U.S. Department of Justice
FY 2017 Budget Request

<div style="border:1px solid">

CYBERCRIME

+$121 Million in Program Increases,
including $2 Million in State, Local and Tribal Programs

</div>

FY 2017 Overview

Cybercrimes are becoming more common, more sophisticated, and more dangerous. Our adversaries increasingly use computers and the Internet to further their illicit activities. Terrorists seek to sabotage critical infrastructure; organized crime syndicates seek to defraud banks and corporations; and spies seek to steal defense and intelligence secrets and intellectual property. Each threatens our nation's economy and security. The significant intrusions of private sector and government networks over the past two years, including the breaches into the Office of Personnel Management, have highlighted the increasing capabilities of these cyber actors.

The Department of Justice has a unique and critical role in cyber security that emphasizes countering and mitigating cyber threats, including by investigating, prosecuting, and providing legal and policy support to other departments for intrusion and cybercrime cases.

The department's FY 2017 Budget provides $121 million in additional resources to investigate and address computer intrusions and cybercrimes, defend the security of the department's critical information networks, and protect against insider threats. The majority of this request provides resources ($85.1 million) to enhance the technical capabilities of Federal Bureau of Investigation (FBI) investigative personnel, increase the number of cyber investigations, and improve cyber collection and analysis.

The request also includes $7.6 million for the Drug Enforcement Administration (DEA), to enhance its ability to combat insider threats and to enhance its cyber security posture. Similarly, $26.4 million is included for Justice Information Sharing Technology (JIST) to maintain and strengthen the department's cyber security environment to counter cyber threats, including insider threats, and to ensure its personnel have unimpeded access to the Information Technology (IT) systems, networks, and data necessary to achieve their missions. These enhancements will build on significant investments made in FY 2015 and FY 2016 to strengthen the department's cyber security posture.

FY 2017 Program Increases

The department requests a total of $121.1 million in program increases to enhance its ability investigate cybercrime and protect its networks.

Investigating Cybercrime

Federal Bureau of Investigation (FBI)

- **Cyber: $85.1 million (non-personnel):** The requested funding will build on the progress and development of the FBI's cyber efforts, which remain a priority for the Director. The FBI will obtain updated and sophisticated IT hardware, IT software, and contractors to expand the foundation of its offensive and defensive operations. Additionally, funding will provide cyber-related training for the FBI's workforce on technical matters and technology to combat highly sophisticated cyber threat actors. FY 2017 current services for this initiative are 1,753 positions (897 agents) and $541.4 million.

Office of Justice Programs (OJP)

- **Economic, High-tech, Cybercrime Prevention**: **An additional $2.0 million** is requested for this grants program, for a total of $15.0 million, to support state and local governments enhance their efforts to combat economic, high-technology, and internet crimes, including the intellectual property crimes of counterfeiting and piracy. The program would also support crime analysis, delivery of evidence-based crime fighting technology - including information sharing systems, software and hardware development, mobile communication solutions to support law enforcement, and re-entry offender case management systems – through grants, training, and technical assistance. The FY 2016 enacted level is $13.0 million.

Protecting Department Networks

- **Cyber Security and Insider Threat: $34.0 million and 11 positions:** Requested funding will establish an insider threat program as mandated by Executive Order 13587, as well as build and sustain additional capability and capacity to monitor DEA's increasingly large and complex classified and sensitive information system resources from threats that could impact DEA operations. The request also includes funding to continue the department's efforts in transforming IT enterprise infrastructure and cybersecurity to address advanced persistent threats and insider threats, including a Department of Justice insider threat tools and analysis hub, expansion of continuous monitoring coverage, and completion of a consolidated Security Operations Center. There are no current services for this initiative.

FY 2017 Program Increases Summary
(Amount in $000s)

Initiative	Component	Positions	Agts/Attys	Amount
Investigating Cybercrime				
Cyber	FBI	0	0	$85,138
Economic, High-tech, Cybercrime Prevention	OJP	0	0	2,000
Protecting Department Networks				
Cyber Security	JIST	0	0	26,440
Insider Threat and Cyber Security	DEA	11	3	7,561
Total, Program Increases		**11**	**3**	**$121,139**

NOTE: Amounts requested by OJP for Cybercrime are also captured in the department's State, Local and Tribal Assistance Fact Sheet.