



**U.S. Department of Justice
FY 2024 Budget Request**

**Keeping Our Country Safe:
Enhance Cybersecurity and Combat Cybercrime
(Amount in \$000s)**

Component/Initiative	Positions	Agents/ Attorneys	\$000s
ENHANCE CYBERSECURITY			
Federal Bureau of Investigation (FBI)			
Cybersecurity	4	1	\$27,219
Subtotal, FBI	4	1	\$27,219
Justice Information Sharing Technology (JIST)			
Cybersecurity Posture Enhancements	6	0	\$55,057
Subtotal, JIST	6	0	\$55,057
National Security Division (NSD)			
Crisis Management System	0	0	\$3,597
National Security Memorandum-8 Security Enhancements	0	0	761
Subtotal, NSD	0	0	\$4,358
U.S. Attorneys (USA)			
Cybersecurity Modernization	4	0	\$10,700
Subtotal, USA	4	0	\$10,700
Subtotal, Cybersecurity	14	1	\$97,334
FIGHT CYBERCRIME			
FEDERAL PROGRAMS			
Criminal Division (CRM)			
Prosecuting Cybercrime and Responding to Criminal Use of Cryptocurrency	26	14	\$4,000
Subtotal, CRM	26	14	\$4,000
Federal Bureau of Investigation (FBI)			
Cyber	192	31	\$63,390
Subtotal, FBI	192	31	\$63,390
National Security Division (NSD)			
Counterintelligence and Export Control, Including Countering Cyber Threats	5	4	\$1,002
Subtotal, NSD	5	4	\$1,002
Subtotal, Federal Programs	223	49	\$68,392

**U.S. Department of Justice
FY 2024 Budget Request**

GRANTS			
Office of Justice Programs (OJP)			
Bureau of Justice Statistics – Better Cybercrime Metrics Act (non-add)	0	0	[\$2,000]
Subtotal, OJP*	0	0	\$0
Office on Violence Against Women (OVW)			
Local Law Enforcement Grants for Enforcement of Cybercrimes (new)	0	0	\$10,000
National Cybercrime Resource Center (new)	0	0	4,000
Subtotal, OVW	0	0	\$14,000
Subtotal, Grants	0	0	\$14,000
Subtotal, Fight Cybercrime	223	49	\$82,392
Total Program Enhancements	237	50	\$179,726

**The total amount for this OJP increase is included in the Civil Rights Fact Sheet.*

The Nation faces an ever-increasing number and variety of cyber threats – whether from nation states, terrorists, or common criminals. Keeping our country safe means combating these threats, and the Department requires significant new resources to do so. At the same time, the Department has an immediate need to harden its own cybersecurity defenses. Executive Order 14028, *Improving the Nation’s Cybersecurity* (May 12, 2021), mandates that Federal agencies implement important cybersecurity improvements, including adoption of a Zero Trust Architecture (ZTA). Additional investments in both counter-cybercrime and cybersecurity resources are necessary to identify, deter, protect against, detect, and respond to cyber threat actors and to protect the Department’s own systems against them.

The Department’s FY 2024 cyber enhancement request, totaling \$179.7 million in program enhancements, supports the Department’s efforts to respond to cybersecurity and cyber threats. Of this amount, \$97.3 million in additional funds will strengthen the Department’s cybersecurity through investment in the Federal Bureau of Investigation (FBI), the Justice Information Sharing Technology (JIST) account, the National Security Division (NSD), and the U.S. Attorneys (USA). An additional \$82.4 million will enhance efforts to investigate, prosecute, and fight cybercrime at the Federal, State, and local levels.

U.S. Department of Justice FY 2024 Budget Request

RESOURCES TO ENHANCE CYBERSECURITY

Federal Bureau of Investigation (FBI): \$27.2 million and four positions (one agent) Cybersecurity

Several highly publicized breaches of systems and data have exposed cybersecurity vulnerabilities in government networks and information systems, including those of the FBI. Over the past two years, the FBI has seen an increase in cybersecurity incidents and has discovered aging software and hardware components within critical segments of its Information Technology infrastructure. The requested resources will allow the FBI to begin to adopt a ZTA to harden its networks, access controls, and system security. A ZTA addresses the shortcomings of past cybersecurity approaches to secure a modernized, cloud-based, and increasingly mobile information infrastructure being continuously targeted by adversaries. The FBI must centrally manage access to FBI resources—data, systems, devices, and networks—to protect sensitive information and national security operations from cybersecurity threats. *Current services are \$122.9 million and 155 positions (five agents).*

Justice Information Sharing Technology (JIST): \$55.1 million and six positions Cybersecurity Posture Enhancements

This request provides funding for implementation of cybersecurity posture improvements including ZTA for unclassified systems (\$11.0 million and three positions), ZTA for National Security Systems (\$13.7 million and zero positions), and Cybersecurity Event Logging (\$30.4 million and three positions). These resources are requested in response to:

Executive Order 14028, OMB memorandum M-21-30, *Protecting Critical Software Through Enhanced Security Measures*,

OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*,

OMB M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*,

OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*,
and

National Security Memorandum (NSM)-8, *National Security Memorandum: Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*.

This funding will also address other opportunities to improve the Department's cybersecurity defense and resilience. 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. *Current services are \$113.1 million and 20 positions.*

U.S. Department of Justice FY 2024 Budget Request

National Security Division (NSD): \$4.4 million and zero positions

Crisis Management System: \$3.6 million and zero positions

This request will support the implementation of the Crisis Management System (CMS) secure telecommunications system, including the applicable hardware, and will allow the NSD to conduct secure telecommunications with the White House and Intelligence Community (IC) entities. The NSD currently uses a CMS overseen by the White House Communications Agency, which has had a substantial increase in the annual operation and maintenance costs compared to prior years. Failure to implement new hardware will result in an unacceptable gap in secure telecommunications for the Division and will severely impact the NSD's ability to connect efficiently and effectively with the White House and IC. *There are no current services for this initiative.*

NSM-8 Security Enhancements: \$761,000 and zero positions

This request will support the implementation of hardware and software required by NSM-8 on Improving the Cybersecurity of National Security, Department of Defense, and IC Systems, in support of Executive Order 14028. This will enhance the security of NSD classified enclaves, allowing for additional security layers and protection within those enclaves. *There are no current services for this initiative.*

U.S. Attorneys (USA): \$10.7 million and four positions (zero attorneys)

Cybersecurity Modernization

Funding will be used to address key National Institute of Standards and Technology cybersecurity framework functions and will support adoption of security practices that lead to a ZTA. With the rising sophistication of advanced cyber and insider threat actors and corresponding increases in the velocity and ferocity of attacks, the U.S. Attorneys' Offices need enhanced cybersecurity capabilities to counter these threats and ensure continuity of the USA's litigation operations with a commensurate level of recurring investment in technology and contractual support. *Current services are \$71.8 million and 237 positions (188 attorneys).*

RESOURCES TO COMBAT CYBERCRIME

Criminal Division (CRM): \$4.0 million and 26 positions (14 attorneys)

Prosecuting Cybercrime and Responding to Criminal Use of Cryptocurrency

The request includes resources for the Computer Crime and Intellectual Property Section (CCIPS) and the Money Laundering and Asset Recovery Section (MLARS) to further the Attorney General's priority of enhancing cybersecurity and fighting cybercrime. MLARS and CCIPS together have led the Department's efforts to assess and respond, through criminal enforcement as well as proposals for legal and regulatory reform, to the explosive growth in the use of cryptocurrencies by criminal actors of all stripes, including the most significant ransomware actors. *Current services are \$22.2 million and 77 positions (56 attorneys).*

U.S. Department of Justice FY 2024 Budget Request

Federal Bureau of Investigation (FBI): \$63.4 million and 192 positions (31 agents)

Cyber

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 the following critical areas: cyber threat identification, analysis, and attribution; and cyber workforce development. These resources will enhance the FBI's efforts regarding its Model Cyber Squads, Cyber Talent Initiative, Accelerated Cyber Training Program, Computer Network Operations, and Virtual Currency program. *Current services for this initiative are classified.*

National Security Division (NSD): \$1.0 million and five positions (four attorneys)

Counterintelligence and Export Control, Including Countering Cyber Threats

This request will support the NSD's counterintelligence and export control work, including national security cyber investigations and prosecutions and enforcement of the Foreign Agents Registration Act (FARA). Among the most significant challenges this Nation continues to face is the rapid expansion, evolution, and sophistication of cyber threats to national security. Highly technical cyber threats require time-intensive and complex investigative and prosecutorial work. These additional resources will help the NSD meet this growing threat head on and address the significant increase in workload related to cyber investigations, prosecutions, and disruption operations expected in FY 2024. In addition to these increasing litigation demands, the FARA Unit continues to see year to year increases in new registrants. The additional requested resources will allow the NSD to address increased workload demands related to FARA. *Current services for this program are \$17.1 million and 55 positions (42 attorneys).*

Office of Justice Programs (OJP): Total [\$2.0 million] (+\$2.0 million)

Better Cybercrime Metrics Act: Total [\$2.0 million] (+\$2.0 million)

The Better Cybercrime Metrics Act of 2022 requires the Bureau of Justice Statistics (BJS), in coordination with the Census Bureau, to include questions relating to cybercrime victimization in the National Crime Victimization Survey (NCVS). To comply with the statute, the BJS requests funds to research and test the most appropriate method to comply with the law while preserving the integrity of the NCVS, implement the methods that are selected, and analyze and report any data collected on cybercrime victimization. *This program is funded within the BJS, for which the total amount is included in the Civil Rights Fact Sheet.*

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

Local Law Enforcement Grants for Enforcement of Cybercrimes: 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, 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. In the National Strategy for Gender Equity and Equality, the Administration committed to convene a U.S. Government task force to further these efforts. *There are no current services for this initiative.*

U.S. Department of Justice FY 2024 Budget Request

National Cybercrime Resource Center: 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 much needed technical assistance and training resources 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 for this initiative.*