U.S. Department of Justice
FY 2022 Budget Request

Augmenting Cyber Investigations and Cybersecurity
(Amount in $000s)

Component/Initiative	Positions	Agents/ Attorneys	Amount
CYBERSECURITY			
Federal Bureau of Investigation (FBI)			
Cybersecurity	22	0	$15,230
Subtotal, FBI	**22**	**0**	**$15,230**
Justice Information Sharing Technology (JIST)			
Cybersecurity/SolarWinds Incident Response	0	0	$78,786
Subtotal, JIST	**0**	**0**	**$78,786**
United States National Central Bureau (USNCB) INTERPOLWashington			
IT Modernization	0	0	$2,634
Subtotal, USNCB	**0**	**0**	**$2,634**
Subtotal, Cybersecurity	**22**	**0**	**$96,650**
CYBER INVESTIGATIONS			
FBI			
Cyber	155	52	$40,000
Subtotal, FBI	**155**	**52**	**$40,000**
Criminal Division (CRM)			
COVID-19 Related Fraud	4	4	$1,016
Subtotal, CRM	**4**	**4**	**$1,016**
Office of Justice Programs (OJP)			
High-tech, White Collar and InternetCrime Prevention	**0**	**0**	$13,000
Subtotal, OJP	**0**	**0**	**$13,000**
Subtotal, Cyber Investigations	**159**	**56**	**$54,016**
Total Program Enhancements	**181**	**56**	**$150,666**

National security remains the Department of Justice’s highest priority. Threats are constantly evolving, requiring additional investments to mitigate those threats in innovative ways. Organized crime syndicates use sophisticated cyberattacks as they seek to defraud banks and corporations, such as the May 2021 Colonial Pipeline ransomware attack, and spies seek to steal defense and intelligence secrets and intellectual property. Each threatens our Nation’s economy and security.

In December 2020, a Texas-based IT firm, Solar Winds, was reported as the immediate target of a complex andsophisticated cyberattack. Cybercriminals used routine computer updates as a Trojan horse to install malicious software targeting up to 18,000 Solar Winds customers, many of which are Federal agencies, to include parts of the Pentagon, the Department of Homeland Security, the State Department, the Department of Energy, the National Nuclear Security Administration, theDepartment of Justice, and the Treasury.

The FY 2022 Budget will support the Department in responding to those cyberattacks by dedicating $150.7 million in program enhancements to strengthen the Department's Information Security Infrastructure funded in the Justice Information Sharing Technology (JIST) appropriation, and the Federal Bureau of Investigation (FBI). These investments cover both Cybersecurity and the need to enhance components Cyber Investigation capabilities. The investments will help protect the Department's systems from cyber threat actor intrusions and identify the perpetrators of cyber crimes and ultimately bring them to justice.

Cybersecurity Resources

FBI

Cybersecurity: $15.2 million and 22 positions

Funding supports the FBI's Enterprise Security Operations Center in operations and forensic analysis, and the Cybersecurity Threat Assessment Program through its advanced security assessment teams. The additional resources will increase the FBI's ability to monitor and manage internal IT assets and defend them against cyberattacks and inside threats.

Cybersecurity Posture: $14.0 million and 20 positions

Funding will ensure robust cybersecurity through targeted investments in engineering, operations, risk management, and modernization. The FBI is requesting 20 positions to monitor, develop, and create compliance procedures. Non-personnel funding would address foundational IT infrastructure re-engineering requirements to keep pace with cybersecurity technologies, deploying technologies across enterprise computer networks and mobile device platforms to defend against cyber and insider threats.

Cybersecurity Threat Assessment Program: $1.2 million and 2 positions

Funding will proactively address cybersecurity vulnerabilities and the growing cyber threat posed by groups exploiting technology to breach the FBI's technical systems and networks, with the intent to cause harm to the FBI mission and reputation. Cybersecurity technical operations are designed to proactively address enterprise vulnerability and asset discovery requirements while having the flexibility to conduct advanced security assessments based on the realities of continuously evolving adversary threats, tactics, and techniques. The Cybersecurity Threat Assessment program objectives are to ensue systems are securely built, the enterprise is continuously monitored for insider threats and external intrusions, and FBI stakeholders are prepared to respond to cyber threats. *Current services: $79.4 million and 45 positions (2 agents).*

DOJ/ JIST

Cybersecurity/SolarWinds Incident Response: $78.8 million and 0 positions

The SolarWinds supply chain attack, orchestrated by an advanced persistent threat actor, demonstrates the increasingly persistent and sophisticated cyber actors and campaigns threatening vital Federal Government networks. The Department must ensure the integrity and operability of its mission critical IT systems. These resources will enable the Department's Justice Security Operations Center (JSOC) to prevent, detect, respond, and remediate the damage from malicious cyberattacks and espionage against the Department and Federal Government. Key enhancements will be made to modernize the Department's cybersecurity capabilities to support the JSOC mission.

Endpoint Detection and Response

The DOJ will implement an integrated set of detection and protection technologies deployed at the device level to prevent attacks, detect malicious activity, and enable holistic investigation and remediation response to security incidents and alerts.

Cybersecurity Event Logging

The DOJ will augment its logging capability to leverage cloud service provider Application Programming Interfaces to provide visibility into workloads, modifications, and enhanced response capabilities.

Cloud Security Upgrades

The DOJ will enhance its Office 365 licensing across all Department users in order to unlock additional security features such as advanced auditing of mailboxes and improved alerting of anomalous activity.

Security Operations Center Maturation

The implementation of the cybersecurity initiatives to enhance JSOC monitoring and visibility will require an increase in support. In addition to the initiatives across logging, monitoring, and cloud visibility, the JSOC will implement deceptive technology, or honeypots, as a technique to secure high value assets and disrupt threat actor lateral movement by misleading or confusing the adversary through intentionally exposing decoy assets.

Multi-Factor Authentication (PIV) / Encryption

The Department will also move to a centralized identity provider and authentication model, which will eliminate the individual federated component trust model exploited in the compromise, and create a universal, mandatory multi-factor authentication. Under this new model, trust will be established at the individual user and/or device level using OMB's mandated PIV as the strong, second form factor, which will also require the DOJ to implement a secure certificate management system to effectively distribute and manage these authenticators. *There are no current services for this program.*

USNCB INTERPOL Washington

IT Modernization: $2.6 million
Requested funding will modernize OA/Envoy, the IT infrastructure that INTERPOL Washington utilizes to carry out its mission of facilitating international law enforcement cooperation. Funding would support the upgrade of OA/Envoy hardware and software that is rapidly approaching the end of its service life. *Current services: $1.2 million and 1 position.*

Cyber Investigation Resources

FBI

Cyber: $40.0 million and 155 positions (52 agents)
Requested funding will strengthen cyber threat identification, analysis, and attribution; synchronized interagency operations; and cyber workforce development.

Cyber Threat Identification, Analysis, and Attribution: $7.7 million and 10 positions
Funding will increase capacity to identify and analyze cyber activity by known actors with intent and capability to harm the United States, create a new capability to attribute malicious cyber activity to individuals or state actors, and increase capacity to share intelligence.

Synchronized Interagency Operations: $31.2 million and 145 positions (52 agents)
Funding and personnel will support the Model Field Office Cyber Squad, ensuring each FBI field office is equipped at the minimum necessary investigative, analytical, technical, and administrative level to address cyber threats.

Cyber Workforce Development: $1.2 million
Funding will support the Accelerated Cyber Training Program to ensure the FBI continues to be the world's premier cyber investigative agency by pairing world-class training facilities with a world-class training program.

Improved attribution through these resources would increase the U.S. Government's ability to deter and respond to malicious cyber activity. *Current services: $458.4 million and 2,124 positions (1,006 agents).*

CRM

COVID-19 Related Fraud: $1.0 million and 4 term positions (4 attorneys)
Of the Criminal Division (CRM) request of $10.1 million and 20 term positions (20 attorneys) to combat COVID fraud, the cybercrime share of this request is $1.0 million and four term positions (four attorneys). The funding and positions will go towards the increase in child exploitation, identify theft, and cyber attacks during the COVID pandemic. This includes ransomware attacking hospitals and charity scams. *Current services: $80.1 million and 293 positions (187 attorneys).*

OJP

Economic, High-tech, White Collar and Internet Crime Prevention: $13.0 million

The additional funding requested for this program ($1.0 million) will support efforts to enhance the capacity of State, local, tribal, and territorial criminal justice systems to prevent, investigate, respond to, and prosecute economic, cyber, and high-tech crimes through specialized training and technical assistance. *Current services: $12.0 million for a total of $13.0 million.*