering hundreds of millions of dollars lost to cyber crime.

MULTIDISCIPLINARY THREAT TEAMS

Squads of cyber-trained Special Agents, Intelligence Analysts, Computer Scientists, Data Analysts, and Digital Operations Specialists in FBI offices nationwide engage, assess, investigate, and respond to cyber threats in their communities.

RESPONDING TO INCIDENTS WITH THE CYBER ACTION TEAM

The FBI's Cyber Action Team is a rapid response technical investigative team distributed nationally to deploy and provide technical assistance to assist in the most complex intrusions and cyber incidents.

Enduring Partnerships

The FBI uses our unique role not only to pursue our own actions but also to enable our partners to defend networks, attribute malicious activity, sanction bad behavior, and take the fight to adversaries overseas.

TRUST-BASED RELATIONSHIPS

With 56 U.S. field offices, hundreds of satellite offices, and liaisons around the world, the FBI has global reach that extends to our communities. The FBI works alongside the public and private sectors in unique hubs built on long-term relationships to share and act on threat information.

ENABLING INDUSTRY ACTION

The FBI works with government, industry, and academia through nonprofit organizations like the National Cyber-Forensics and Training Alliance (NCFTA) and the National Defense Cyber Alliance (NDCA) to identify and disrupt cyber crime and national security threats.

SERVING AS THE INDISPENSABLE U.S. GOVERNMENT PARTNER

While law enforcement and counterintelligence actions are at the core of the FBI's mission, we can more significantly impact the threat when we sequence and coordinate our actions with domestic and international partners. Our information, access, and relationships are not only for FBI use; they are resources for others to leverage.

CROSS-BORDER PARTNERSHIPS TO ADDRESS A GLOBAL THREAT

FBI Cyber Assistant Legal Attachés in countries around the world work closely with international counterparts to share information, coordinate action, and seek justice for victims of cyber crime.