



**U.S. Department of Justice
FY 2023 Budget Request**

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

Component/Initiative	Positions	Agents/ Attorneys	Amount
ENHANCE CYBERSECURITY			
Drug Enforcement Administration (DEA)			
IT Infrastructure	0	0	\$3,000
Subtotal, DEA	0	0	\$3,000
Federal Bureau of Investigation (FBI)			
Tool Modernization	0	0	\$3,400
Centralized Logging	0	0	\$24,480
Blue and Red Teams	3	1	\$3,958
IT Asset Monitoring	6	0	\$3,068
Forensic Analysis	0	0	\$2,042
Subtotal, FBI	9	1	\$36,948
Justice Information Sharing Technology (JIST)			
Strengthening Cybersecurity	15	0	\$40,000
Supply Chain Risk Management	2	0	\$500
Subtotal, JIST	17	0	\$40,500
Subtotal, Cybersecurity	26	1	\$80,448
FIGHT CYBERCRIME			
FBI			
Cyber	137	39	\$51,975
Subtotal, FBI	137	39	\$51,975
National Security Division (NSD)			
Counterintelligence and Export Control, including Countering Cyber Threats	6	6	\$1,362
Subtotal, NSD	6	6	\$1,362
U.S. Attorneys (USA)			
Cyber Crime (Combat Cybercrime and Strengthen USA cyber security)	50	50	\$15,267
Subtotal, USA	50	50	\$15,267
Subtotal, Fight Cybercrime	193	95	\$68,604
Total Resources	219	96	\$149,052

The Department requires significant investments to continue combating the latest cyber threats to our security, economy, and way of life. Criminal enterprises conduct cyberattacks to defraud banks and corporations, as displayed in the May 2021 Colonial Pipeline ransomware attack. Spies, conducting malicious cyber activities, continually seek to steal critical defense and intelligence secrets and intellectual property. These threats pose serious challenges to our Nation's well-being.

U.S. Department of Justice FY 2023 Budget Request

The Department's FY 2023 cyber enhancement request, totaling \$149.1 million, supports the Department's efforts to respond to cyber threats by dedicating \$80.4 million in additional funds to strengthen the Department's information security infrastructure contained in the requests of both the Justice Information Sharing Technology (JIST) and the Federal Bureau of Investigation (FBI). An additional \$68.6 million within the request will support other efforts to fight cybercrime. These new investments will further protect the Department's systems from cyber threat actor intrusions and will help identify and bring to justice the perpetrators of cybercrimes. The 2023 request reiterates the full previous FY 2022 request to strengthen cyber investigative and cybersecurity capabilities.

RESOURCES TO ENHANCE CYBERSECURITY

Drug Enforcement Administration (DEA): \$3.0 million and 0 positions **IT Infrastructure**

Requested resources will address potential cybersecurity risks and improve the DEA's security capabilities. Funding will support the DEA's efforts to reduce response times across security operations, minimize system downtimes, and establish a proactive recovery plan with consistent strategies that can be deployed throughout the DEA enterprise. *Current services are \$238.3 million and 132 positions (2 agents).*

Federal Bureau of Investigation (FBI): \$36.9 million and 9 positions (1 agent) **Cybersecurity: \$36.9 million and 9 positions (1 special agent)**

The FBI's request will enhance its cybersecurity posture. FBI data, including national security data, is vulnerable to external cyber and insider threat attacks. Current tools are not capable of fully monitoring the numerous enterprise systems in place across the FBI and are not aligned with the ever-changing technological landscape, including the emergence of the cloud and the increase in mobile platforms. The FBI must invest in tools to enhance its cybersecurity posture to meet Federal mandates for a secure IT enterprise. This enhancement request features five specific investments to protect FBI data more effectively:

Tool Modernization: \$3.4 million and 0 positions

This request will provide for the deployment of industry-standard software tools and personnel to address a series of cybersecurity initiatives. This effort consists of additional contractors and Endpoint Detection and Response and Security Operations Center tool modernization. Implementing this capability supports the processing of a substantially larger amount of data being generated by the growing centralized logging capability.

Centralized Logging: \$24.5 million and 0 positions

As the volume and speed of information increases, the FBI must make major investments to protect its networks, systems, and data sets. Adversaries persistently attempt to infiltrate the FBI's networks and systems, threatening the integrity of investigations and prosecutions and undermining the capabilities of the Intelligence Community. The FBI requests funding both to maintain current and build out future advanced cybersecurity capabilities. These efforts will enable the FBI to better identify, respond to, and mitigate a wide range of sophisticated malicious cyber and insider threats.

U.S. Department of Justice FY 2023 Budget Request

Blue and Red Teams: \$4.0 million and 3 positions (1 agent)

This FBI request to expand the Advanced Security Assessment Team (Blue and Red Teams) will enable the FBI to continuously assess and enhance its security posture through threat-driven, cybersecurity technical operations based on adversarial tools, techniques, and procedures. The primary purpose of the two teams is to proactively assess the overall information security and cybersecurity management of FBI systems beyond vulnerability scans.

IT Asset Monitoring: \$3.1 million and 6 positions

This FBI request will address foundational cybersecurity monitoring capabilities for the FBI's IT infrastructure, as well as the needed personnel to monitor FBI assets effectively and efficiently for cyberattacks. It will also provide technologies for the FBI's cyber defenders to prevent and respond to attacks against the FBI's infrastructure. Specifically, the requested resources will be used to enhance monitoring of FBI IT assets and to deploy technologies to support increased visibility into the FBI's existing IT assets and emerging technologies, such as cloud and mobility platforms.

Forensic Analysis: \$2.0 million and 0 positions

This request will enhance the FBI incident response and digital forensics capabilities, allowing the FBI to better respond to compromises of Federal Government systems, process and analyze investigative data, and forensically analyze the FBI's cloud and mobile activity data. This request will also provide substantial improvements to the FBI's cybersecurity posture and agility. *Current services for the above FBI enhancements are \$87.1 million and 144 positions (3 agents).*

The FY 2023 request was built on the FY 2022 President's Budget investment of \$15.2 million which is still essential to our FY 2023 request.

Department of Justice/Justice Information Sharing Technology (JIST): \$40.5 million and 17 positions

Strengthen Cybersecurity: \$40.0 million and 15 positions

This JIST request of \$40.0 million and 15 positions will provide critical resources to continue enhancing the Department's cybersecurity-strengthening activities as originally requested in FY 2022. This request will provide continued remediation of the SolarWinds incident, while also addressing other opportunities to strengthen JIST/Department cybersecurity defense and resilience. The additional personnel will plan, implement, and deploy technology to ensure additional cybersecurity capabilities are integrated throughout the Department. In accordance with Executive Order 14028, the Department's Office of the Chief Information Officer (OCIO) will review and implement recommendations from three primary lines of effort: Deterrence, Disruption, and Accountability; Strengthening Our Defenses and Building Resilience; and Ensuring Our Workforce and Policies Reflect our Values and the Implications of Emerging Technologies.

Supply Chain Risk Management: \$500,000 and 2 positions

The JIST request of \$500,000 and 2 positions will focus specifically on continued work towards enhancing supply chain risk management while supplementing the \$40.0 million Strengthening Cybersecurity request. The OCIO will improve the Department's supply chain risk management with a focus on providing insight into the source and potential vulnerability of critical systems and technology. This request will also provide the

U.S. Department of Justice FY 2023 Budget Request

development of new capabilities to analyze the cyber-specific risks associated with critical software vendors and a plan to mitigate those threats. These efforts will enable JIST to provide additional capacity to conduct supply chain risk assessments; increase analytic capabilities; improve software security; and implement security requirements for critical software per Executive Order 14028 and Office of Management and Budget Memorandum M-21-30. *Current Services for the above JIST enhancements are \$87.3 million and 4 positions.*

The FY 2023 request was built on the FY 2022 President's Budget investment of \$78.8 million. The remaining \$75.0 million is still essential to our FY 2023 request.

RESOURCES TO FIGHT CYBERCRIME

Federal Bureau of Investigation (FBI): \$52.0 million and 137 positions (38 agents)

Cyber

The requested resources will strengthen the foundation needed for the FBI to remain the world's premier cyber investigative agency. These enhancements will better equip the FBI to work with allies and partners to impose risk and consequences on cyber adversaries through joint, sequenced operations. This request focuses on the development of three critical areas, including Cyber Threat Identification, Analysis, and Attribution; Cyber Threat Intelligence Platform; and Incident Response. *Details of this request and current services are classified.*

The FY 2023 request was built on the FY 2022 President's Budget investment of \$40.0 million, which is still essential to our FY 2023 request.

National Security Division (NSD): \$1.4 million and 6 positions (6 attorneys)

Counterintelligence and Export Control, including Countering Cyber Threats

This request will support the NSD's work related to countering cyber threats to our national security. Highly technical cyber threats require time-intensive and complex investigative and prosecutorial work. These investigations are novel; present difficulties of attribution; raise challenges associated with electronic evidence; and require balancing of prosecutorial and intelligence-related interests. These additional resources will help the NSD address the significant increase in workload related to cyber investigations, prosecutions, and disruption operations expected in FY 2023. *Current services are \$14.8 million and 49 positions (36 attorneys).*

U.S. Attorneys (USA): \$15.3 million and 50 positions (50 attorneys)

Cyber Crime (Combat Cybercrime and Strengthen USA Cybersecurity)

This request will support increased positions to pursue actors behind rising malicious activities such as illegal interception of data, compromises of network integrity, and infringement on intellectual property. This request will also provide essential training on cybercrime and digital evidence for all criminal prosecutors. In addition, this request seeks cybersecurity resources that will support information technology infrastructure, applications, and the defense of data necessary to ensure that the USAO community can achieve its litigation mission. *Current services are approximately \$64.2 million and 242 positions (193 attorneys).*

For additional information, please consult the FY 2023 Budget and Performance Summary.