FEDERAL BUREAU OF INVESTIGATION

CYBER STRATEGY

FBI CYBER

DIVISION

Table of Contents

Executive Summary

This Strategy sets the course for FBI Cyber Division to defend the American people and the nation's critical infrastructure in cyberspace. It defines our priorities, objectives, and framework for countering malicious cyber activity directed at the United States. It guides how the FBI uses its unique combination of law enforcement, intelligence, and national security authorities to disrupt and deter cyber adversaries, support victims, build world-class capabilities, and drive coordinated action. This Strategy speaks to our partners across government, industry, and the international community, and to the adversaries who must understand they face determined pursuit and real consequences for targeting the United States.

The FBI's mission is to protect the American people and uphold the Constitution of the United States. The FBI is the only member of the Intelligence Community with broad authority to address both criminal and national security threats to the homeland, a distinction that is central to the cyber domain.

Under Presidential Policy Directive 41, the FBI leads the U.S. Government's threat response to significant cyber incidents by investigating, collecting evidence and intelligence, identifying others targeted by the same actor or campaign, and pursuing disruption opportunities. Under 18 U.S.C. § 1030, the Computer Fraud and Abuse Act, the FBI investigates the full range of computer intrusion offenses, from cybercriminal enterprises and ransomware actors to state-sponsored espionage and destructive cyber operations targeting U.S. networks and critical infrastructure. Under Executive Order 12333, the FBI conducts counterintelligence activities within the United States and coordinates those activities across the Intelligence Community, including activities to identify, exploit, disrupt, or protect against espionage, intelligence collection, and sabotage conducted for or on behalf of foreign powers, activities that today are increasingly carried out through cyber means. These authorities converge: the same intrusion may constitute a criminal violation, an intelligence collection operation, and a national security threat, and FBI Cyber is positioned to address all three simultaneously.

This Strategy operationalizes President Trump's Cyber Strategy for America where FBI authorities apply. FBI Cyber executes the President's directives by conducting court-authorized operations to shape adversary behavior, by empowering critical infrastructure owners and operators with timely threat intelligence to defend their networks, by protecting American innovators to sustain superiority in critical and emerging technologies, and by building the cyber workforce of tomorrow.

This Strategy also advances the FBI's Enterprise Strategy, under which FBI Cyber supports the mission to Defend the Homeland. In an era when adversaries no longer need to cross a physical border to reach the American people, this Strategy outlines how the FBI defends the homeland in cyberspace.

The cyber threat to the United States is escalating in both scale and sophistication. State-sponsored cyber actors collect intelligence, steal proprietary data, and pre-position access to disrupt the nation's critical infrastructure. Ransomware groups paralyze companies and trigger cascading effects across industries. These actors operate within an increasingly professionalized ecosystem of developers, affiliates, and service providers. AI-enabled tools and social engineering amplify these threats, compressing intrusion timelines and lowering barriers to entry for less sophisticated actors. From anywhere in the world, attackers can disrupt airports, schools, water systems, and financial institutions. The economic toll is immense: ransomware, operational outages, digital asset theft, and intellectual property theft cost the United States billions annually, with impacts extending far beyond financial loss.

Countering these threats, holding offenders accountable, and supporting the victims they target is what the FBI's Cyber Program exists to do. No single agency can counter this threat alone, and the FBI will lead where its authorities and capabilities are strongest, alongside its domestic, international, and industry partners.

FBI Cyber's mission is to impose cost on cyber adversaries through unique authorities, world-class capabilities, and enduring partnerships. Our vision is to protect the safety, security, and confidence of the American people in a digitally connected world.

To achieve this, the FBI Cyber Strategy is built on four pillars:

- **Pillar I**: Investigate, Disrupt, and Impose Cost on Cyber Adversaries
- **Pillar II**: Support Victims
- **Pillar III**: Increase Impact through Partnerships
- **Pillar IV**: Enhance FBI's Cyber Capabilities

The pages that follow explain how the FBI will deliver on each of these pillars.

Threat Picture

Today's cyber threat picture is shaped by two overlapping forces: disciplined, state-sponsored actors leveraging national power to penetrate U.S. networks and critical infrastructure for intelligence collection and disruption, and a mature, profit-driven criminal marketplace that industrializes ransomware, fraud, and cryptocurrency theft. Both sets of adversaries conduct attacks from permissive environments, use anonymizing technologies, and rapidly shift tactics to target everything from virtual currency exchanges to hospitals, power grids, and municipal networks.

These adversaries operate within ecosystems made up of the people and organizations conducting attacks, the infrastructure they rely on, the money that sustains their activity, and the tools they deploy. FBI Cyber uses an intelligence-driven strategy to disrupt multiple parts of those ecosystems at once, focusing on high-impact targets to create lasting results. FBI Cyber prioritizes legal actions that hold adversaries personally accountable: arrests, prosecutions, and extraditions wherever they are achievable.

But permissive jurisdictions often allow these adversaries to hide beyond the immediate reach of U.S. law enforcement. For that reason, FBI Cyber measures success against a broader set of outcomes that reduce harm and bring relief to victims. Disrupting infrastructure denies operational continuity; seizing funds degrades adversaries' ability to scale and pay collaborators; and dismantling tools forces them to rebuild their tradecraft. Each action makes it harder, costlier, and riskier to target U.S. victims while making clear that operating from a supposed safe haven does not mean operating without consequences.

Pillar I:
Investigate, Disrupt, and Impose Cost on Cyber Adversaries

This pillar establishes the FBI's enterprise framework for disrupting cyber adversaries and imposing cost on those who target the United States in cyberspace. Threat-specific strategies for each of the FBI's principal cyber adversaries will cascade from this framework into operational priorities and campaigns at the section and unit level.

FBI investigations and analysis identify the people and institutions, infrastructure, money flows, and tools that scaffold adversary activity. That insight drives operations to degrade campaigns before they cause further harm to the American people or U.S. critical infrastructure.

Objective 1.1: Investigate Cyber Intrusions

As the federal lead for threat response to significant cyber incidents, the FBI brings the full weight of its criminal and national security authorities to every investigation. To address the scope and pace of the threat, the FBI organizes its cyber workforce into Cyber Threat Teams that build deep subject-matter expertise across the full range of threats and respond to cyberattacks against U.S. networks and critical infrastructure. The FBI maintains the ability to deploy specialized cyber personnel within hours of a significant incident. In every engagement, our cyber personnel capture, analyze, and disseminate information to protect victims and plan further operations against the threat.

The FBI investigates and disrupts nation-state pre-positioning on U.S. critical infrastructure, working with the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and international partners to expose these campaigns.

The FBI defends U.S. elections from foreign cyber threats. The FBI investigates and disrupts foreign actors targeting election infrastructure, political campaigns, and election officials, sharing intelligence with federal, state, and local partners to protect those targeted.

What our personnel see when responding to a cyber incident may be the first indicator of a broader campaign. Each investigation generates intelligence that helps assemble the broader picture, where these actors reside, how they operate, what infrastructure and shell companies they hide behind, and how best to stop them. Victim reporting and the technical evidence that comes with it are essential to this process. They fuel both individual investigations and the development of disruption operations that extend well beyond any single case. The FBI also conducts proactive victim notifications, identifying compromised organizations through our intelligence collection and alerting them before adversaries can achieve their objectives.

FBI investigations also protect American innovation. Foreign intelligence services and state-linked criminal actors target U.S. defense contractors, advanced technology firms, and research institutions to steal intellectual property, advance their own technological capabilities, and undermine U.S. economic security. FBI Cyber will continue to investigate, disrupt, and hold accountable those engaged in cyber-enabled theft of American innovation.

Objective 1.2: Prioritize Joint, Sequenced Operations

FBI Cyber operates seamlessly across criminal and counterintelligence authorities, sequencing operations to apply whichever authority best disrupts the adversary at a given phase of a campaign. Joint, sequenced operations will be conducted at speed and at scale, in coordination with domestic, international, and industry partners to achieve maximum impact. Threat intelligence and access to adversary infrastructure, networks, and support ecosystems will identify the best operational opportunities. FBI Cyber employs a "best athlete" model in which the partner with the strongest authority, access, or capability leads the relevant phase of an operation, allowing multi-phased campaigns to apply sustained pressure on adversaries across jurisdictions and authorities. These operations dismantle adversary infrastructure, seize stolen cryptocurrency, disrupt nation-state intrusion campaigns, and take down pervasive ransomware variants.

The FBI's Virtual Assets Unit integrates investigative, technical, and analytic expertise to trace and seize cryptocurrency across a broad array of FBI cases, including ransomware payments, nation-state intrusions, and the proceeds of cyber-enabled fraud schemes.

The FBI will use the full range of its authorities and support cost imposition across every instrument of national power. In support of this approach, FBI Cyber will detect shifts in adversary intent and capability, disrupt their ability to profit or operate safely, expose their tradecraft and enablers, bring offenders to justice with domestic and international partners, and provide the evidence and intelligence that underpin sanctions, diplomatic action, and partner law enforcement actions.

Objective 1.3: Attribute Malicious Cyber Activity

Cyber adversaries invest heavily in anonymity, employing sophisticated tradecraft and operating through complex mixtures of government apparatuses, enabling companies, hackers-for-hire, and stolen or compromised infrastructure to obscure their identities. The FBI will continue to build and refine the intelligence necessary to attribute malicious cyber activity with confidence. Each investigation adds to a growing body of knowledge across the full spectrum of cyber threats, moving us closer to the evidentiary benchmarks required to identify, publicly expose, and hold accountable both the actors responsible and the enterprises that support them.

Attribution is strongest when FBI evidence is combined with Intelligence Community holdings, foreign partner intelligence, private-sector telemetry, and victim reporting. FBI Cyber will continue to integrate these inputs to accelerate attribution and enable the operational decisions that follow.

Pillar II:
Support Victims

When cyberattacks disrupt institutions, the consequences land on the people who depend on them. Whether the target is a business, critical infrastructure, or a government agency, the FBI responds with urgency and brings the investigative and operational capabilities the situation demands.

In every engagement, FBI Cyber scopes its collection strictly to the crime, gathering the evidence and intelligence required to support law enforcement actions and technical disruptions. The FBI uses the least intrusive investigative method feasible when collecting intelligence or evidence, protecting privacy and civil liberties without limiting the FBI's effectiveness against cyber adversaries.

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

Objective 2.1: Share Cyber Threat Intelligence with Urgency

Timely intelligence can stop an intrusion attempt before it becomes a breach. Shared rapidly, cyber threat intelligence allows network defenders to block known indicators, hunt for adversary tradecraft, and reduce the time threat actors remain in their networks. The FBI will pursue capabilities that enable urgent, automated sharing of cyber threat intelligence with critical infrastructure owners and trusted private-sector partners.

FBI Cyber will develop and deploy automated indicator-sharing mechanisms that narrow the gap from FBI threat detection to partner notification from days to hours, and from hours to minutes. Urgent sharing builds the closer public-private partnership the threat demands, giving victims and trusted partners information they can use to defend systems, contain intrusions, and recover operations.

Objective 2.2: Quickly Engage After Incidents

When cyber incidents occur, FBI Cyber will engage victims with the same urgency and operational rigor the FBI brings to investigations. The FBI pursues the actor, not the victim. When the FBI identifies the targeting of a device, network, or account, it will notify victims and targeted entities directly and provide intelligence and support to help them defend, contain, and recover. The FBI's nationwide presence through 56 field offices, and hundreds of resident agencies, complemented by more than 20 Cyber Assistant Law Enforcement Attachés stationed around the world, allows the FBI to respond wherever and whenever incidents demand it.

The FBI will also continue to identify and proactively notify organizations that have been compromised or are at imminent risk, often reaching them before they know there is a problem. The FBI will continue to invest in these relationships in advance, so when it has actionable threat intelligence to share, it will know the right points of contact. Early engagement protects victims, preserves evidence and investigative leads, and enables disruption of the actors responsible.

Objective 2.3: Deliver Specialized Capabilities to Victims

FBI Cyber maintains specialized teams and programs that reinforce field office response when victim environments demand expertise beyond standard cyber incident response. These capabilities deploy where they can have the greatest impact, complementing the field cyber workforce that leads day-to-day investigations and operations.

Critical infrastructure is a priority for FBI Cyber given the consequences of cyberattacks against the systems that underpin national security and the everyday services Americans rely on. To strengthen the FBI's response to victims operating critical infrastructure, FBI Cyber is expanding its Industrial Control Systems (ICS) Coordinator program to designate dedicated personnel in every field office. ICS Coordinators build operational technology expertise to support victim engagement in environments where information technology, operational technology, and physical processes intersect, and where standard incident response approaches do not always apply.

The Recovery Asset Team, part of the FBI's Internet Crime Complaint Center (IC3), works directly with financial institutions to freeze fraudulent transfers, helping return hundreds of millions of dollars to victims annually.

The Cyber Action Team deploys specialized personnel to respond to major cyber threats and attacks against critical services, drawing on special agents, computer scientists, intelligence analysts, and information technology specialists from across the FBI enterprise.

Objective 2.4: Facilitate Reporting of Cyber Incidents

Early reporting gives the FBI the evidence, indicators, and financial details needed to advance investigations, notify other victims, and move against the actors responsible. FBI Cyber will maintain reliable channels of communication between the FBI and those it protects. IC3 provides the American public a dependable mechanism to report suspected criminal cyber activity. The FBI analyzes and disseminates information received through IC3 for investigative and intelligence purposes and for public awareness. FBI Cyber will continue to enhance IC3's tools and technology to accelerate the processing of complaint data and strengthen its value to investigations and partnerships.

All FBI field offices will prioritize building direct relationships with local businesses and organizations to ensure open channels for swift reporting of cyber incidents.

Pillar III:
Increase Impact Through Partnerships

Cyber investigations depend on evidence, telemetry, infrastructure access, foreign legal process, technical expertise, and victim reporting that no single organization holds. This pillar reflects FBI Cyber's commitment to expand and deepen relationships throughout government, with international allies, with state, local, tribal, and territorial partners, and across the private sector. Each partnership extends our reach, scales our capabilities, and increases our impact.

FBI Cyber builds enduring relationships across the U.S. Government, foreign governments, and established industry programs. Partner selection follows operational need within appropriate legal, ethical, and security baselines, and operational results often depend on the partner who holds the specific evidence, infrastructure access, or authority a given disruption requires.

The private sector holds first-hand visibility into adversary activity, and private entities look to the FBI for key insights to help prevent adversary actions on their networks and for actionable tactics, techniques, and procedures when an incident has occurred. Behind the FBI's most significant cyber operations are industry partners whose intelligence, technical expertise, or operational coordination made the outcome possible. The FBI engages industry as an operational partner in this fight.

Objective 3.1: Share Actionable Intelligence

The FBI will turn intelligence into action. FBI Cyber will produce and rapidly disseminate timely intelligence that drives operations, strengthens defenses, and sharpens decision-making. Our analysts will assess tactical developments and strategic trends across every area of responsibility, connect actors and motives across cyber intrusions, and expose emerging threats before they take hold. Every intelligence product will be crafted to enable joint action, direct resources where they matter most, and give partners a clearer view of the threat.

The FBI will deliver clear, authoritative intelligence to the National Security Council, the Office of the National Cyber Director, policymakers, and other government leaders through official internal and external channels. These leaders will have the intelligence they need to make decisions that defend the nation. FBI Cyber will also move threat information rapidly to network defenders. Joint Cybersecurity Advisories, produced with Intelligence Community partners, will help organizations affected by intrusions respond decisively and enable many more to harden their networks before adversaries strike.

Objective 3.2: Strategically Partner Across U.S. Government and with Allies

FBI Cyber will coordinate closely with U.S. Government partners, including the Office of the National Cyber Director and the National Security Council. Through the FBI-led National Cyber Investigative Joint Task Force (NCIJTF), the FBI integrates the unique capabilities of more than 30 member agencies, combines data and tools, coordinates and deconflicts operations, and shares analytical results across the cyber community. NCIJTF serves as a central integration point for investigative and intelligence activity against the most consequential cyber threats facing the nation.

The Joint Ransomware Task Force, co-chaired by the FBI and CISA, brings together federal intelligence analysis to strengthen coordinated action against ransomware operators, the infrastructure they use, and the affiliates and service providers that make up the broader ransomware ecosystem.

FBI Cyber will also work alongside state, local, tribal, and territorial law enforcement and government partners. Field offices coordinate incident response, victim engagement, and information sharing with agencies often on the front lines of protecting critical services and affected communities.

Internationally, FBI Cyber sustains operational cooperation through Five Eyes cyber engagement, the Cyber 9 coalition, Europol, and bilateral relationships with allied cyber services.

Because cyber threats cross borders, the FBI must maintain global reach. Cyber Assistant Law Enforcement Attachés stationed in U.S. embassies build coalitions with allies against cyber adversaries. The FBI will continue to strategically place and support these Cyber ALATs where they can best address the shifting cyber threat.

Objective 3.3: Join Forces with the Private Sector

Field offices in every region of the country will forge direct relationships with industry partners, ensuring open channels of communication and trusted points of contact before crisis hits. A steady, two-way exchange of information between the FBI and the private sector is essential to detecting adversary activity earlier, notifying victims faster, and disrupting infrastructure before campaigns can scale.

FBI Cyber will continue to strengthen private-sector collaboration through several long-standing programs. InfraGard connects critical infrastructure owners and operators with the FBI to share education, networking, and information on security threats and risks. The National Cyber-Forensics and Training Alliance (NCFTA) is a nonprofit corporation that provides a neutral, trusted environment in which industry, academia, and law enforcement share confidential information to identify, mitigate, and disrupt cybercriminal threats globally. The National Defense Cyber Alliance (NDCA), formed in coordination with the FBI, serves as a focal point for the coordination, integration, and sharing of cyber threat intelligence between cleared defense contractors and the U.S. Government, helping to defend the defense industrial base and protect American innovation.

FBI Cyber will also expand executive engagement through three programs. CISO Academy brings chief information security officers from across the country to FBI Headquarters to engage with senior FBI leaders and subject-matter experts. Cyber Executive Summits convene regional industry leaders through FBI field offices to align priorities and strengthen incident-response readiness. The Leadership in Cyber (LinCY) program builds trusted relationships between FBI Cyber leaders and senior counterparts across industry, U.S. government agencies, and international cyber law enforcement organizations, enabling coordinated action during major incidents. Together, these programs establish the executive-level trust that enables fast, coordinated action when crises arise.

Pillar IV:
Enhance FBI's Cyber Capabilities

Cyber investigations demand personnel who combine technical expertise with investigative judgment, intelligence acumen, and the ability to extract leads from vast and complex datasets. Recruiting, developing, and retaining this cadre is foundational to every other pillar of this Strategy.

Cyber adversaries are increasingly sophisticated and well-resourced, and the pace of technological change continues to compress the time between threat and impact. This pillar establishes FBI Cyber's commitment to build and sustain the workforce, expertise, and technology required to meet the threat at the speed and scale the mission demands.

Objective 4.1: Recruit and Retain Top Cyber Talent

The FBI will compete for and retain the best cyber talent in the nation. FBI Cyber requires special agents, intelligence analysts, computer scientists, data scientists, malware analysts, cryptocurrency specialists, technical operators, and field cyber leaders, and will prioritize hiring, development, and retention across these roles to ensure the workforce is sized, skilled, and structured to meet evolving mission requirements. FBI Cyber will also pursue appropriate recruitment, exchange, and training partnerships with academia, industry, and other government and military organizations to draw from the broadest possible talent base.

Through the Field Cyber Resources initiative, FBI Cyber establishes a baseline for field office cyber teams and distributes cyber talent to meet investigative and operational needs across the country. The initiative provides targeted resources required for cyber investigations and operations.

The FBI's people are its decisive advantage, and the FBI will invest in them accordingly.

Objective 4.2: Develop Our Cyber Expertise

The FBI will cultivate the leaders and technical experts required to operate in a rapidly evolving threat environment. FBI cyber leadership at headquarters and in field offices must be equipped to lead teams, advance the FBI Cyber Strategy, and represent the FBI in engagements with domestic, international, and industry partners. FBI Cyber will provide training, mentorship, and professional development opportunities that build subject-matter expertise, strengthen ethical leadership, and prepare emerging leaders for greater responsibility.

The FBI's Cyber Education and Training Unit (CETU) develops and delivers the technical and operational training that builds proficiency across the cyber workforce, blending classroom instruction

with vendor training, technical certifications, and hands-on scenarios that prepare personnel for victim engagement, evidence collection, intrusion analysis, and operational execution. CETU will equip FBI Cyber personnel to operate at the pace and complexity of the threat.

Objective 4.3: Implement New Technical Tools and Techniques

The FBI will continuously improve and upgrade the technical capabilities required to investigate, attribute, and disrupt cyber adversaries. Where capabilities exist, the FBI will adopt and refine them. Where they do not, the FBI will develop or acquire them.

FBI Cyber will outfit its personnel with the hardware, software, and analytic platforms needed to sift through the highly complex and voluminous datasets unique to FBI authorities, where case-breaking insight often resides. The FBI will continue to develop its Computer Network Operations (CNO) program, providing investigative teams with the court-authorized or otherwise lawfully authorized technical operations tools to remotely collect, conduct surveillance, and disrupt the activities of nation-state and cybercriminal actors when traditional investigative techniques will not achieve the required outcome. The CNO program is supported by reverse engineering, intrusion analysis, and both in-house and open-source tools and platforms. Enhanced threat detection and hunt capabilities, developed and deployed in coordination with Intelligence Community, law enforcement, and private-sector partners, extend FBI Cyber's reach against adversaries operating on U.S. networks and abroad.

The FBI is also preparing its evidentiary and tradecraft systems for the post-quantum cryptographic transition, ensuring that long-running prosecutions and sensitive collection remain durable against adversaries who themselves move to quantum-resistant tooling.

Objective 4.4: Adopt Artificial Intelligence to Scale Operations

Cyber adversaries are using artificial intelligence to accelerate attacks, evade detection, and scale campaigns. The FBI will use AI-enabled tools where they improve speed, scale, accuracy, and operational decision-making under FBI authorities. FBI Cyber will deploy AI-enabled tools to triage large datasets, surface relationships, accelerate malware analysis, prioritize victim notifications, map adversary infrastructure, support attribution, and identify patterns that no human analyst could process at the required pace. Consistent with President Trump's Cyber Strategy for America, FBI Cyber will rapidly adopt agentic AI in ways that securely scale defense and disruption, and will implement AI-enabled tools to detect, divert, and deceive threat actors where operationally appropriate.

This capability directly supports the FBI's mission to impose cost on cyber adversaries. AI-enabled tools will help triage, correlate, prioritize, and accelerate work that remains under human review and legal controls. The FBI will integrate artificial intelligence responsibly, with appropriate safeguards for civil liberties, accuracy, and operational security, and in coordination with the Intelligence Community, CISA, and private-sector innovators. AI adoption is central to how FBI Cyber will impose cost at scale.

Conclusion

With this Strategy as our roadmap, the FBI will impose cost on cyber actors who target the United States through decisive action, rapid victim support, integrated partnerships, and continuous investment in tools and capabilities. FBI Cyber will disrupt adversaries before they can act, expose them when they do, and hold them accountable wherever they hide. These efforts will prioritize support for victims in both recovery and defense and will strengthen the partnerships that make collective action possible. The FBI will bring the full weight of its authorities, capabilities, and partnerships to bear in defending the homeland and securing the digital future of the American people.

FBICYBER

DIVISION