

U.S. DEPARTMENT OF JUSTICE
FY 2025 Budget Request



Keeping Our Country Safe:
**Protect National Security, Fight Cybercrime, and
 Enhance Cybersecurity**

Component/Initiative	Positions	Agents/ Attorneys	\$000s
PROTECT NATIONAL SECURITY			
FEDERAL PROGRAMS			
Federal Bureau of Investigation (FBI)			
Counterintelligence	44	14	\$17,792
Restoration of 2023 National Security and Law Enforcement Personnel	270	65	\$85,363
Subtotal, FBI	314	79	\$103,155
Subtotal, Federal Programs	314	79	\$103,155
GRANTS			
Office of Justice Programs (OJP)*			
<i>Research on Domestic Radicalization</i>	0	0	\$7,500
Subtotal, OJP	0	0	\$7,500
Subtotal, Grants	0	0	\$7,500
Subtotal, Protect National Security	314	79	\$110,655
FIGHT CYBERCRIME			
FEDERAL PROGRAMS			
Federal Bureau of Investigation (FBI)			
Cyber	12	4	\$7,000
Subtotal, FBI	12	4	\$7,000
National Security Division (NSD)			
Countering National Security Cyber Threat	22	20	\$5,000
Subtotal, NSD	22	20	\$5,000
Subtotal, Federal Programs	34	24	\$12,000

Component/Initiative	Positions	Agents/ Attorneys	\$000s
GRANTS			
Office of Justice Programs (OJP)*			
<i>Economic, High-Tech, White Collar Cybercrime Prevention</i>	0	0	\$10,000
Subtotal, OJP	0	0	\$10,000
Office on Violence Against Women (OVW)			
Local Law Enforcement Grants for Enforcement of Cybercrimes Against Individuals	0	0	\$10,000
National Resource Center on Cybercrime Against Individuals	0	0	4,000
Subtotal, OVW	0	0	\$14,000
Subtotal, Grants	0	0	\$24,000
Subtotal, Fight Cybercrime	34	24	\$36,000
ENHANCE CYBERSECURITY			
Justice Information Sharing Technology (JIST)			
Cybersecurity Posture Enhancements	6	0	\$51,540
Subtotal, JIST	6	0	\$51,540
Subtotal, Enhance Cybersecurity	6	0	\$51,540
Total Program Enhancements	354	103	\$198,195

* OJP Program is base funding only and is not included in narrative below.

A core tenet of the Department's strategic goal to Keep Our Country Safe is the commitment to protect the American people from a multitude of serious and evolving threats. The Nation faces threats from actors including organized criminal networks, nation-state adversaries, domestic extremists, international terrorists, and common criminals. The Department of Justice must remain vigilant and be adequately resourced to combat and investigate these threats, ensuring that those who choose to break our laws face criminal enforcement and consequences.

The Department actively investigates, disrupts, and prosecutes threats to America's national and economic security. This includes not only traditional espionage efforts but also foreign influence operations, economic espionage, and attacks on critical infrastructure. In addition, protecting the Homeland against threats from terrorists, both from abroad and within, remains a critical priority for the Department. In these areas, continued and new resources are needed to match the increasing risks that face the country.

In today's national security landscape, one of the most significant threats is that arising from cybercrimes. As the President's National Cybersecurity Strategy describes, "Malicious cyber activity has evolved from nuisance defacement, to espionage and intellectual property theft, to damaging attacks against critical infrastructure, to ransomware attacks and cyber-enabled influence campaigns designed to undermine public trust in the foundation of our democracy." To counter cyber threats, the Department requires additional resources to enforce cybercrime laws and to assist victims in how to respond to cyber-attacks.


Additionally, the Department has an immediate need to strengthen its own cybersecurity defenses and protect its infrastructure from adversaries who seek to do us harm. It is imperative to continue implementation of a zero-trust architecture (ZTA) for both unclassified and national security systems, while further progressing towards the Department and Administration's goals of achieving comprehensive cybersecurity event logging across components. While the Department has made substantial progress, more work and resources are required to achieve a cybersecurity posture that is maximally integrated and resilient.

The Department's FY 2025 request to protect national security, fight cybercrime, and enhance cybersecurity totals \$198.2 million and 354 positions (76 agents and 27 attorneys). Of this amount, \$103.2 million and 314 positions (72 agents and 7 attorneys) will address national security needs of the Federal Bureau of Investigation (FBI) and provide continued funding for an Office of Justice Programs (OJP) grant to research domestic radicalization. An additional \$36.0 million and 34 positions (4 agents and 20 attorneys) will expand and enhance cybercrime efforts across the FBI and the National Security Division (NSD) and through grants provided by the OJP and Office on Violence Against Women (OVW). Finally, this request will strengthen the Department's cybersecurity by providing an additional \$51.5 million and six positions for the Justice Information Sharing Technology (JIST) account, which supports Departmental enterprise investments in Information Technology modernization and critical cybersecurity requirements.

Resources to Protect National Security

FEDERAL PROGRAMS

Federal Bureau of Investigation (FBI): \$103.2 million

 314 positions
(72 agents,
7 attorneys)

→ Counterintelligence: \$17.8 million

44 positions (12 agents,
2 attorneys)

→ Restoration of 2023 National Security and Law Enforcement Personnel: \$85.4 million

270 positions (60 agents,
5 attorneys)

Counterintelligence: \$17.8 million and 44 positions (12 agents, 2 attorneys)

The FBI remains the lead agency for exposing, preventing, and investigating intelligence activities in the U.S. As the Department's largest member of the Intelligence Community (IC), the FBI plays a critical role in uncovering threats to national security and penetrating national and transnational networks that have a desire and capability to enact harm on the American public. The FBI's counterintelligence work encompasses a broad mission that seeks to protect the secrets of the IC, the Nation's valuable assets, advanced technologies, and critical infrastructure. The goals of FBI's counterintelligence mission also include the FBI's efforts to counter the activities of foreign spies and prevent weapons of mass destruction and sensitive information from falling into the wrong hands. **Current services and additional details are classified.**

Restoration of 2023 National Security and Law Enforcement Personnel: \$85.4 million and 270 positions (60 agents, 5 attorneys)

The Department expects that the FBI will lose funding for 900 positions (200 agents) under an FY 2024 Annualized Continuing Resolution (ACR). However, this enhancement, plus a \$149.0 million base adjustment required in FY 2025, will allow the FBI to restore key positions that are crucial to achieving the FBI's dual national security and law enforcement mission. The FBI's nearly 35,000-person workforce, including Special Agents and support professionals such as intelligence analysts, language specialists, scientists, and information technology specialists, enables the Bureau to fulfill its mission of protecting the American people and upholding the Constitution. The FBI will add these positions across multiple headquarters programs, including Criminal Justice Information Services (CJIS), which equips partners with necessary information to protect the United States, while also preserving civil liberties. In addition, Counterterrorism, which remains among the FBI's top priorities, facilitates the FBI's response to increased threats to the Homeland, both from international and domestic sources. The requested resources will also support Operational Technology and Laboratory programs, which provide significant assistance to State and local agencies, particularly in digital forensics for child exploitation cases, internet fraud, and financial crimes. Additionally, they create innovative investigative tools and provide critical support such as laboratory examinations for both the FBI and Federal partner operations. This increase in resources will also sustain the FBI's programs for Criminal Investigations, Intelligence Production, International Operations, Security, and other critical functions, designed to effectively counter the threats facing the Nation. **There are no current services.**

Resources to Fight Cybercrime

FEDERAL PROGRAMS

Federal Bureau of Investigation (FBI): \$7.0 million

 12 positions
(4 agents)

Cyber: Total: \$7.0 million and 12 positions (4 agents)

As the lead Federal agency for investigating cyber-attacks and intrusions, the FBI collects and shares intelligence and engages with victims while working diligently to unmask those committing malicious cyber activities, regardless of their location. Malicious cyber activity threatens the public's safety and America's national and economic security. The FBI's cyber strategy is to impose risks and consequences on cyber adversaries, aiming to change the behavior of criminals and nation-states who believe they can compromise United States networks, steal financial and intellectual property, and endanger critical infrastructure. The FBI capitalizes on its use of a unique mix of authorities, capabilities, and partnerships to impose consequences against cyber adversaries. The requested resources will increase the FBI's capacity for unilateral, joint, and enabled operations with other Federal, State, local, and international partners. The request focuses on the development of Victim Engagement and Incident Response. **Current services and additional details are classified.**

National Security Division (NSD): \$5.0 million

 22 positions
(20 attorneys)

Countering National Security Cyber Threats: Total \$5.0 million and 22 positions (20 attorneys)

This request will support the NSD's efforts in combating national security cyber-based attacks, which remain some of the most significant challenges faced by the Nation. Highly technical cyber threats require time-sensitive and complex investigative and prosecutorial work. These additional resources will help the NSD effectively confront the growing threat head on and address the significant increase in workload associated with cyber investigations, prosecutions, and disruptions operations crucial to national security challenges. **Current services are \$3.3 million and 11 positions (10 attorneys).**

GRANTS

Office on Violence Against Women (OVW): Total \$14.0 million (+\$14.0 million)

→ Local Law Enforcement Grants for Enforcement of Cybercrimes Against Individuals: Total \$10.0 million (+\$10.0 million)

Local Law Enforcement Grants for Enforcement of Cybercrimes Against Individuals: Total \$10.0 million (+\$10.0 million)

This funding supports a new program to advance the Administration's priority of addressing the serious issue of online harassment, stalking, and abuse. The White House's Gender Policy Council, the Domestic Policy Council, and the National Security Council convened an Interagency Policy Committee on Online Harassment, Stalking, and Abuse that has focused on sexual exploitation and abuse of children online, "revenge porn," the use of online platforms and social media sites for trafficking individuals, cyberstalking, and the use of the internet for domestic terrorism or extremism. Funding under this grant program can be used to train law enforcement personnel

to identify and protect victims of cybercrimes, use Federal, State, Tribal, local and other resources to assist victims, identify and investigate these crimes, enforce laws that prohibit these crimes, and utilize technology to assist in investigation and enforcement actions. The funding also can be used to train prosecutors, judges, judicial personnel, and emergency dispatch personnel to respond to these crimes; support assistance to State, Tribal, or local law enforcement agencies to enforce laws that prohibit cybercrimes against individuals; educate the public about cybercrimes against individuals; fund victim assistants in law enforcement agencies; establish task forces to conduct investigations and prosecutions; and acquire equipment necessary to conduct forensic evidence analysis. In the FY 2023 Enacted Budget, this program was funded at \$7.0 million through a set-aside in the Office of Justice Programs' Edward Byrne Memorial Justice Assistance Grant Program. **There are no current services.**

→ National Resource Center on Cybercrimes Against Individuals: Total \$4.0 million (+\$4.0 million)

National Resource Center on Cybercrimes Against Individuals: Total \$4.0 million (+\$4.0 million)

Like the Local Law Enforcement Grants for Enforcement of Cybercrimes Against Individuals, this funding supports a new program that advances the Administration's priority of addressing the serious issue of addressing online harassment, stalking, and abuse. Authorized in the Violence Against Women Act 2022. This national resource center will provide essential technical assistance and training resources focused on cybercrimes against individuals for Federal, State, and local government agencies, community-based organizations, and other professionals and interested parties. These resources will include the collection, preparation, analysis, and dissemination of information and statistics on these crimes and research on the causes and effects of these crimes, as well as model solutions to prevent and deter such crimes and enforce relevant criminal laws. The OVW will collaborate with the Office for Victims of Crime to implement this initiative. **There are no current services.**

Resources to Enhance Cybersecurity

Justice Information Sharing Technology (JIST): \$51.5 million

 6 positions

Cybersecurity Posture Enhancements

The Department requests additional resources for the Justice Management Division's Office of the Chief Information Officer to continue its essential, time-sensitive cybersecurity investments Department-wide. This enhancement provides funding to support the Department's efforts to comply with Executive Order 14028, *Improving the Nation's Cybersecurity*, as well as OMB memoranda M-21-30, M-21-31, M-22-01, and M-22-09. The resources will support three crucial investment areas outlined in those directives: \$31.4 million and four positions for Cyber Event Logging, \$6.4 million and two positions in support of ZTA for unclassified systems,

and \$13.7 million in support of ZTA for national security systems. The additional positions will plan the execution, deployment, and operation of the technology to make sure these capabilities are developed and integrated throughout the Department. This request builds on prior resources in the JIST account that have made substantial progress toward Event Logging and ZTA targets but reiterates the need expressed in the FY 2024 request for additional funding to make further progress in complying with the directives, insulating the Department's assets from malicious breaches and minimizing the risk of adverse effects to the Department's work in service of the public. **Current services are \$112.9 million and 30 positions.**