

Department of Justice Criminal Division



FY 2016 President's Budget

Table of Contents

I. Overview.....	2
II. Summary of Program Changes.....	12
III. Appropriations Language and Analysis of Appropriations Language.....	13
IV. Program Activity Justification.....	13
A. Enforcing Federal Criminal Laws	
1. Program Description	
2. Performance Tables	
3. Performance, Resources, and Strategies	
V. Program Increases by Item.....	20
A. Mutual Legal Assistance Treaty (MLAT) Reform	
B. International Law Enforcement and Justice Development	
C. Strategic Initiatives to Address to Cyber Threats	
D. International Law Enforcement and Justice Development	
VI. Exhibits	
A. Organizational Chart	
B. Summary of Requirements	
C. FY 2015 Program Changes by Decision Unit	
D. Resources by DOJ Strategic Goal/Objective	
E. Justification for Technical and Base Adjustments	
F. Crosswalk of 2014 Availability	
G. Crosswalk of 2015 Availability	
H. Summary of Reimbursable Resources	
I. Detail of Permanent Positions by Category	
J. Financial Analysis of Program Changes	
K. Summary of Requirements by Object Class	
L. Status of Congressionally Requested Studies, Reports, and Evaluations	

I. Overview for Criminal Division

A. Criminal Division Mission and FY 2016 Budget Summary

The Criminal Division's mission is to develop, enforce, and supervise the application of all federal criminal laws, except those specifically assigned to other divisions. Furthermore, the Division must identify and respond to critical and emerging national and international criminal threats and lead the enforcement, regulatory, and intelligence communities in a coordinated nationwide response to reduce those threats.

The events of September 11, 2001, highlighted the need for increased nationwide coordination and information sharing. The Division serves a critical role in coordinating among the Department's criminal law components, including the U.S. Attorneys' Offices. As a "headquarters" office, the Division also serves as the central point of contact for foreign countries seeking law enforcement assistance. No other organization within the Department or the U.S. Government is equipped to fulfill this role – one that is more critical than ever considering the continually increasing globalization and sophistication of crime.

To sustain mission needs, the Criminal Division requests a total of 1,063 permanent positions, 1,173 direct Full-Time Equivalent work years (FTE), and \$242,476,000 in its Salaries and Expenses appropriation for Fiscal Year (FY) 2016. The Division's request will maintain the current level of services, while providing funding for necessary resources to reform the Mutual Legal Assistance Treaty (MLAT) process, support our international training programs, namely the Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT) and the International Criminal Investigative Training Assistance Program (ICITAP), and combat the growing and evolving cyber threat as well as the increasing threat of transnational intellectual property crime.

B. Program Activities and Major Responsibilities

The Criminal Division engages in several program activities to achieve its mission: (1) investigating and prosecuting, (2) providing expert guidance and advice, (3) reviewing the use of law enforcement tools, and (4) fostering global partnerships. Every day, the Criminal Division performs these functions at the forefront of federal criminal law enforcement.

(1) Investigating and Prosecuting

- Investigating and prosecuting the most significant cases and matters
- Coordinating a wide range of criminal investigations and prosecutions that span multiple jurisdictions and involve multiple law enforcement partners

With its investigation and prosecution activities, the Division strives to support its mission by investigating and prosecuting aggressively, but responsibly. By providing both national perspective and leadership, the Division undertakes complex cases and ensures a consistent and coordinated approach to the nation's law enforcement priorities, both domestically and internationally. The Division has a "birds-eye" view of white collar crime, public corruption,

organized crime, narcotics, violent crime, and other criminal activities, and consequently is uniquely able to ensure that crimes that occur across borders do not go undetected or ignored.

Select Recent Criminal Division Accomplishments

- In FY 2014, the Fraud Section continued its investigation and prosecution of individuals and entities for violations of the Foreign Corrupt Practices Act (“FCPA”) and related crimes. During the fiscal year, the Fraud Section resolved 11 cases against corporations with penalties and forfeiture in excess of \$550 million, and it charged, or resolved charges against 13 individuals in FCPA or FCPA-related cases.
- The Securities and Financial Fraud Unit (“SFF”) of the Fraud Section continues to focus on the prosecution of complex and sophisticated securities, commodities, and other financial fraud cases. SFF has tackled some of the largest frauds in the financial services industry and a wide mix of market manipulation and insider trading cases, including conducting an ongoing investigation into possible manipulation of foreign exchange rates, LIBOR, and other international interest rate benchmarks. During FY 2014, SFF resolved five cases against corporations with penalties, restitution, and forfeiture exceeding \$484 million, and it charged, or resolved charges, against 49 individuals including the conviction of three former corporate executives.
- On June 30, 2014, BNP Paribas S.A. (BNPP), a global financial institution headquartered in Paris, agreed to enter a guilty plea and pay \$8.973 billion, including forfeiture of \$8.833 billion and a fine of \$140 million, for conspiring to violate the International Emergency Economic Powers Act (IEEPA) and the Trading with the Enemy Act (TWEA) by processing billions of dollars of transactions through the U.S. financial system on behalf of Sudanese, Iranian, and Cuban entities subject to U.S. economic sanctions. The agreement by the French bank to plead guilty was the first time a global bank has agreed to plead guilty to large-scale, systematic violations of U.S. economic sanctions. The case was prosecuted by the Money Laundering and Bank Integrity Unit of the Criminal Division’s Asset Forfeiture and Money Laundering Section (AFMLS), and the Money Laundering and Asset Forfeiture Unit of the U.S. Attorney’s Office for the Southern District of New York.

(2) Providing Expert Guidance and Advice

- Developing and supporting effective crime reduction strategies and programs
- Driving policy, legislative, and regulatory reforms
- Providing expert counsel and training in criminal enforcement matters to state, local, federal enforcement partners

The Criminal Division serves as the strategic hub of legal and enforcement experience, expertise, and strategy in the fight against national and international criminal threats. Consequently, its expert guidance and advice are crucial to the successful application of criminal law throughout the country. The Division leads the national effort to address emerging criminal trends, including the increasingly international scope of criminal activity. The guidance provided to

U.S. Attorneys' Offices and other federal law enforcement partners ensures the uniform application of the law and furthers the Department of Justice's mission to ensure justice.

Select Recent Criminal Division Accomplishments

- From June 16–27, 2014, the Albanian State Police deployed over 1,000 officers in a multi-day operation to dismantle narcotics production in the town of Lazarat in southern Albania. Lazarat is known as a lawless, marijuana hub that has been off limits to the police for approximately 15 years. Total annual production of marijuana has been estimated at 1,000 tons, with an estimated street value in Western Europe of \$6 billion. For several months prior to the operation, ICITAP-trained undercover officers had successfully infiltrated the village and were providing critical information. Despite coming under fire from high-powered rifles, mortars, and rocket-propelled grenades, the police units combined operational tactics with proactive negotiation resulting in the surrender of cartel leaders and the arrest of 33 criminals. During the operation, police used extensive personal protective equipment supplied by ICITAP and the New Jersey National Guard. The police seized 362 light weapons; 24 machine guns; one anti-aircraft gun; 210,000 rounds of ammunition; 1,200 bricks of high explosives; 625 grenades; 360 mortar rounds; 19 anti-personnel mines; and assorted drug processing equipment. In addition, the police seized and burned over eight kilograms of heroin and nearly 57 metric tons of processed marijuana along with 135,000 marijuana plants.

(3) Reviewing the Use of Law Enforcement Tools

- Approving and overseeing the use of the most sophisticated investigative tools in the federal arsenal

The Division serves as the Department's "nerve center" for many critical operational matters. It is the Division's responsibility to ensure that investigators are effectively and appropriately using available sensitive law enforcement tools. These tools include Title III wiretaps, electronic evidence-gathering authorities, correspondent banking subpoenas, and the Witness Security Program, to name a few. In the international arena, the Division manages the Department's relations with foreign counterparts and coordinates all prisoner transfers, extraditions, and mutual legal assistance requests. Lastly, the Division handles numerous requests for approval from the field to use sensitive law enforcement techniques, in conjunction with particular criminal statutes. For example, the Division reviews every racketeering indictment that is brought across the nation. In these ways, the Division serves a critical and unique role.

Select Recent Criminal Division Accomplishments

- In 2014, the Computer Crimes and Intellectual Property Section (CCIPS) dismantled an extremely damaging botnet and prosecuted its administrator. CCIPS was at the forefront of a multi-national effort to disrupt the Gameover Zeus Botnet – a global network of infected victim computers used by cyber criminals to steal millions of dollars from businesses and consumers – and unsealed criminal charges in Pittsburgh, Pennsylvania, and Omaha, Nebraska against Evgeniy Mikhailovich Bogachev, a Russian national who

served as an administrator of the botnet. In a related action, U.S. and foreign law enforcement officials worked together to seize computer servers central to the malicious software or “malware” known as Cryptolocker, a form of “ransomware” that encrypts the files on victims’ computers until they pay a ransom. This criminal scheme generated over \$27 million in illicit profits. The Department obtained court authorization for the FBI to provide victim information to Computer Emergency Response Teams (CERTs) around the world and to private industry partners in a position to assist victims in ridding their computers of the Gameover Zeus malware.

- During FY 2013, the attorneys in the Division’s Office of Enforcement Operations’ Electronic Surveillance Unit reviewed 2,170 requests to conduct electronic surveillance, covering 7,444 facilities. Those requests continue to increase in complexity, reflecting targets’ (primarily narcotics traffickers) ever-increasing efforts to conceal their criminal activities from law enforcement scrutiny and interference. Several of those cases involved obtaining authorization for the first time ever to conduct electronic surveillance on facilities using new and emerging technologies.

In addition, the Unit continued to be very active in providing electronic surveillance training and guidance to Assistant United States Attorneys, as well as to investigative agents from many law enforcement agencies. These trainings result in higher-quality submissions from the field, allowing the unit to obtain the required authorizations from the Criminal Division’s Deputy Assistant Attorneys General without unnecessary delays.

(4) Fostering Global Partnerships

- Helping international law enforcement partners build capacity to prosecute and investigate crime within their borders by providing training and assistance
- Negotiating Mutual Legal Assistance Treaties with international parties to enhance cooperative efforts with international parties

The Division reaches out to its international partners to ensure the safety of Americans at home and abroad. Posts in ten countries are maintained to foster relationships and participate in operations with international law enforcement and prosecutors. The Division also has personnel in developing democracies across the globe, providing assistance to foreign governments in developing and maintaining viable criminal justice institutions; their responsibility is to sustain democracy and promote greater cooperation in transnational criminal matters, and the capacity to provide modern professional law enforcement services, based on democratic principles and respect for human rights.

Select Recent Criminal Division Accomplishments

- Per the request of the U.S. Embassy in Kiev and the Prime Minister of Ukraine, ICITAP deployed an elections security advisor on short notice to help the country prepare for the May 25, 2014, presidential elections. On May 19, ICITAP took part on a U.S. Embassy election security team that briefed Prime Minister Yatsenyuk and the heads of his criminal justice and security ministries on recommendations to help ensure a stable and

secure environment at 40,000 nationwide polling stations. ICITAP presented its recommendation to immediately establish a Joint Operational Center (JOC), which would allow for a single point to process election and security information and serve as a nexus for unity of command during elections. Of the team's 10 proposed recommendations, the prime minister only approved ICITAP's recommendation and directed the JOC to be stood up immediately. During the week leading up to the elections, ICITAP responded to the prime minister's direct request for assistance in establishing the JOC. Ukraine's cabinet of ministers approved ICITAP's recommendation on the same day it was proposed and agreed to locate the JOC at Ukraine's Central Elections Commission.

- OPDAT's Resident Legal Advisors (RLAs) in Indonesia supply on-going, vital support to the Government of Indonesia on terrorism issues, working closely with the Attorney General's Terrorism and Transnational Crime Task Force (Satgas), which was created with OPDAT assistance. This long-term relationship has been very productive, resulting in the conviction of close to two hundred terrorists, as well as dozens of successful human trafficking, intellectual property, and money laundering prosecutions. The Satgas task force concept has served as a model for the creation of other specialized units, most notably, the Anti-Corruption Task Force and the Natural Resources Crimes Task Force.
- In just its first full year of operation, the OPDAT RLA program in Niger had a major impact on the terrorism investigation and prosecution efforts in that country. Niger has been confronted with threats from a variety of violent extremist organizations, including this year's incursions by Boko Haram. The OPDAT RLA, working cooperatively with French, European Union, and other international partners, implemented a series of activities designed to encourage Nigerien prosecutors, investigators, and judges to utilize their laws, modern law enforcement tools, and cooperation to more fully and effectively combat the terrorist threats. These efforts contributed to the successful use by Niger's specialized terrorism prosecutors and investigators of new investigative and procedural tools that resulted in the arrest and indictment of multiple suspected terrorists.
- In 2014, the OPDAT RLA program in Kenya, designed to improve the country's capacity to combat terrorism, terror financing (CFT), and money laundering (AML), achieved a number of successes. For example, the RLA's technical support to Kenyan counterparts was critical to the establishment of Kenya's new Financial Reporting Center (FRC), an agency that handles AML/CFT reporting. The RLA's work with the FRC and with the Kenya prosecutor's office to improve its efforts to enforce the new terrorism and money laundering laws and to begin to implement aspects of the mutual legal assistance and asset forfeiture legislation led the international Financial Action Task Force to remove Kenya from the International Cooperation Review Group (ICRG) process (the "black list"). This was a significant milestone because it increases Kenya's opportunities to engage in international commerce and facilitates economic development.
- Corruption remains the most significant crime problem in the Philippines, and historically, most defendants have been acquitted after lengthy trial proceedings. Accordingly, the OPDAT RLA has focused his efforts on supporting the institutional development of the Office of the Ombudsman, which has the legal authority to prosecute

major corruption cases and is now enjoying an improving conviction rate. With assistance from the RLA, the Ombudsman created pilot prosecutor/investigator teams for high-profile cases, including the Pork Barrel scam, the most important corruption case in recent Philippine history. This case has resulted in the indictment of three senators as well as the investigation of various congressmen for steering development funds to non-existent non-governmental organizations in return for large kickbacks.

- In Mexico, OPDAT’s relationships with the three branches of Mexican government have resulted in transformational changes in the Mexican justice sector. The past year has been particularly groundbreaking, as OPDAT RLAs have worked closely with the Mexican legislature and Office of the Attorney General (PGR) to develop Mexico’s new Code of Criminal Procedure, which finally passed on February 5, 2014. The new code, which includes significant input from OPDAT, puts Mexico on a path towards an accusatorial system, and is the basis for a three year training program to prepare the PGR for the transition and greater coordination with the U.S. justice system.
- OPDAT RLAs working on Trafficking in Persons (TIP) in the Western Hemisphere are helping DOJ respond to the Unaccompanied Children crisis by delivering critical technical assistance to justice sector institutions in the region, as well providing information to Department leadership and Congressional delegations as to the root causes and circumstances surrounding the crisis. Specifically, the OPDAT RLA in Honduras is traveling across the region to establish relationships and promote collaboration among the neighboring countries, and is providing technical assistance in cases not only in Honduras, but also in Guatemala and El Salvador. In Mexico, OPDAT RLAs are expanding TIP programming to include other countries in the region, also contributing to a much-needed regional approach and collaboration on this issue which affects U.S. national security.

C. The Criminal Division’s Strategic Priorities

The Criminal Division leverages its substantial expertise in a broad array of federal criminal subject matters to help the Department achieve all three Strategic Goals: (1) Prevent Terrorism and Promote the Nation’s Security Consistent with the Rule of Law, (2) Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law; and (3) Ensure and Support the Fair, Impartial, Efficient, and Transparent Administration of Justice at the Federal, State, Local, Tribal and International Levels (see table below).

Department of Justice’s Strategic Plan	
Goal One: Prevent Terrorism and Promote the Nation’s Security Consistent with the Rule of Law	1.1 Prevent, disrupt, and defeat terrorist operations before they occur by integrating intelligence and law enforcement efforts to achieve a coordinated response to terrorist threats
	1.2 Prosecute those involved in terrorist acts
	1.4 Combat cyber-based threats and attacks through the use of all available tools, strong public-private partnerships, and the investigation and

	prosecution of cyber threat actors
Goal Two: Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law	2.1 Combat the threat, incidence, and prevalence of violent crime, by leveraging strategic partnerships to investigate, arrest, and prosecute violent offenders and illegal firearms traffickers
	2.2 Prevent and intervene in crimes against vulnerable populations and uphold the rights of, and improve services to America’s crime victims
	2.3 Disrupt and dismantle major drug trafficking organizations to combat the threat, trafficking, and use of illegal drugs and the diversion of illicit drugs
	2.4 Investigate and prosecute corruption, economic crimes, and transnational organized crime
	2.5 Promote and protect American civil rights by preventing and prosecuting discriminatory practices
Goal Three: Ensure and Support the Fair, Impartial, Efficient, and Transparent Administration of Justice at the Federal, State, Local, Tribal and International Levels	3.1 Promote and strengthen relationships and strategies for the administration of justice with law enforcement agencies, organizations, prosecutors, and defenders, through innovative leadership and programs
	3.6 Prevent and respond to genocide and mass atrocities and ensure that perpetrators of such crimes are held accountable in the United States, and if appropriate, their home countries

In working to achieve these goals, the Division has identified the following key strategic outcomes to address the country’s most critical justice priorities:

- Ensuring **trust and confidence in government institutions**, by reducing public corruption at every level of government;
- Ensuring the **stability and security of domestic and global markets**, as well as the integrity of government programs, by reducing fraud, money laundering, and other economic crimes;
- **Disrupting and dismantling criminal organizations and networks that act across state and national boundaries** and that threaten our country through violence, drug trafficking, and computer crime;
- Combating **cyber-based threats and attacks**;
- **Protecting our children** from exploitation and **vindicating human rights**, wherever possible;
- **Promoting the Rule of Law** around the world; and

- **Supporting national security** and crime-fighting efforts across federal, state, and local governments.

The Division also plays a key role in the development and implementation of the Department's Smart on Crime initiative, a comprehensive review of the criminal justice system in order to identify reforms that would ensure federal laws are enforced more fairly and efficiently. Examples of the Division's work in this initiative are as follows:

- Participated in a Department working group that assisted the Attorney General in developing the Smart on Crime Strategy, including new charging policies for drug offenses, a new policy on the collateral consequences of conviction, and a new guidance memo on prosecution priorities for US Attorneys.
- Worked with the Bureau of Prisons to craft a new policy on compassionate release for elderly and infirm prisoners.
- Advocated, as the Department's ex-officio member of the U.S. Sentencing Commission, for reductions in guideline drug penalties enacted by the Commission in 2014 as well as for their retroactive application to tens of thousands of imprisoned drug offenders.
- Participated in the Federal Reentry Roundtable, an inter-branch working group focused on improving Federal offender reentry outcomes, and served as the policy advisor to the Charles Colson Task Force on Federal Corrections, a congressionally mandated task force to study and make recommendations to improve federal sentencing and corrections.

D. Challenges to Achieving Outcomes

Many factors, both external and internal, impact the Criminal Division's capacity to accomplish its goals. While some of these factors are beyond its control, the Division strives to navigate these obstacles successfully and to minimize the negative impact that these factors have on the Division's critical mission.

External Challenges

1. Globalization of Crime: The increasing globalization of crime and the emergence of transnational threats will continue to bring new challenges to law enforcement, both at home and abroad. In its commitment to combat transnational threats, the Criminal Division continues to serve as the Department's "global headquarters," effectively developing criminal policies and legislation, while monitoring both national and transnational criminal trends. As important, the Division is the central clearinghouse for all requests by foreign countries for evidence of crimes that may be in the United States and for all requests by U.S. law enforcement authorities for evidence of crimes that may reside abroad. The Division has the breadth of experience and the unique capability to build essential global partnerships to successfully combat transnational crimes, but requires critical resources to keep pace with the increasing demand for its services.
2. Advances in Technology: New technologies have generated cutting-edge methods for committing crimes, such as use of the Internet to commit identity theft and use of peer-to-peer software programs to share large volumes of child pornography in real-time. These

technologies continue to pose many challenges to law enforcement agents and prosecutors alike. It is the Division's job to keep pace with these cutting-edge methods of technology and provide training and assistance to other prosecutors and investigators.

3. Weak International Rule of Law: Some countries lack effective policies, laws, and judicial systems to investigate and prosecute criminals in their countries. These weaknesses create obstacles for the Division, as it tries to bring criminals to justice and seize their ill-gotten profits.
4. Increasing Statutory Responsibilities in a Challenging Fiscal Environment: New legislation that increases the Division's responsibilities has placed additional demands on the Division's resources. This includes the steady increase in the number of mandatory reporting requirements to which the Division must respond.

Internal Challenges

The Criminal Division faces a number of internal challenges due to growing demands. These challenges include the following:

1. Automated Litigation Support: Cases and matters the Division prosecutes and investigates are complicated and complex and require a massive amount of data to be processed and stored.
2. Information and Network Security: To stay one step ahead of criminals, the Division needs to acquire the most advanced IT equipment and software available. Additionally, it must ensure that it is invulnerable to cyber attacks or computer intrusions.

E. Budget and Performance Integration

This budget demonstrates how the Criminal Division's resources directly support the achievement of the Department's strategic goals and priorities – both nationally and internationally.

The Division reports as a single decision unit; therefore, its resources are presented in this budget as a whole. Total costs represent both direct and indirect costs, including administrative functions and systems. The performance/resources table in Section IV of this budget provides further detail on the Division's performance-based budget.

F. Environmental Accountability

The Criminal Division has taken significant steps to integrate environmental accountability into its daily operations and decision-making process:

- The Division has initiated (paperless) electronic transmittal of all service work requests and internal administrative services, which saves paper and reduces its carbon footprint.

- The Division has completed the balancing of the water system to conserve and provide more efficient use of its supplemental air conditioning units.
- The Division is continuing to work with building management to install occupancy sensors in all offices in the Bond building to save energy. New light fixtures will also be installed to satisfy energy saving requirements. These fixtures provide low watts per square foot with energy saving ballast and controls.
- The Division continues to take steps to improve the recycling and environmental awareness programs within the Division. The Division has a comprehensive recycling program that includes the (1) distribution of individual recycling containers to every federal and contract employee, (2) inclusion of recycling flyers in all new employee orientation packages, (3) publication of energy and recycling articles in the Division's Security and Operations Support newsletter, and (4) creation of a recycling section on the Division's Intranet site. The Division is in ongoing discussions with two of its leased buildings to use "Single Stream" recycling which would enhance the Division's program overall by removing the requirement for tenants to separate recyclables.

II. Summary of Program Changes

Item Name	Description				Page
		Pos.	FTE	Dollars (\$000)	
MLAT Reform	The requested positions and resources would allow the Division to implement the four elements—(1) Centralization, (2) Training and Outreach, (3) Reducing the Backlog, and (4) Technology—as the Department has defined to address the MLAT issues.	141	141	\$32,111	20
International Law Enforcement and Justice Development	This request would fully fund the headquarters operating expenses of its International Criminal Investigative Training Assistance Program (ICITAP), the Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT), and the Office of Administration’s International Training and Financial Management unit (ITFM), which solely supports the financial management and execution of ICITAP’s and OPDAT’s programs.	107	83	\$12,434	30
Strategic Initiatives to Address Cyber Threats	This request would allow the Criminal Division to combat the growing and evolving cyber threat. The additional resources will increase the Division’s capability in four key areas: cybercrime investigations and prosecutions; advice and advocating legal tools and authorities; international cooperation and outreach; and forensic support.	54	29	\$6,123	40
Intellectual Property	This request would help the Criminal Division to better combat the increasing threat of transnational intellectual property crime. The additional resources will be used to place two DOJ Attachés overseas that will serve as regional International Computer Hacking and Intellectual Property coordinators (ICHIPs). A portion of this enhancement also be used to increase the capacity of the Division’s domestic IP program to provide critical support to the ICHIP/Attachés and ensure the coordinated use of ICHIP resources overseas.	11	6	\$2,205	48

III. Appropriations Language and Analysis of Appropriations Language

Appropriations Language

No changes to appropriations language.

IV. Program Activity Justification

A. Enforcing Federal Criminal Laws

<i>Enforcing Federal Criminal Laws</i>	Direct Pos.	Estimate FTE	Amount (000)
2014 Enacted	750	620	\$174,189
2015 Enacted	750	674	\$178,042
Adjustments to Base and Technical Adjustments	0	0	\$11,561
2016 Current Services	750	674	\$189,603
2016 Program Increases	313	259	\$52,873
2016 Program Offsets	0	0	\$0
2016 Request	1,063	933	\$24,476
Total Change 2015-2016	313	259	\$64,434

1. Program Description

The mission of the Criminal Division is to develop, enforce, and supervise the application of all federal criminal laws, except those specifically assigned to other divisions. The Criminal Division is situated at headquarters to work in partnership with both domestic and international law enforcement. While U.S. Attorneys and state and local prosecutors serve a specific jurisdiction, the Criminal Division addresses the need for centralized coordination, prosecution, and oversight.

The Division complements the work of its foreign and domestic law enforcement partners by centrally housing subject matter experts in all areas of federal criminal law, as reflected by the 16 Sections and Offices that make up the Division's Decision Unit "Enforcing Federal Criminal Laws:"

- Appellate Section;
- Asset Forfeiture and Money Laundering Section;
- Capital Case Section;
- Child Exploitation and Obscenity Section;
- Computer Crime and Intellectual Property Section;
- Human Rights and Special Prosecutions Section;
- International Criminal Investigative Training Assistance Program;
- Narcotic and Dangerous Drug Section;
- Office of Administration;

- Office of the Assistant Attorney General;
- Office of Enforcement Operations;
- Office of International Affairs;
- Office of Overseas Prosecutorial Development, Assistance and Training;
- Office of Policy and Legislation;
- Organized Crime and Gang Section; and
- Public Integrity Section.

The concentration of formidable expertise, in a broad range of critical subject areas, strengthens and shapes the Department's efforts in bringing a broad perspective to areas of national and transnational criminal enforcement and prevention. To capture this range of expertise, the Division's Performance and Resource Table is organized into three functional categories: prosecutions and investigations; expert guidance and legal advice; and the review of critical law enforcement tools. In addition, the chart shows the Division support of the Department's Strategic Goals and Objectives.

2. Performance Tables

PERFORMANCE AND RESOURCES TABLE												
Decision Unit: Enforcing Federal Criminal Law												
RESOURCES			Target		Actual		Projected		Changes		Requested (Total)	
			FY 2014		FY 2014		FY 2015		Current Services Adjustments and FY 2016 Program Changes		FY 2016 Request	
Total Costs and FTE (reimbursable FTE are included)			FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
			971	\$174,189	620	\$173,528	674	\$178,042	259	\$64,434	933	\$242,476
TYPE	STRATEGIC OBJECTIVE	PERFORMANCE	FY 2014		FY 2014		FY 2015		Current Services Adjustments and FY 2016 Program Changes		FY 2016 Request	
Program Activity	1.2, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 3.6	1. Prosecutions and Investigations	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
			466	\$83,611	298	\$83,293	324	\$85,460	5	\$9,432	329	\$94,892
Workload		Cases Opened	430		345		352		5		357	
Workload		Cases Closed	378		434		278		4		282	
Workload		Cases Pending	1,171		1,091		1,041		75		1,116	
Workload		Appellate Work - Opened	3,207		3,304		2,595		0		2,595	
Workload		Appellate Work - Closed	3,198		2,795		1,995		0		1,995	
Workload		Appellate Work Pending	3,088		3,319		3,915		609		4,515	
Workload		Matters Opened	932		769		762		12		774	
Workload		Matters Closed	994		943		805		12		817	
Workload		Matters Pending	1,365		1,253		1,108		-44		1,064	

PERFORMANCE AND RESOURCES TABLE

Decision Unit: Enforcing Federal Criminal Law

RESOURCES		Target		Actual		Projected		Changes		Requested (Total)		
		FY 2014		FY 2014		FY 2015		Current Services Adjustments and FY 2016 Program Changes		FY 2016 Request		
Program Activity	1.1, 1.2, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.6	2. Expert Guidance and Legal Advice	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
					359	\$64,450	229	\$64,205	249	\$12,434	97	\$20,043
Workload		Number of Legislative and Policy Analysis matters Completed	5,314		6,304		4,668		262		4,930	
Workload		Number of Programmatic Coordination Activities	11,127		11,428		10,757		605		11,362	
Workload		Number of Legal Advisory Matters Completed	33,406		39,620		35,054		1,971		37,025	
Workload		Number of Training Sessions/Presentations	3,605		3,628		4,053		228		4,281	
Program Activity	1.1, 1.2, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.6	3. Law Enforcement Tools	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
					146	\$26,128	93	\$26,029	101	\$26,706	157	\$34,959
Workload		Number of Mandatory Reviews Completed	20,944		21,744		19,218		2,000		21,218	
Workload		Favorably Resolved Criminal Cases	90%		98%		90%				90%	
Workload		Favorable Resolved Civil Cases	80%		N/A		80%				80%	

Data Definition, Validation, Verification, and Limitations: Definitions: Prosecutions and Investigations: This program activity includes cases or investigatory matters in which the Criminal Division has sole or shared responsibility. The case breakouts include cases from the following Sections/Offices: Fraud Section, Public Integrity Section, Computer Crimes and Intellectual Property Section, Child Exploitation and Obscenity Section, Organized Crime and Gang Section, Narcotic and Dangerous Drug Section, Asset Forfeiture and Money Laundering Section, Human Rights and Special Prosecutions Section, and Capital Case Section. Appeals: Appellate Section. Expert Guidance & Legal Advice: This program activity includes oral and written advice and training to federal, state, local, and foreign law enforcement officials; coordination and support of investigations, prosecutions, and programs at the national, international and multi-district levels; and oral and written analysis of legislation and policy issues, development of legislative proposals, advice and briefing to Departmental and external policy makers, and participation in inter-agency policy coordination and discussions. Law Enforcement Tools: This program activity includes the work the Division does in specific areas of criminal law in reviewing and approving the use of law enforcement tools throughout the law enforcement community. Validation: In FY 2002, the Division initiated a multi-phased workload tracking improvement initiative. To date, improvements include definition and policy clarifications, uniform guidance and reporting, case tracking database improvements for end user benefit, and a regular data validation process to ensure system integrity.

Strategic Objective		PERFORMANCE MEASURE TABLE									
		Decision Unit: Enforcing Federal Criminal Laws									
		Performance Report and Performance Plan Targets		FY 2010	FY 2011	FY 2012	FY 2013	FY 2014		FY 2015	FY 2016
				Actual	Actual	Actual	Actual	Target	Actual	Target	Target
1.1, 1.2, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.6	OUTPUT Measure	Number of Legislative and Policy Analysis Matters Completed	6,524	7,458	5,875	6,493	5,314	6,304	4,668	4,930	
	OUTPUT Measure	Number of Programmatic Coordination Activities	3,509	4,492	5,226	11,892	11,127	11,428	10,757	11,362	
	OUTPUT Measure	Number of Legal Advisory Matters	19,039	24,438	39,726	42,986	33,406	39,620	35,054	37,025	
	OUTPUT Measure	Number of Training Sessions/Presentations	2,767	3,612	3,845	5,133	3,605	3,628	4,053	4,281	
	OUTPUT Measure	Number of Mandatory Reviews Completed	46,125	19,237	19,090	26,977	20,944	21,477	19,218	21,218	
	OUTCOME Measure	Favorably resolve criminal cases	90%	96%	93%	97%	90%	89%	90%	90%	
	OUTCOME Measure	Favorably resolve civil cases	100%	100%	N/A	100%	80%	N/A	80%	80%	

3. Performance, Resources, and Strategies

a. Performance Plan and Report for Outcomes

Outcome Measure

The Department's long-term outcome goal for the litigating divisions, including the Criminal Division, is the percentage of criminal and civil cases favorably resolved during the Fiscal Year. The goals are 90 percent (criminal) and 80 percent (civil). The Division has consistently met or exceeded the goals. In FY 2014, the Division met both outcome goals and is on track to meet both of them in FY 2015.

Prosecutions and Investigations Workload

The Division leads complex investigations and tries significant prosecutions. Many of these cases are of national significance, require international coordination, have precedent-setting implications, and involve the coordination of cross-jurisdictional investigations.

Other Critical Division Workload

In addition to investigating and prosecuting criminal cases, the Division plays a central role in the Department's mission by reviewing the use of critical law enforcement tools, including the approval of all requests for wiretapping under Title III. The Division also provides expert guidance and legal advice on significant legislative proposals, analyzes Department-wide and government-wide law enforcement policy, conducts training for the field, and engages in programmatic coordination.

b. Strategies to Accomplish Outcomes

The Criminal Division's mission is to develop, enforce, and exercise general oversight for all federal criminal laws. In fulfilling this mission, the Division plays a central role in assisting the Department in accomplishing its Strategic Goals and Objectives. The Division contributes to ten of the Department's eighteen strategic objectives. The performance measures and outcome measures, reported in the budget, measure performance in a combination of strategic objectives covering the entire breadth of the Division's work.

c. Priority Goals

The Criminal Division contributes to two priority goals:

Financial Fraud/Healthcare Fraud: Protect the American people from financial and healthcare fraud: In order to efficiently and effectively address financial fraud and healthcare fraud, by September 30, 2015, reduce by 3 percent the number of financial and healthcare fraud investigations pending longer than 2 years.

Vulnerable People: Protect vulnerable populations by increasing the number of investigations and litigation matters concerning child exploitation, human trafficking, and non-compliant sex offenders; and by improving programs to prevent victimization, identify victims, and provide services. By September 30, 2015, working with federal, state, local, and tribal partners, to protect potential victims from abuse and exploitation through three sets of key indicators:

- Open investigations concerning non-compliant sex offenders (4% over average of FYs 2012, 2013), sexual exploitation of children (3% over average of FYs 2011, 2012, 2013), and human trafficking (2% over FY 2013)
- Open litigation matters concerning sexual exploitation of children and human trafficking (5% increase over baseline)
- Percent of children recovered within 72 hours of issuance of an AMBER alert (90%)

The Division's progress regarding these two goals is reported quarterly to the Department.

V. Program Increases by Item

Item Name: Mutual Legal Assistance Treaty (MLAT) Reform

Strategic Goal:

Goal One: Prevent Terrorism and Promote the Nation’s Security Consistent with the Rule of Law	1.1 Prevent, disrupt, and defeat terrorist operations before they occur by integrating intelligence and law enforcement efforts to achieve a coordinated response to terrorist threats
	1.2 Prosecute those involved in terrorist acts
	1.4 Combat cyber-based threats and attacks through the use of all available tools, strong public-private partnerships, and the investigation and prosecution of cyber threat actors
Goal Two: Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law	2.1 Combat the threat, incidence, and prevalence of violent crime by leveraging strategic partnerships to investigate, arrest, and prosecute violent offenders and illegal firearms traffickers
	2.2 Prevent and intervene in crimes against vulnerable populations and uphold the rights of, and improve services to America’s crime victims
	2.3 Disrupt and dismantle major drug trafficking organizations to combat the threat, trafficking, and use of illegal drugs and the diversion of licit drugs
	2.4 Investigate and prosecute corruption, economic crimes, and transnational organized crime
	2.5 Promote and protect American civil rights by preventing and prosecuting discriminatory practices
Goal Three: Ensure and Support the Fair, Impartial, Efficient, and Transparent Administration of Justice at eh Federal, State, Local, Tribal and International Levels	3.1 Promote and strengthen relationships and strategies for the administration of justice with law enforcement agencies, organizations, prosecutors, and defenders, through innovative leadership and programs
	3.6 Prevent and respond to genocide and mass atrocities and ensure that perpetrators of such crimes are held accountable in the United States, and if appropriate, their home countries

Budget Decision Unit(s): Enforcing Federal Criminal Law

Organizational Program: Criminal Division

Program Increase: Positions 141 Atty 77 FTE 141 Dollars \$32,111,000

Description of Item

In order to safeguard our nation and our citizens, the United States must actively and timely share critical law enforcement information with our foreign partners. United States and foreign law enforcement authorities make formal requests to each other for evidence in criminal cases through a process referred to as “mutual legal assistance” (MLA), made often through our Mutual Legal Assistance Treaties (MLATs). Over time, and with the increase in electronic evidence, it is essential that the Department transform and update how we handle international MLA requests in criminal and counterterrorism matters. Without modernizing the MLA process, our relationships with our international law enforcement partners and U.S. Internet communication providers are at risk, and our national security and diplomatic efforts are threatened.

The Criminal Division’s Office of International Affairs (OIA) serves as the “central authority” for the entire United States under our international treaties for responding to MLA requests and sending MLA requests overseas. State, local, and federal prosecutors in the United States work through OIA to obtain foreign evidence in their cases, and foreign prosecutors send their requests for evidence located in the United States to OIA. The centrality of OIA and its critical role in handling formal requests for evidence cannot be overstated: requests for evidence from overseas must be made through OIA, and foreign counterparts must work through OIA to obtain evidence located in the United States. OIA has seen a dramatic growth in mutual legal assistance requests in general, and for cases involving Internet Service Provider (ISP) records in particular, but resources for OIA have fallen far behind, resulting in a large backlog of requests and significant delays in response time. OIA’s difficulty in responding to foreign requests promptly jeopardizes the effectiveness of U.S. law enforcement and our diplomatic efforts. OIA’s difficulty in ensuring that foreign authorities have the evidence to prosecute crime and terrorism in their countries damages our interests in effective law enforcement worldwide and threatens reciprocal cooperation when we seek evidence from other countries for our own cases.

Further, the delays in responding to requests for ISP records in particular threaten the competitiveness of ISPs and our model of Internet governance. Because of the difficulties in timely responses to foreign requests for ISP records, we have seen increased foreign calls for moving or mirroring U.S. ISP data storage overseas; foreign demands that U.S. ISPs produce information directly in response to foreign orders; and foreign proposals that U.S. ISPs be subjected to national or multilateral data protection regimes. These proposals place U.S. companies in difficult positions and threaten our own cybersecurity.

The President, through his National Security Strategy, has recognized the importance of centralizing international mutual cooperation in criminal justice and counterterrorism matters. The Strategy calls for our law enforcement agencies to “cooperate effectively with foreign governments” in order to “provide safety and security,” and, in particular, states that the U.S. will “strengthen our international partnerships” to counter cybersecurity threats. To this end, President Obama has called upon our allies and partners to “join in building a new framework for international cooperation to protect all our citizens from the violence, harm, and exploitation wrought by transnational organized crime.”

We can build the “new framework for international cooperation” envisaged by the President’s National Security Strategy. To do so, however, the Criminal Division’s OIA must be provided with the resources necessary to modernize the process by which MLA requests are handled and receive resources so that those requests can be handled in a timely manner. The payoff would be dramatic. We would strengthen foreign countries’ ability to gather evidence to fight crime in their countries and before it reaches our shores, and we would strengthen reciprocal obligations for foreign countries to provide evidence that U.S. prosecutors request for criminal cases here. We would undercut key arguments for “decentralizing” the Internet or negotiating a new U.N. Cybercrime Convention – arguments that have only gained force following Edward Snowden’s disclosures from the National Security Agency – while also demonstrating that effective cooperation is possible under the Budapest Cybercrime Convention. Further, we demonstrate that the United States is leading the transformation of the way that MLA requests are handled worldwide.

To achieve these goals, the Division is requesting an increase of **141 positions (77 attorneys), 141 FTE, and \$32,111,000.**

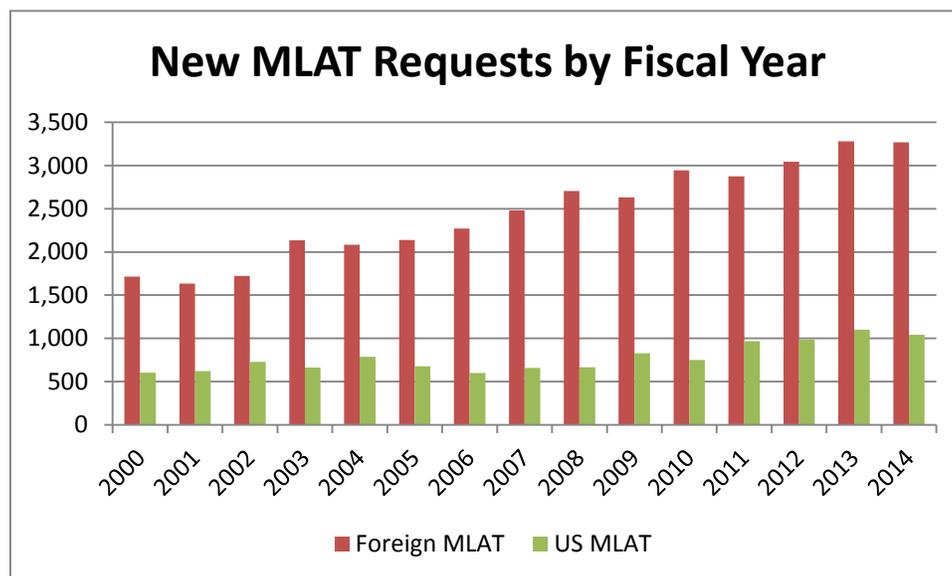
Support of the Department’s Strategic Goals

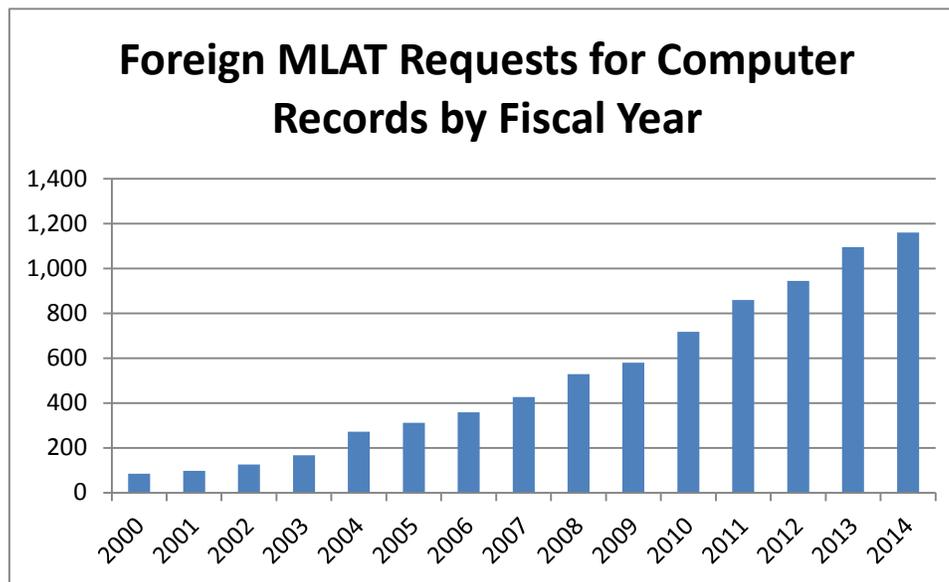
As MLA requests are made in all types of criminal cases, this budget request directly supports all three of the Department’s strategic goals and many of its objectives. The requested increase will improve efficiency and effectiveness of the MLA handling process and strengthen our international programs.

Justification

1. The Department’s Increasing Workload Shouldered by Decreasing Personnel

MLA requests generally are made in the following situations: (1) if a court order is needed to obtain the evidence; (2) to meet formalities to assure the evidence is admissible; and/or (3) where use of the MLAT process is dictated by the domestic law of one of the two countries. Since FY 2000, the number of requests for assistance from foreign authorities handled by OIA has increased nearly 85 percent, and the number of requests for computer records has increased over 1,000 percent.





As illustrated above, the growth of foreign requests for computer records far outpaces that for MLA requests generally. The increased number of cases is not the only challenge, however. The high legal standards for obtaining ISP records, particularly for the content of communications, makes the process of evaluating foreign requests difficult and time consuming. The legal standard required when content of communications is sought is probable cause – typically requiring a search warrant – and OIA usually must work closely with our foreign partners and U.S. law enforcement agents stationed abroad to compile the evidence and prepare the required documents to secure court approval.

In fiscal year 2014, OIA opened 3,270 foreign requests for assistance. That same year, OIA granted assistance in whole or in part, in 1,465 cases, or 45% of the requests.

While its workload has dramatically increased, OIA has seen minimal changes in its staffing, and in fact suffered significant attrition during the Department-wide hiring freeze. The significant period of short staffing has increased OIA’s case backlog.

Importantly, not all OIA resources can be devoted to MLA requests. OIA’s work with foreign MLATs is only one of several of its unique, and largely non-discretionary functions, including preparing U.S. requests for extradition of foreign fugitives and working with foreign authorities to secure the surrender of fugitives; preparing all U.S. requests for foreign evidence and witnesses; negotiating all extradition treaties and MLATs with the Department of State; and formulating international criminal justice policy. There are more than 1,000 fugitive requests alone every year.

2. Limited Technology

The case management system currently in use for managing all of OIA’s case work has not seen a significant upgrade since its implementation in 1999. As a result, there is a lack of transparency for OIA to see the progress of each request at each iterative step, e.g., receipt of the request, conclusion of review by OIA, receipt of the request by a U.S. Attorney’s Office, court order date, and date evidence when it was received. More importantly, a significant source of frustration for our state, local and foreign partners is that no public-facing system or website is

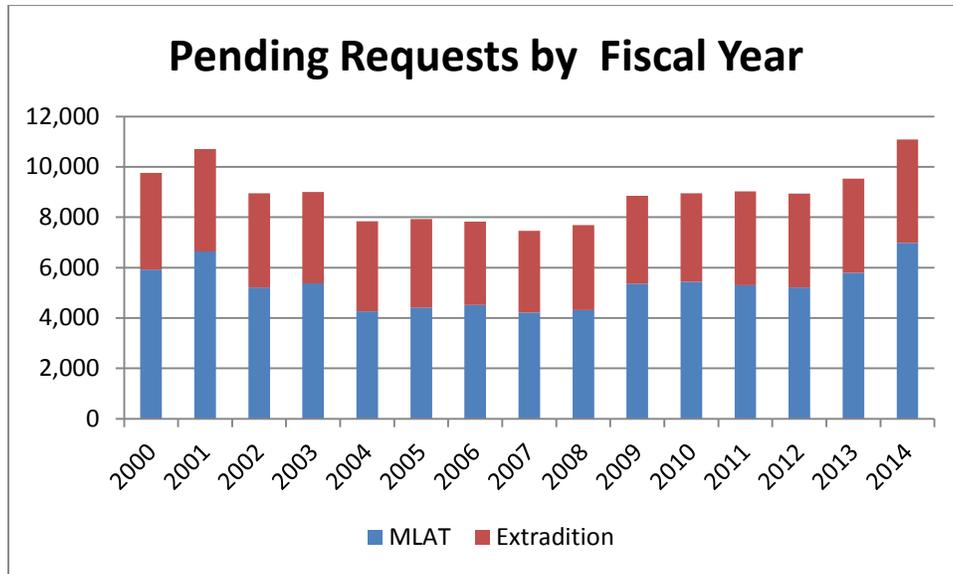
available for them to monitor the status of their requests. Creating a secure, external website with information available to state and local counterparts as well as foreign authorities would reduce time and resources spent in communicating basic information, providing guidance, and transmitting exemplars and templates, and it would be a significant step toward transparency in the process.

3. Structural Impediments

President Obama signed into law the *Foreign Evidence Request Efficiency Act of 2009*, codified at Title 18, United States Code Section 3512, which, among other things, was intended to implement efficiencies and create flexibility in the execution of foreign assistance requests. It creates venue in the District of Columbia for court orders to compel the production of evidence sought by foreign authorities. This significant structural change allows OIA to respond directly to requests for evidence that require court orders, rather than working through U.S. Attorneys' Offices (USAOs) in the district in which the evidence is located. Through this legislation, the Obama Administration has made possible a paradigm shift in how mutual legal assistance requests are handled; but to actualize this shift, OIA requires additional legal and professional personnel to undertake work currently performed by USAOs.

Because of the lack of OIA resources, OIA still relies on USAOs to handle many requests for evidence. This process results in many inefficiencies. Often, Assistant U.S. Attorneys (AUSAs) defer execution of foreign MLA requests while they address more pressing cases in their districts. Moreover, duplication of efforts occurs because all matters must be reviewed by OIA for legal sufficiency and consistency with DOJ and federal policy, but all matters that are referred to the USAOs for execution are likewise reviewed for legal sufficiency by the AUSAs responsible for securing the necessary court orders. Currently, OIA has approximately 4,800 pending foreign MLA requests and, of those, approximately 1,500 to 2,000 are pending execution with USAOs and U.S. law enforcement agencies.

Between FYs 2002 and 2008, OIA managed its steadily increasing volume of work without additional resources, through the efficient use of paralegals and improved case management practices. In FY 2009, however, OIA reached its saturation point and its backlog began to increase steadily as a result. In FY 2014, as illustrated in the chart below, OIA's backlog reached more than 11,000 cases for the first time since FY 2001.



Currently, OIA is handling approximately 5,400 requests from U.S. prosecutors directed to foreign countries for the return of fugitives and production of evidence, and approximately 5,300 requests for fugitives and evidence received from foreign counterparts. Approximately 4,800 of those foreign requests are for evidence, and of that 4,800, approximately 1,600 of the requests are for computer records.

Based on historical experience and a qualitative review of OIA’s existing process, it has been determined that between 120 and 150 cases would be a manageable caseload per OIA attorney under the current model, where AUSAs are still responsible for court filings and appearances. Yet, OIA case attorneys currently carry nearly three times the manageable caseload -- an average caseload of 362 cases each -- a caseload that has increased 81 percent in the last six years, from an estimated caseload of 200 cases per attorney in FY 2008.

Projected OIA Backlog Increases FY 2015-2020 (No Additional Resources)¹

FY	Projected Backlog	Projected Caseload Backlog per Attorney
2015	11,522	281
2016	12,066	294
2017	12,721	310
2018	13,600	332
2019	14,713	359
2020	16,067	392

¹ These projections are based on FY 2014 pending cases and attorney resources as well as anticipated increases in caseload. Actual case execution and changes to pending cases can vary depending on the types of requests OIA receives and the personnel resources available to execute them.

OIA has been rendered unable to meet all incoming foreign requests, even after refusing cases on “*de minimis*” grounds, over the objections of the Department’s foreign counterparts that there is no treaty exception for such cases. As a result, we are facing criticisms and increasing frustration from our foreign counterparts, such as:

- On February 20, 2013, the Latvian Prosecutor General held a press conference to publicly criticize the United States for its failure to respond in a timely manner to Latvia’s requests for mutual legal assistance. To this point, Latvia has been one of the U.S.’s most reliable partners in Eastern Europe.
- On April 5, 2013, the Division received a letter from Germany’s Director General of Criminal Law criticizing OIA’s “*de minimis*” policy. He stated that while focusing on only serious forms of criminality “can be one way of ensuring effective criminal prosecutions” in an age experiencing a “significant rise in cross-border offenses,” the *de minimis* policy is “not a path provided for in the mutual legal assistance agreements that the USA has concluded with the European Union and with Germany. Those agreements provide for an **obligation** to execute mutual legal assistance requests. They do not provide for a refusal of execution in cases involving less serious offenses. **Germany’s approach has been to provide the necessary increase in staff.**” (*emphasis in original*).

Solutions and Resourcing Strategy

Several concurrent approaches are required to address this multi-faceted problem, namely: (1) centralization; (2) training and outreach, (3) reducing the backlog, and (4) technology. Centralizing the handling of requests within OIA as envisioned by the *Foreign Evidence Request Efficiency Act of 2009* will yield the most efficient and effective MLAT process. In addition, coordinated training and outreach to foreign partners is critical to ensure MLAT requests meet U.S. legal standards. There is an urgent need for increased resources to reduce the backlog and keep pace with incoming requests. Finally, new technology, including a web-based system for interacting with foreign partners, is necessary to provide transparency and better communication to meet the expectations of our state, local, and foreign partners.

1. Centralization:

The Department requires additional resources to use the authorities provided by the 2009 legislation and centralize the execution of foreign MLAs with OIA, working with the USAO in the District of Columbia, rather than distributing the requests to USAOs in the districts in which the evidence is located. A few matters involving physical searches, witness interviews, or related case investigations will continue to be referred to USAOs where the evidence is located, and the USAO in the Northern District of California will need to deal directly with ISPs on novel or particularly complex issues. But centralization will significantly reduce the delays and redundancy in the handling the vast majority of MLA requests.

OIA has engaged in a pilot project, with the support and expertise of the Criminal Division’s Computer Crime and Intellectual Property Section (CCIPS) and the USAO in the District of Columbia to refine and centralize the process. Based upon the experience with a centralized

process in OIA's pilot project, time for executing legally sufficient, straightforward requests for subscriber and transactional information would be reduced. With respect to requests for content of communications requiring a probable cause standard, which now take up to one year to execute, OIA expects that additional, adequate resources would cut response time in half.

2. Training and Outreach:

Training our foreign counterparts, particularly ones from different legal systems, will be critical to improving the MLAT process. Many foreign partners require assistance in showing that the probable cause standard required to receive the content of communications is met. The Department of Justice – OIA, CCIPS and the FBI – will develop a comprehensive program to train foreign authorities in U.S. legal standards for obtaining evidence and in cyber investigations.

OIA would also train its own attorneys, particularly the ones hired specifically to work on MLAT modernization, and work with the AUSAs in the USAOs in the District of Columbia and the Northern District of California to secure uniformity and guidelines for review and tracking.

Additionally, DOJ, with the Department of State, would engage in outreach with foreign governments and encourage them to empower their MLAT “Central Authorities” (or equivalents) so that they can screen their own requests for evidence located in the United States and help their prosecutors and law enforcement agencies in making MLA requests that meet U.S. legal standards.

By focusing training on high-volume MLAT partners who have particular difficulty in meeting U.S. legal standards and working with sophisticated partners who are already eager to engage in improving MLAT success, the quality of the requests received should improve and result in faster processing times. OIA would assign DOJ Attachés to work directly with foreign counterparts in countries such as Brazil and Turkey, as well as other important partners such as Germany, the Dominican Republic, Australia and Eastern Europe. These in-country attachés would be able to work directly with foreign counterparts, as well as U.S. Embassy law enforcement agency attachés, to resolve problems and address legal and treaty issues in complex and urgent cases before requests are sent to OIA, and to provide consistent, hands-on advice to cure systemic problems.

3. Reducing the Backlog and Improving Response Times:

Additional resources also are needed to address the current backlog of pending MLA requests. With those resources, OIA would staff an “intake unit” to handle all incoming MLA requests. Additional personnel resources would directly reduce response time.

Once adequately staffed, OIA would strive first to reduce its pending case levels to its 2008 low of approximately 7,500. This would include reducing backlogs of cases at both at OIA and among cases already awaiting action at USAOs. It is expected that the additional resources would, over time, allow OIA to eliminate the backlog, so that the number of cases closed in a given year will match (if not exceed) the number of new cases opened. These additional

attorneys will not only handle any existing backlog, but will also take on new MLAT and extradition requests, and some will be dedicated to supporting the necessary operation of the office, including legislative and policy development, litigation, and management.

4. Improved Technology:

New technology is vital to modernize OIA's case tracking and management system, with an estimated expense of \$3 million per year for three years. With additional resources, OIA would: (a) update its neglected internal website used currently by OIA and others within DOJ; (b) establish an external website of resources and email interface for foreign users; (c) fund in-house technological and analytic resources to manage those systems and keep them current; and (d) provide online advice and exemplars for foreign partners to accept MLAT requests electronically (beyond the email and PDF capacities now in use) and allow for automated status updates.

Conclusion

The MLAT handling process must be overhauled in a comprehensive and responsible manner to address the globalization of crime and growth of electronic communications, and to ensure U.S. law enforcement retains the ability to seek reciprocal assistance from foreign partners. Just as critical is our need to safeguard U.S. security and economic interests that have become threatened by foreign frustration with a U.S. predominance of the Internet that is coupled with a perceived U.S. unresponsiveness to foreign authorities' need for U.S.-based evidence.

Impact on Performance

The requested positions will allow the Division to implement the four elements — (1) centralization, (2) training and outreach, (3) reducing the backlog, and (4) technology improvement—that the Department has identified as required to modernize the handling of MLA requests. Because MLA requests involve numerous types of crime, including terrorism and threats to our national security, child exploitation, financial fraud, transnational organized crime, and cybercrime, fulfilling this request will contribute to accomplishing many performance objectives of the Department.

Funding

Base Funding

FY 2014 Enacted				FY 2015 Enacted				FY 2016 Current Services			
Pos	atty	FTE	\$(000)	Pos	atty	FTE	\$(000)	Pos	atty	FTE	\$(000)
90	61	82	\$19,550	90	61	82	\$19,982	90	61	82	\$21,280

Personnel Increase Cost Summary

Type of Position/Series	Modular Cost per Position (\$000)	Number of Positions Requested	FY 2016 Request (\$000)	FY 2017 Net Annualization (change from 2016) (\$000)	FY 2018 Net Annualization (change from 2017) (\$000)
Clerical and Office Services (0300-0399) (Full Year Clerical)	\$101	2	\$202	\$0	\$0
Clerical and Office Services (0300-0399) (Full Year Professional)	\$168	5	\$840	\$0	\$0
Attorneys (0905) (Full Year Domestic)	\$232	70	\$16,240	\$0	\$0
Attorneys (0905) (Full Year Foreign)	\$740	7	\$5,180	\$0	\$0
Paralegals / Other Law (0900-0999) (Full Year)	\$168	57	\$9,576	\$0	\$0
Total Personnel		141	\$32,038	\$0	\$0

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2016 Request (\$000)	FY 2017 Net Annualization (change from 2016) (\$000)	FY 2018 Net Annualization (change from 2017) (\$000)
IT Equipment	N/A	N/A	\$0	\$500	\$0
Travel	N/A	N/A	\$73	\$0	\$0
Foreign Service National	\$60	7	\$0	\$420	\$0
Total Non-Personnel	N/A	N/A	\$73	\$920	\$0

Total Request for this Item

	Pos	Atty	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)	FY 2017 Net Annualization (change from 2016) (\$000)	FY 2018 Net Annualization (change from 2017) (\$000)
Current Services	90	61	82	\$21,280	\$0	\$21,280	\$0	\$0
Increases	141	77	141	\$32,038	\$73	\$32,111	\$920	\$0
Grand Total	231	138	223	\$53,318	\$73	\$53,391	\$920	\$0

V. Program Increases by Item

Item Name: **International Law Enforcement and Justice Development**

AG Targeted Priority Options:

AG Priority Goals	Protecting Americans from national security threats
	Protecting Americans from violent crime
	Protecting Americans from healthcare and financial fraud
	Protecting the most vulnerable members of society

Strategic Goals and Strategic Objectives:

Goal One: Prevent Terrorism and Promote the Nation’s Security Consistent with the Rule of Law	1.1 Prevent, disrupt, and defeat terrorist operations before they occur by integrating intelligence and law enforcement efforts to achieve a coordinated response to terrorist threats
	1.2 Prosecute those involved in terrorist acts
	1.4 Combat cyber-based threats and attacks through the use of all available tools, strong public-private partnerships, and the investigation and prosecution of cyber threat actors
Goal Two: Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law	2.1 Combat the threat, incidence, and prevalence of violent crime by leveraging strategic partnerships to investigate, arrest, and prosecute violent offenders and illegal firearms traffickers
	2.2 Prevent and intervene in crimes against vulnerable populations and uphold the rights of, and improve services to, America’s crime victims
	2.3 Disrupt and dismantle major drug trafficking organizations to combat the threat, trafficking, and use of illegal drugs and the diversion of illicit drugs
	2.4 Investigate and prosecute corruption, economic crimes, and transnational organized crime
	2.5 Promote and protect American civil rights by preventing and prosecuting discriminatory practices
Goal Three: Ensure and Support the Fair, Impartial, Efficient, and Transparent Administration of Justice at the Federal, State, Local, Tribal, and International Levels	3.1 Promote and strengthen relationships and strategies for the administration of justice with law enforcement agencies, organizations, prosecutors, and defenders through innovative leadership and programs
	3.6 Prevent and respond to genocide and mass

	atrocities and ensure that perpetrators of such crimes are held accountable in the United States, and if appropriate, their home countries
--	--

Budget Decision Unit: Enforcing Federal Criminal Laws
Organizational Program: Criminal Division

Program Increase: Positions 107 Atty 13 FTE 83 Dollars 12,434,000

Description of Item

The Criminal Division is requesting 107 positions, including 13 attorneys, 83 FTE, and \$12,434,000 to fully fund the headquarters operating expenses of its International Criminal Investigative Training Assistance Program (ICITAP), the Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT), and the Office of Administration’s International Training and Financial Management unit (ITFM), which solely supports the financial management and execution of ICITAP’s and OPDAT’s programs.

Justification

ICITAP’s and OPDAT’s headquarters operations are vital to the funding, origination, development, oversight, management, and implementation of DOJ’s foreign assistance programs. Without the efforts of headquarters personnel – who participate in a myriad of interagency initiatives, develop program plans and proposals, ensure funding and oversight for program implementation, liaise with international partners, apply extensive institutional knowledge of justice sector standards and development assistance best practices, and advocate on behalf of the Attorney General – the Department would have no voice in Security Sector Assistance (SSA) and related rule of law and governance assistance discussions and decision-making. Indeed, without such efforts, there would be no DOJ overseas technical assistance programs, significantly undermining our national security goals.

As presently structured, a majority of funding for the headquarters and field operations of both sections comes from Interagency Agreements and the overhead provided for in this agreements. Currently, only senior management for ICITAP and ICITAP are funded out of departmental resources. No Department funds are budgeted for headquarters operations, including headquarters staff salaries, office space (including furnishings, rent, and utilities), information technology, and security needs. The budget items requested are solely for the support of the base headquarters operations of ICITAP and OPDAT, such as headquarters salaries, office space, and related headquarters business needs. The budget items requested are not for assistance programs, which would continue to be funded through Interagency Agreements.

Base operating budgets for ICITAP and OPDAT headquarters are essential to the Department’s ability to fulfill its critical new role and increased responsibilities under Presidential Policy Directive 23 on Security Sector Assistance (PPD-23), which significantly advances the Department’s own priorities and builds upon OPDAT and ICITAP’s solid track record. Base budgets will enable the Department to maintain a core group of experienced justice sector assistance experts at ICITAP and OPDAT to: 1) sustain a consistent presence in ongoing interagency SSA policy, strategic planning, and program development activities; 2) participate in

interagency assessments and deftly manage implementation of SSA in priority countries; and 3) be at the ready to swiftly and effectively respond in times of crisis or emergency.
Current Funding Source Is Unpredictable and Undermines Mission Objectives

The current funding model for the headquarters operation of ICITAP and OPDAT relies completely upon funding allocated as the result of negotiated percentages of each Interagency Agreement (IAA) with its funders, primarily the Department of State (State).

Funding ICITAP and OPDAT headquarters' operations as a percentage of each individual agreement has proven to be very unpredictable and, therefore, inefficient. In any given year, these two offices – and accordingly the Division and the Department – are unsure how much funding they will have to operate. Furthermore, the timing, planning, and focus of the offices' assistance programs are almost totally dependent on the priorities of the funding agencies, which prevents the Division from fully and timely leveraging its expertise as it relates to the justice sector and rule of law priorities of the Department.

In underwriting the annual headquarters operating expenses of ICITAP and OPDAT, the Department of Justice will establish a stable funding source for its overseas SSA and related rule of law and good governance initiatives, in support of the U.S. government's national security missions and foreign policy priorities.

Presidential Policy Directive 23 on Security Sector Assistance (PPD-23)

Through ICITAP and OPDAT, the Department of Justice plays a central role in the policy formulation, strategic development, and implementation of global assistance programs that further U.S. national security interests. As described below, PPD-23 calls for an integrated interagency approach to international security sector assistance. For this reason, one of the Department's three strategies to achieve Objective 1.1 of the Department of Justice Strategic Plan for 2014-2018 is to "Build and maintain a Security Sector Assistance (SSA) workforce aimed at strengthening the ability of the United States to promote national security by assisting allies and partner nations to build their own security capacity." The two components most responsible for Department of Justice SSA to partner nations are ICITAP and OPDAT. It is therefore incumbent on the Department of Justice to maintain and secure the base operations of ICITAP and OPDAT in order to achieve Objective 1.1 and to meet its commitments under PPD-23.

PPD-23, which was signed by President Obama on April 5, 2013, mandates a whole-of-government approach to the government's policy development, strategic planning, engagement, and implementation of international SSA. The Directive is "aimed at strengthening the ability of the United States to help allies and partner nations build their own security capacity, consistent with the principles of good governance and the rule of law." SSA, as defined in PPD-23, includes assistance to international partners who are "state security and law enforcement providers, government security and justice management and oversight bodies, civil society, institutions responsible for border management, customs and civil emergencies, and non-state justice and security providers."

As set forth in PPD-23, the Department of Justice, along with the Departments of Homeland Security and Treasury, is a presumptive implementer of SSA in areas “involving [those agencies’] expertise, experience, or counterpart ministries, agencies, or equivalents,” including counterterrorism and justice sector matters. In addition to implementation responsibilities, the Department of Justice is expected to be a full participant in policy formulation, as well as assistance program planning and development. This is consistent with the whole-of-government approach articulated in the National Security Strategy, the State Department’s 2010 Quadrennial Diplomacy and Development Review (QDDR), and the Presidential Policy Directive 6 on Global Development.

The Department currently participates in a broad array of interagency initiatives that address security sector interests, as well as complementary rule of law and good governance issues. As PPD-23 is implemented, there will be increased demands on the Department to actively participate in ongoing interagency policy formulation, strategic planning, assessment, program design, and SSA delivery. While the Department of State will lead the implementation of PPD-23, the Department of Justice plays a critical role in the development and implementation of SSA policy, planning, and programming.

In order to meet its responsibilities and duties under PPD-23, the Department must seek critical funding for the primary components responsible for leading its SSA efforts: ICITAP and OPDAT. A base budget for two offices will enable the Department of Justice to be a full participant in the ongoing interagency SSA process and thereby fulfill the mandates of PPD-23. At the same time, it will allow the Department to form SSA policy, as well as to design and implement SSA programs in priority countries in a manner that significantly advances the Department’s strategic goals listed above.

ICITAP and OPDAT are recognized within the interagency realm and by foreign counterparts as having a longstanding record of excellence in the area of SSA, and they thus provide an existing, credible platform upon which the Department can build its capacity to deliver SSA in accordance with PPD-23. Both organizations possess highly qualified and experienced headquarters personnel with significant expertise in developing and implementing effective and sustainable overseas SSA and related assistance in the rule of law and governance areas. No other components within the Department of Justice currently provide this expertise and function for the Department.

Specifically, ICITAP furnishes development assistance and training to foreign police, criminal and anticorruption investigative entities, forensic laboratories, and correctional systems. OPDAT helps to develop sustainable foreign justice sector institutions, including prosecutors and courts, and legislation consistent with international standards. Jointly, ICITAP and OPDAT strengthen the capacities of foreign criminal justice institutions to work together to both prevent and reduce transnational crime and terrorism and to ensure the fair, effective, and secure administration of justice. They promote evidence-based investigations and prosecutions, the safeguarding of human rights, and adherence to international norms and best practices. Further, ICITAP and OPDAT work together to harness the expertise of other Department components and offices to provide cohesive policy and program development and implementation. ICITAP

and OPDAT ultimately help to establish interoperability and cooperation between the U.S. and foreign criminal justice systems.

Currently, the combined global reach of ICITAP and OPDAT spans 88 countries worldwide. In over 40 countries, ICITAP and OPDAT have established field offices and deployed federal staffs who serve as members of the U.S. embassy team. These individuals are subject matter experts who work with the host country to achieve complex objectives, such as the creation and passage of new legislation and the development of new law enforcement policies and procedures based on new or existing laws and international standards. These subject matter experts develop country-specific knowledge of law enforcement capabilities and culture and establish meaningful relationships with local law enforcement and government officials.

Such relationships are critical to developing strong international partners for the Department of Justice. Crimes committed in the United States often have ties to networks or operations in other countries. To address these threats, the partnerships developed by ICITAP and OPDAT enable DOJ to combat transnational crime, including terrorism, at its source in line with Goal 3 of the Department's FY2014-18 Strategic Plan, and, in particular, Objective 3.1.

ICITAP and OPDAT Protect and Promote National Security

The development of the capacity of foreign justice components – including police, prosecutorial, forensics, and corrections services – is not simply a matter of foreign assistance; it is also a matter of our national security. Properly conducted, such development helps protect the United States in two ways: first, it provides the foreign country with the means to investigate and prosecute terrorism and transnational crime, before it reaches the borders of the United States; and second, it provides the United States with effective foreign law enforcement partners on whom we can draw to address terrorism and transnational criminal issues that do reach the United States. The national security interests of the United States in this regard are particularly vital when the foreign countries in question are ones that require significant reconstruction and stabilization, for it is precisely these countries that can become havens for transnational crime and terrorism.

Consistent with PPD-23, the Department, through the Criminal Division, and specifically through ICITAP and OPDAT, is appropriately playing an ever-increasing and central role in U.S. government-funded international SSA programs and associated rule of law development initiatives. This central role strengthens the Department's ability to achieve the top priority goal of its FY 2014-18 Strategic Plan: "Protect Americans from terrorism and other threats to National Security." To perform this role effectively at home and abroad, the Division must maintain a permanent capacity to manage these complex global programs. The Division's knowledge and expertise – not only in the development of international best practices, but also in the establishment of critical relationships with foreign law enforcement and criminal justice sector counterparts through ICITAP and OPDAT – are inextricably linked to and underpin the Department's efforts to investigate and prosecute terrorists and international criminal groups.

Permanent Funding Source Will Enable the Division to Fulfill Mission Objectives

Because of their longstanding, unique expertise and experience in international justice sector development assistance, ICITAP and OPDAT are best suited to lead in SSA and related international rule of law and good governance efforts. With permanent funding, ICITAP and OPDAT will, for the first time, establish a stable platform for planning and implementing criminal justice reform and capacity building programs abroad, ensuring the consistent use of best practices and also maximizing the influence of the Department's resident knowledge and expertise in key policy and strategic decision-making regarding SSA and related rule of law matters. Most importantly, this would demonstrate the Department of Justice's commitment to lead and coordinate overseas justice sector and rule of law activities, in line with the directives of PPD-23, as a full partner of the Department of State and other agencies engaged in this whole-of-government endeavor.

The requested funds would also permit both sections to maintain the appropriate level of staffing to enable the Criminal Division to carry out critical coordinating functions and other responsibilities in support of national security and other high priority international law enforcement initiatives such as:

- **Partnerships in Africa and the Middle East.** In the aftermath of the “Arab Awakening” and in response to increased activities by extremist groups in the Sahel, ICITAP and OPDAT are helping U.S. allies in this critical region fight terrorism, counter violent extremism, and sustain moderate, secular institutions. An example of ICITAP and OPDAT's efforts to build these partnerships is a recently developed asset recovery project under the auspices of the Deauville Partnership with Arab Countries in Transition, which was implemented in partnership with the Asset Forfeiture and Money Laundering Section. Furthermore, in cooperation with other USG agencies, donor nations, and the Syrian authorities, ICITAP and OPDAT are leveraging their considerable post-conflict experience and expertise to engage in an institutional development program for Syria, designed to create a fair and competent criminal justice sector that will protect Syrian democracy and serve as an effective partner with the U.S. justice sector.
- **Strategy to Combat Transnational Organized Crime.** On July 25, 2011, the National Security Staff released its *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security*. Priority 6 of the Strategy is to promote the development of criminal justice capacities on a worldwide basis, to the point where international law enforcement capabilities and cooperation among states are self-sustaining.
- **Global Counterterrorism Forum (GCTF).** Launched in September 2011, the GCTF is an informal multilateral counterterrorism (CT) platform, with 30 member states, that regularly convenes key CT policymakers and practitioners from around the globe. With its primary focus on countering violent extremism and strengthening criminal justice and other rule of law institutions necessary to prevent and counter terrorism, the GCTF aims to diminish terrorist recruitment and increase the number of countries capable of dealing with terrorist and related security threats within their borders and regions. The Department has been an active participant in the GCTF since its inception and has played a key role in the GCTF's Criminal Justice Working Group. The Working Group's

signature contribution to date is the *Rabat Memorandum of Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector*. The Department is currently implementing capacity building programs to address specific good practices articulated in the Rabat Memorandum. Working with the Department of State Counterterrorism Bureau (S/CT) and the United Nations Interregional Crime and Justice Research Institute (UNICRI), the Department also produced a document that enumerates and promotes a number of “best practices” for terrorist rehabilitation and reintegration programs in prisons. This document, formally known as the “Rome Memorandum of Good Practices for the Rehabilitation and Reintegration of Violent Extremist Offenders,” was endorsed by the 30 foreign GCTF member countries at the June 2012 GCTF Ministerial.

- **Supplemental Terrorism Funding.** The Criminal Division continues to serve as a ready resource to develop the capacity of foreign counterparts in countries that are key allies in thwarting terrorism, including capacity building in the areas of anti-money laundering, combating the financing of terrorism, and cybersecurity.

Without permanent base funding for ICITAP and OPDAT, the Division will not be able to support ongoing projects, if funding streams decline or if the timing of the receipt of new agreements lags. Additionally, the ebb and flow created by the current uneven funding process will create undue inefficiencies and loss of institutional capabilities. Worse, the Department and the Division will play a less active role in international rule of law development and justice sector capacity building programs, which will negatively impact our law enforcement personnel and prosecutors as they pursue criminals in foreign countries and attempt to bring them to justice either in the United States or abroad.

Further, because ICITAP and OPDAT must rely on IAAs to fund a majority of their headquarters’ expenses, the lack of a predictable funding source for ICITAP and OPDAT compromises the Division’s ability to build and maintain the organizational capacity to support future initiatives, implement law enforcement strategies, and perform essential headquarters functions. Additionally, if this continues, it will leave the State Department with only one option: turn to private contractors who, in many cases, are inexperienced and unfamiliar with U.S. government policy positions and legislative drafting standards, and who are often mistakenly perceived as representing or speaking on behalf of U.S. law enforcement. Among the many serious consequences of this practice is the loss to the Division and the Department of critical opportunities to build the very strategic partnerships between the U.S. and foreign law enforcement that the Department’s own current strategic plan highlights as essential to prosecuting transnational crime and terrorism.

Impact on Performance

The Division’s international training and development programs, ICITAP and OPDAT, together provide unique and significant roles and functions that support and advance the Department’s 2014-2018 Strategic Plan, specifically *Goal One: Prevent Terrorism and Promote the Nation’s Security Consistent with the Rule of Law; Goal Two: Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law; and Goal 3: Ensure and Support the Fair,*

Impartial, Efficient, and Transparent Administration of Justice at the Federal, State, Local, Tribal, and International Levels.

The Department of Justice will continue to play an increasing leadership role in the U.S. government's foreign assistance process at all stages. This is consistent with the Attorney General's role and responsibility as the chief law enforcement officer of the federal government and with his responsibilities on national security issues. As highlighted in the Department's Strategic Plan, the Department is "committed to expanding the scope and depth of international partnerships by enhancing collaboration; helping to establish rule of law through international treaties and training and assistance; and using international working groups to foster communication to enhance investigations, intelligence sharing, and threat awareness." Moreover, as directed by the President in PPD-23, the Department is now a full participant in the planning, assessment, program design, and implementation of interagency security sector assistance. The Criminal Division needs to be ready when called upon to act.

The work of the Criminal Division unquestionably furthers and strengthens the strategic goals of both the Department of Justice and the U.S. Government in preventing and combating transnational crime, building strong international partners, and institutionalizing criminal justice sector best practices and rule of law on a global scale. The Department will significantly strengthen its position in USG planning, development, and implementation of international justice sector development if it is able to fully fund its existing institutional capacity for overseas rule of law development: namely, ICITAP's and OPDAT's base budgets. If ICITAP's and OPDAT's headquarters' operations are not funded, the Department will neither be able to enlarge its role nor ensure its current level of involvement in rule of law development missions in the future.

Funding

Base Funding

FY 2014 Enacted				FY 2015 Enacted				FY 2016 Current Services			
Pos	atty	FTE	\$(000)	Pos	atty	FTE	\$(000)	Pos	atty	FTE	\$(000)
12	6	10	\$2,530	12	6	10	\$2,586	12	6	10	\$2,758

Personnel Increase Cost Summary

Type of Position/Series	Modular Cost per Position (\$000)	Number of Positions Requested	FY 2016 Request (\$000)	FY 2017 Net Annualization (change from 2016) (\$000)	FY 2018 Net Annualization (change from 2017) (\$000)
Clerical and Office Services (0300-0399) – Encumbered Expert Professional	\$186	5	\$930	\$150	\$0
Clerical and Office Services (0300-0399) – NEW Expert Professional	\$99	11	\$1,089	\$957	\$330
Clerical and Office Services (0300-0399) – Encumbered Professional	\$110	24	\$2,640	\$1,248	\$0
Clerical and Office Services (0300-0399) – NEW Professional	\$66	26	\$1,716	\$1,144	\$1,352
Clerical and Office Services (0300-0399) – Encumbered Clerical	\$81	2	\$162	\$30	\$0
Clerical and Office Services (0300-0399) – NEW Clerical	\$58	3	\$174	\$114	\$0
Accounting and Budget (0500-0599) – Encumbered Expert Professional	\$186	2	\$372	\$60	\$0
Accounting and Budget (0500-0599) – Encumbered Professional	\$110	8	\$880	\$416	\$0
Accounting and Budget (0500-0599) – NEW Professional	\$66	7	\$462	\$308	\$364
Attorneys (0905) - Encumbered	\$234	13	\$3,042	\$0	\$0
Business & Industry (1100-1199) – Encumbered Expert Professional	\$186	2	\$372	\$60	\$0
Business & Industry (1100-1199) – Encumbered Professional	\$110	1	\$110	\$52	\$0
Forensic/Physical Sciences (1300-1399) – NEW Expert Professional	\$99	1	\$99	\$87	\$30
Education/Training (1700-1799) – Encumbered Expert Professional	\$186	1	\$186	\$30	\$0
Travel Services (2101) – Encumbered Professional	\$110	1	\$110	\$52	\$0
Total Personnel		107	\$12,344	\$4,708	\$2,076

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2016 Request (\$000)	FY 2017 Net Annualization (change from 2016) (\$000)	FY 2018 Net Annualization (change from 2017) (\$000)
Travel	N/A	N/A	\$90	\$0	\$0
Total Non-Personnel	N/A	N/A	\$90	\$0	\$0

Total Request for this Item

	Pos	Atty	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)	FY 2017 Net Annualization (change from 2016) (\$000)	FY 2018 Net Annualization (change from 2017) (\$000)
Current Services	12	6	10	\$2,758	\$0	\$2,758	\$0	\$0
Increases	107	13	83	\$12,434	\$90	\$12,434	\$4,708	\$2,076
Grand Total	119	19	93	\$15,192	\$90	\$15,282	\$4,708	\$2,076

V. Program Increases by Item

Item Name: Strategic Initiatives to Address to Cyber Threats

AG Targeted Priority Options: Protecting Americans from national security threats

Strategic Goal:

<p>Goal One: Prevent Terrorism and Promote the Nation’s Security Consistent with the Rule of Law</p>	<p>1.4 Combat cyber-based threats and attacks through the use of all available tools, strong public-private partnerships, and the investigation and prosecution of cyber threat actors</p>
<p>Goal Two: Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law</p>	<p>2.4 Investigate and prosecute corruption, economic crimes, and transnational organized crime</p>

Budget Decision Unit(s): Enforcing Federal Criminal Laws

Organizational Program: Criminal Division

Program Increase: Positions 54 Atty 24 FTE 29 Dollars \$6,123,000

Description of Item

Cyber threats continue to evolve and the harm they cause – both in terms of financial loss and their impact on security and privacy – continues to mount. In its recent Cyber Threat Strategic Report to Congress (March 16, 2014), the Department declared that it places a high priority on responding to these threats and identified six strategic initiatives that the Department must pursue. The Criminal Division will play a central role in each of these initiatives: it is best situated to provide training to investigators and attorneys on cybercrime and digital evidence; it can enhance the number and capacity of digital forensic experts; it provides technical and legal expertise throughout the Department; it promotes information sharing efforts with the private sector; it builds and strengthens relationships with foreign law enforcement partners, which are critical to the sharing of electronic evidence; and it excels at the development of sound cyber policy. In order to fulfill this critical role, the Division requires an increase of 54 positions (24 attorneys), 29 FTE, and \$6,123,000.

Justification

Threats to the nation's computer networks and cyber systems continue to evolve, as do the nature and capabilities of those responsible for the threats. Cybercrime has increased dramatically over the last decade, and our financial infrastructure has suffered repeated cyber intrusions. It has become far too commonplace an occurrence that our email accounts are hijacked, our financial information siphoned away, and our personal information compromised. The technology revolution – which has brought enormous benefits to individuals, U.S. companies, and the U.S. economy as a whole – has also facilitated these criminal activities, making available a wide array of new methods that identity thieves can use to access and exploit the personal information of others. Skilled criminal hackers are now able to perpetrate large-scale data breaches that leave, in some cases, tens of millions of individuals at risk of identity theft. Today's criminals, who often sit on the other side of the world, can hack into computer systems of universities, merchants, financial institutions, credit card processing companies, and data processors to steal large volumes of sensitive and valuable information. They then peddle the stolen information to other criminals, use the information for their own financial gain, or sometimes even terrorize and extort their victims.

In December 2013, Target, the second-largest U.S. discount chain, announced that credit and debit card data for as many as 40 million consumers were compromised. Target then disclosed on January 10, 2014 that thieves had also accessed the personal information, including names, phone numbers, home addresses, and/or email addresses, of as many as 70 million people – information that is valued by criminals because it can be used to lure victims with fake emails or hack into other accounts. A few days later, retailer Neiman Marcus Inc. reported that it also was the victim of a suspected cyberattack over the holidays in which some of its customers' credit card information may have been stolen. Target and Neiman Marcus are just two of the latest known victims.

Criminal hacking can have serious consequences even when conducted on a smaller scale or where not committed for financial gain. The Department has vigorously pursued hackers who have used the Internet to invade Americans' privacy. In 2011, for example, the FBI successfully investigated a hacker named Luis Mijangos. He infected the computers of victims with malicious software that gave him complete control over their computers. He deliberately targeted teens and young women, reading their emails, turning on their computer microphones and listening to conversations taking place in their homes, and, most importantly for him, watching them through their webcams as they undressed. Even more disturb, Mijangos then extorted certain victims by threatening to post intimate pictures on the Internet unless the victims provided him with even more salacious images or videos of themselves. When one victim shared Mijangos' threats with a friend, Mijangos retaliated by posting nude pictures of the victim on her friend's social networking page. At the time of his arrest, FBI computer forensics experts had determined that Mijangos had infected more than 100 computers that were used by approximately 230 individuals, at least 44 of them minors. The Court sentenced Mijangos to 72 months in federal prison.

The Justice Department is vigorously responding to hacking and other cybercrimes through the tenacious work of the Criminal Division's Computer Crime and Intellectual Property Section,

also known as CCIPS, which partners with Computer Hacking and Intellectual Property Coordinators in U.S. Attorney's Offices across the country as part of a network of almost 300 Justice Department cybercrime prosecutors. In addition to the direct investigation and prosecution of cybercrimes, the Division has provided extensive legal and policy guidance in furtherance of these goals. It has supported and trained the members of the National Security Cyber Specialist program – prosecutors focused on cyber threats from terrorists and foreign governments – both in the National Security Division and in U.S. Attorneys' Offices around the country. The Division has consistently led legislative development addressing emerging criminal threats to both the security of computer systems and networks and to the nation's intellectual property. It has engaged in complex legal reviews of tools and programs that protect critical government and private sector networks against security threats and attacks. Attacks on American companies that have been attributed to sophisticated criminal organizations and even foreign nations in recent months, causing many millions of dollars of damage, have only increased the interest in such legislation and legal reviews.

To further these efforts as well as to provide assistance to organizations seeking to protect themselves, the Criminal Division announced in December 2014 that it had created a dedicated Cybersecurity Unit within CCIPS, which will have responsibility on behalf of the Criminal Division for efforts to enhance public and private cybersecurity. Amid the growing complexity and volume of cyber attacks, prosecutors from the Cybersecurity Unit will provide a central hub for expert advice and legal guidance regarding the criminal electronic surveillance statutes for both U.S. and international law enforcement conducting complex cyber investigations to ensure that the powerful law enforcement tools are effectively used to bring the perpetrators to justice while also protecting the privacy of everyday Americans. This Unit will also work to ensure that the advancing cyber security legislation is shaped to most effectively protect our nation's computer networks and individual victims from cyber attacks. Because the private sector has proved to be a crucial partner in our fight against all types of online crime, prosecutors from the Cybersecurity Unit will be engaging in extensive outreach to facilitate cooperative relationships with our private sector partners. The resources sought in this request will help to expand the work and outreach of the Cybersecurity unit, and permit the lessons learned from ongoing investigations and prosecutions to be communicated to both public-sector and private-sector partners. These efforts will ultimately aid in public and private sector efforts to protect themselves from cyber threats and enable investigators and prosecutors across the country to hold those responsible to account.

The Criminal Division, through CCIPS, in conjunction with the FBI and the U.S. Attorneys' Offices in Pittsburgh and Omaha, used traditional law enforcement actions and innovative legal and technical measures to block and disrupt the ability of the two malware schemes. In April, 2014, these threats were neutralized by a combination of (a) court orders to authorize disruption of the malicious software, (b) the indictment of a key defendant, (c) the seizure of servers in 6 different countries by law enforcement partners, and (d) coordinated remediation by the Department of Homeland Security and private-sector partners. This dramatic result was made possible by the leadership and energies of CCIPS attorneys.

As cyber threats have expanded exponentially over the last decade, the investigative agencies have responded by doubling or tripling the number of agents assigned to cyber cases. Indeed, as

recently as FY 2014, the FBI received \$86.6 million and 152 positions (60 agents) in support of its Next Generation Cyber (NGC) initiative to increase victim engagement, improve cyber collection and analysis, and extend centralized capabilities to the field. It is essential that the number of prosecutors keeps pace with the resources the investigative agencies are dedicating to cyber cases.

On May 16, 2014, the Department transmitted to Congress a multiyear Cyber Threat Strategic Report. This report described the Department's decades-long efforts to address cyber threats and associated challenges; the structure of DOJ's cyber threat response; and DOJ's way forward to thwart cybercrime and cyber threats to the national security and other key targets. In order to accomplish this critical result, the Report identified six Strategic Initiatives:

- 1. Ensure that all of DOJ's investigators and attorneys receive training on cybercrime and digital evidence.*
- 2. Increase the number of digital forensic experts and the capacity of available digital forensic hardware.*
- 3. Enhance DOJ's expertise in addressing complex cyber threats.*
- 4. Improve information sharing efforts with the private sector.*
- 5. Expand and strengthen relationships with international law enforcement and criminal justice partners on cybercrime to enhance the sharing of electronic evidence.*
- 6. Enhance capacity in the area of cyber policy development and associated legislative work.*

The Division, through CCIPS, plays a central role in fulfilling each of these initiatives. The Division requires a budget enhancement to enable the Department to succeed in fulfilling this important mission.

1. Ensure that all of DOJ's investigators and attorneys receive training on cybercrime and digital evidence.

CCIPS has extensive experience conducting top-flight cyber training. CCIPS attorneys and technical experts have developed detailed courses on collecting electronic evidence, computer forensics for prosecutors, complex online crimes, and investigating and prosecuting the theft of trade secrets. These courses consistently receive excellent reviews. CCIPS provides annual training to CHIP prosecutors from across the country as well, through presentations at U.S. Attorneys' Offices. CCIPS creates manuals, develops briefing materials, sends out several monthly newsletters on cybercrime topics, and posts advice and FAQs on its intranet site (traffic to the site has grown dramatically). As nationally recognized experts on cybercrime and digital evidence, CCIPS will be central to the Department's goal of training its entire workforce.

In order to fulfill this initiative, the Division will require additional resources. CCIPS will create training materials, including video and other multimedia, and conduct a "train-the-trainers" program that could provide basic cyber training to prosecutors across the country. Advanced training will also be necessary, and CCIPS attorneys and digital investigative analysts are in the best position to supply it.

2. Increase the number of digital forensic experts and the capacity of available digital forensic hardware.

The Cyber Threat Strategic Report stated that “prosecutors and investigators must have additional support from appropriately trained digital analysis experts that are committed solely to the needs of the prosecutor, not only during the evolving investigative phase of cyber cases, but throughout trial preparation, trial, and sentencing.” It pointed out that this support must include:

- early assessment pre-seizure planning of digital evidence to address technical and legal complications;
- triage and in-depth examinations that recognize and address the complexities with the collection of evidence;
- a team approach with investigative agency forensic resources to provide more surgically tailored exams to identify critical pieces of digital evidence earlier in an investigation;
- expert consultation throughout the investigation and prosecution regarding digital evidence issues, including supplemental analysis to identify digital evidence artifacts in aid of the prosecution to anticipate or rebut defenses;
- assistance in trial preparation, including the development of innovative and accurate ways to present digital evidence, common technologies, and network processes at trial; and,
- support during trial, including consultation regarding defense expert testimony and assistance in responding to changing defense strategies.

The CCIPS Cybercrime Lab has advocated for just this sort of digital investigative capability, and it has shown the way forward by modeling the very type of digital forensic support that most effectively supports successful prosecutions. Yet the Report correctly noted that “[a]lthough the lab has proven to be a great asset to DOJ, its effectiveness is necessarily limited by its current size. DOJ must increase the size of the CCIPS Cybercrime Lab to ensure it can provide support for prosecutors handling legally and technically complex investigations and prosecutions.”

3. Enhance DOJ’s expertise in addressing complex cyber threats.

The Cyber Threat Strategic Report emphasized that the Department “must also enhance the expertise of its workforce regarding cyber threats and related cyber issues. Specifically, in light of the growth in number and complexity of cyber threats, DOJ must further develop two mutually supportive cadres of experts: First, it must increase the number of cyber experts that are available to respond to complex cyber threats, and ... [s]econd, DOJ needs to increase its capacity of experts focused on identifying and developing solutions to future cyber attacks.” The Criminal Division, through CCIPS, is ideally situated to play this important role (and indeed is explicitly identified as one such component in the Report). CCIPS has led the way in developing innovative prosecutorial strategies to respond to new and complex cyber threats. It has a unique combination of highly technical digital investigative analysts and specialized attorneys dedicated to the problems of cybercrime and digital evidence. It has effectively coordinated multi-district and international efforts to address global criminal enterprises. CCIPS has asserted a leadership role in efforts against botnets and malicious software (such as Gameover Zeus and Cryptolocker), illegal online marketplaces, and

criminal carding forums. Additional resources are necessary to allow CCIPS to continue to maintain that leadership role as these problems grow in complexity.

4. Improve information sharing efforts with the private sector.

The Cyber Threat Strategic Report recognized that the Department “must increase its focus on building and maintaining relationships with the private sector for the purpose of information sharing.” For example, early outreach to companies that store large amounts of credit card data and other sensitive personal information can make the difference, when the company later suffers a security breach, between a prompt report to law enforcement and no report at all. Expanding industry outreach would enhance the generation of cases, and – perhaps just as importantly – identify areas of particular need or importance so that resources can be focused on prosecutions that have the greatest impact.

Building and maintaining such relationships requires a sustained effort by attorneys with a deep understanding of the investigation and prosecution of cyber crime and the needs and motivations of business. With enhanced funding, the Division, through CCIPS, is the right component to meet this growing need.

5. Expand and strengthen relationships with international law enforcement and criminal justice partners on cybercrime to enhance the sharing of electronic evidence.

The Cyber Threat Strategic Report explained the critical role that foreign law enforcement plays in addressing cyber threats. Because so many cyber investigations involve evidence or offenders located in foreign countries, working with foreign law enforcement is often the only way to solve these crimes and bring offenders to justice. Criminals continue to use gaps and inefficiencies in international law enforcement capabilities to evade detection, attribution, and punishment.

The Division has long recognized this difficulty and has for years devoted significant resources to building relationships through robust training programs for foreign law makers and law enforcement officials to enhance their capacity to investigate cybercrime and collect electronic evidence. Using a balanced approach of frank policy discussions with countries that have similar capabilities, combined with multilateral training initiatives aimed at countries whose legal or technical infrastructure to address cyber threats is at an earlier developmental stage, the Division has improved the capacity to address cybercrime around the world. CCIPS attorneys lead efforts in Africa, Eastern Europe, and Latin America, including through multi-lateral organizations such as the Organization of American States and the Asia-Pacific Economic Cooperation. As computer infrastructures expand in developing countries, and offenders who victimize Americans inevitably follow, the need for this sort of international engagement continues to grow.

CCIPS is ideally situated to fulfill this role, but has already had difficulty meeting the current demand. With additional resources, the Division, through CCIPS, will reach out more effectively to foreign law enforcement partners to expand and strengthen these key relationships.

6. Enhance capacity in the area of cyber policy development and associated legislative work.

The Cyber Threat Strategy Report emphasized that the Department must “maintain and further develop specialized personnel responsible for addressing policy issues in legislative and interagency forums.” Such personnel will permit the Department to contribute its expertise to the development and implementation of the Administration’s directives, executive orders, initiatives, and legislative proposals related to cyber threats, cybersecurity, and investigative tools. The Department “must provide leadership in policy issues that arise in interagency policy-making discussions of cyber issues.”

The Department also needs to continue to examine ways to expand the use of existing tools to counter the cyber threat. Together with network operators, the Department “will pursue policies that promote creative solutions to the challenge of cybersecurity, consistent with the Department’s commitment to protecting privacy and civil liberties.” It will work collaboratively with Congress and the Federal Rules Committee on changes to legislation and procedural rules that affect DOJ’s ability to detect, deter, and disrupt cyber threats.

Once again, the Division is the best place to develop personnel expert in cyber policy. CCIPS has drafted and negotiated cyber legislation, developed amendments to modernize the Federal Rules of Procedure, played a key role in Administration policy development, assisted in the development of national security and cybersecurity policies, and provided expert legal advice on a wide range of cyber issues. The Division needs additional resources in order to play a central role in fulfilling this important initiative.

Impact on Performance

Each additional Criminal Division attorney, laboratory professional, and related support position dedicated to this effort will have a widespread impact on the Department’s ability to successfully prosecute cyber criminals, use digital evidence, and share information with the private sector. By training investigators and prosecutors, by developing relationships with foreign law enforcement partners, and by serving as a center of expertise, investment in CCIPS helps cyber investigators and prosecutors across the country succeed.

Increases in the seriousness of the threat and the investigative resources devoted to addressing it have caused commensurate increases in the Division’s cyber workload – yet the resources devoted to it have not. To reverse this trend, and to fulfill the Department’s strategic initiatives, the Criminal Division must receive increased resources.

Funding

Base Funding

<i>FY 2014 Enacted</i>				<i>FY 2015 Enacted</i>				<i>FY 2016 Current Services</i>			
Pos	atty	FTE	\$(000)	Pos	Atty	FTE	\$(000)	Pos	atty	FTE	\$(000)
122	79	96	\$28,414	118	76	92	\$27,984	118	76	92	\$29,763

Personnel Increase Cost Summary

Type of Position/Series	Modular Cost per Position (\$000)	Number of Positions Requested	FY 2016 Request (\$000)	FY 2017 Net Annualization (change from 2016) (\$000)	FY 2018 Net Annualization (change from 2017) (\$000)
Clerical and Office Services (0300-0399)	\$66	2	\$132	\$88	\$104
Clerical and Office Services (0300-0399)	\$58	3	\$174	\$114	\$0
Attorneys (0905)	\$117	24	\$2,808	\$2,616	\$0
Paralegals / Other Law (0900-0999)	\$66	13	\$858	\$572	\$676
Information Technology Mgmt (2210)	\$99	12	\$1,188	\$1,044	\$360
Total Personnel		54	\$5,160	\$4,434	\$1,140

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2016 Request (\$000)	FY 2017 Net Annualization (change from 2016) (\$000)	FY 2018 Net Annualization (change from 2017) (\$000)
Equipment	N/A	N/A	\$900	\$0	\$0
Travel	N/A	N/A	\$63	\$0	\$0
Total Non-Personnel	N/A	N/A	\$963	\$0	\$0

Total Request for this Item

	Pos	Atty	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)	FY 2017 Net Annualization (change from 2016) (\$000)	FY 2018 Net Annualization (change from 2017) (\$000)
Current Services	118	76	92	\$29,763	\$0	\$29,763	\$0	\$0
Increases	54	24	29	\$5,160	\$963	\$6,123	\$4,434	\$1,140
Grand Total	172	100	121	\$34,923	\$963	\$35,886	\$4,434	\$1,140

V. Program Increases by Item

Item Name: Intellectual Property Enforcement

Strategic Goal

Goal Two: Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law	2.4 Investigate and prosecute corruption, economic crimes, and transnational organized crime
--	--

Budget Decision Unit(s): Enforcing Federal Criminal Law

Organizational Program: Criminal Division

Program Increase: Positions 11 Atty 7 FTE 6 Dollars \$2,205,000

Description of Item

The Criminal Division requests an enhancement of 11 positions (including 7 attorneys), 6 FTE, and \$2,205,000 to place two DOJ Attachés overseas to fight transnational crime, with particular emphasis on intellectual property crime. These DOJ Attachés will serve as regional International Computer Hacking and Intellectual Property coordinators (ICHIPs) and will be well positioned to combat the increasing threat of transnational intellectual property crime. The Criminal Division also requests that a portion of this enhancement be used to increase the capacity of the Division's domestic IP program to provide critical support to the ICHIP/Attachés and ensure the coordinated use of ICHIP resources overseas.

Support of the Department's Strategic Goals

The requested enhancement will support Goal Two: Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law (Objective 2.4: Investigate and prosecute corruption, economic crimes, and transnational organized crime). The Division has been involved developing the Department's strategy to enforce intellectual property laws and will continue to play a critical role implementing these strategies and objectives moving forward.

Justification

Protecting intellectual property rights is essential to safeguarding confidence in our economy, creating economic growth, and ensuring integrity, fairness, and competitiveness in the global marketplace. In today's environment, however, where virtually every significant intellectual property crime investigated and prosecuted in the United States has an international component, it is impossible to address intellectual property crime adequately without significant and strong international engagement.

The Department of Justice has long recognized that intellectual property crime, including offenses involving copyrights, trademarks and trade secrets, among others, not only has a significant international component but in many cases also has a substantial overlap with other economic crimes, including those related to cyber offenses, money laundering and tax evasion, and smuggling. Because the vast majority of intellectual property and other computer crimes originate in other countries, the Department has made its efforts to strengthen international law enforcement relationships a top priority.

The Department has collaborated with other U.S. agencies and foreign law enforcement counterparts to address international intellectual property crime through a combination of joint criminal enforcement operations, case referrals for foreign investigations and prosecutions, training and technical assistance programs for foreign law enforcement, judiciary, and legislators, and engagement in bilateral and multi-lateral working groups that address trademark counterfeiting and copyright piracy.

The Department has also worked vigorously to develop international methods to address cybercrime through cooperative case work, rapid information sharing, and long-term engagement to train law enforcement and improve legal regimes to respond to the threat of Internet-based crime and the proliferation of electronic evidence in a wide range of offenses.

Instances of international intellectual property crime may be addressed effectively by direct contact between prosecutors and investigators on specific cases. However, to address systemic and pervasive international intellectual property crime effectively, greater and more sustained engagement is essential. For example, since 2006, through the Department's Intellectual Property Law Enforcement Coordinator (IPLEC) Program, the Department has deployed experienced federal prosecutors overseas to take the lead on our intellectual property protection efforts in key regions including Asia and Eastern Europe (from 2008 until 2011 in Sofia, Bulgaria, with a new IPLEC recently posted in Bucharest, Romania). Through the IPLEC program, the Department has seen a substantial increase in foreign enforcement and cooperative casework where U.S. law enforcement has had a visible and ongoing presence in the most active countries or regions. This enhancement request would allow for the expansion of the program to additional critical regions and also cover the rapidly developing and overlapping area of international cybercrime.

ICHIPs/Attachés

The Criminal Division has identified several important areas (in order of priority) for the placement of ICHIP Attachés. The cross-designation of these positions as ICHIPs/DOJ Attachés is critical to the success of the Department's overseas law enforcement mission. The effectiveness of cross-designating the current Asia IPLEC/Attaché position is well-documented and gives operational advantages not necessarily available to ICHIPs who do not also possess the DOJ Attaché designation. For example, a DOJ Attaché has greater access to case files and resources because they are not perceived as doing intellectual property work exclusively; ICHIPs, by contrast, can be marginalized by foreign law enforcement if they are thought of as limited to one area of expertise. Since intellectual property crime often intersects with other

types of cases, like international organized crime, the designation of these new positions as solely ICHIPs will hinder their effectiveness in fighting the intellectual property crime threat. The Division plans to hire attorneys with a strong background in criminal prosecution who are capable of and invested in focusing on the intellectual property crime threat in these regions. This approach will help ensure that the bulk of the ICHIP/Attachés' time and effort will contribute to the Department's efforts against intellectual property and cybercrime.

All foreign placements would be subject to approval of the State Department and individual embassies or consulates. Since conditions in these regions could change, countries in these regions will remain under review and the Division (in consultation with the State Department and the White House's Intellectual Property Enforcement Coordinator) will make a final determination regarding the locations in all identified regions if these resources are funded.

China: China continues to be the largest source of trademark counterfeiting and copyright piracy in the world and bears a direct or indirect relationship to the majority of economic espionage and federal trade secret prosecutions in the United States. The Department has met with some success in developing joint investigations through the Intellectual Property Criminal Enforcement Working Group (IPCEWG) of the U.S.-China Joint Liaison Group for Law Enforcement Cooperation. However, an ongoing presence in the country will move existing cases at a faster pace and greatly increase the ability to address new investigations and leads in a timely manner.

South Asia: The violation of intellectual property rights, particularly counterfeiting and copyright piracy, are ongoing problems in a number of South Asian countries. India and Pakistan have each been listed on the USTR *Special 301 Priority Watch List* for several years, and, after China, are two of the largest sources of manufacture for counterfeit and unauthorized pharmaceuticals. The U.S. has invested in training law enforcement officials in Pakistan and investigators, prosecutors, and judges in India to improve the protection of intellectual property rights. Additionally, South Asia has a burgeoning information technology industry and an increasingly electronically-sophisticated populace. Growing cyber threats and terrorism investigations in that region require enhanced law enforcement relationships and training to increase investigations, as well as cooperation in those investigations, that rely heavily on electronic evidence. A regional ICHIP/Attaché, most likely stationed at the U.S. Embassy in India, would substantially improve the opportunities to build on the foundation of training and develop joint cases.

Domestic Intellectual Property Program Support for ICHIP/Attachés

With the potential implementation of the ICHIP/Attaché program, there will be substantial need for support within the U.S., including attorneys, professional staff, and a cybercrime analyst.

Attorneys: Additional attorneys positioned at Criminal Division headquarters are necessary to meet the demands posed by increased international capacity and to ensure that ICHIP/Attaché resources are effectively used, managed, and supported. The Division's Computer Crime and Intellectual Property Section (CCIPS) provides subject matter expertise on computer and intellectual property crimes, manages the domestic Computer Hacking and Intellectual Property

(CHIP) program, and has assisted in and overseen aspects of the prior IPLECs' responsibilities. CCIPS is also the Department's liaison to the National Intellectual Property Coordination Center ("IPR Center") and its 20 domestic and international partner agencies. Likewise, the Criminal Division's Office of International Affairs (OIA) oversees the Department's Attaché program and coordinates the extradition or other legal return of international fugitives and all international evidence-gathering. Attorneys in each office will ensure that foreign leads are provided and followed by U.S. investigative agencies, and that appropriate cases are pursued within the U.S. to provide deterrence to foreign criminals and criminal organizations. Such attorneys will also provide legal support in the Northern District of California to address the overwhelming flow of legal process and evidentiary requests in intellectual property and cybercrime cases that are addressed to Silicon Valley companies.

Professional Staff: Additional professional staff are necessary to ensure the smooth administration of hiring, retention, and support of the ICHIP/Attaché program.

Cybercrime Analyst: In recent years, there has been a rapidly increasing demand for technical training by the CCIPS Cybercrime Lab by foreign countries seeking to develop expertise in cyber forensics and computer crime. The proposed additional cybercrime analyst will allow CCIPS to greatly increase the amount of training provided, while directly supporting foreign investigations.

This enhancement also requests individual travel and programming budgets to be administered by the ICHIPs within their regions as well as additional travel, litigation support, and domestic training resources that will be used to increase the capacity and effectiveness of the overall intellectual property program.

Impact on Performance:

These requested resources will directly support the Department's Strategic Goal 2: *Prevent crime, protect the rights of the American people, and enforce federal law*; Strategic Objective 2.4: *Investigate and prosecute corruption, economic crimes, and transnational organized crime*. In particular, they will allow the U.S. Government to:

- Develop the capacity of nations in several important regions to combat intellectual property and computer crimes;
- Increase the number and scope of cooperative international prosecutions targeting high-tech and intellectual property crimes;
- Increase coordination of international cases involving computer crimes, intellectual property crimes, and digital evidence;
- Build upon the successful integration of intellectual property and cybercrime expertise that currently exists in the domestic CHIP Network;
- Strengthen the DOJ Attaché program's ability to address transnational organized crime.

Funding

Base Funding

<i>FY 2014 Enacted</i>				<i>FY 2015 Enacted</i>				<i>FY 2016 Current Services</i>			
Pos	atty	FTE	\$(000)	Pos	atty	FTE	\$(000)	Pos	atty	FTE	\$(000)
22	18	18	\$5,173	19	16	15	\$4,538	19	16	15	\$4,833

Personnel Increase Cost Summary

Type of Position/Series	Modular Cost per Position (\$000)	Number of Positions Requested	FY 2016 Request (\$000)	FY 2017 Net Annualization (change from 2016) (\$000)	FY 2018 Net Annualization (change from 2017) (\$000)
Attorneys (0905) (Domestic)	\$117	5	\$585	\$545	\$0
Attorneys (0905) (Foreign)	\$504	2	\$1,008	\$602	\$0
Paralegals / Other Law (0900-0999)	\$66	4	\$264	\$176	\$208
Total Personnel		11	\$1,857	\$1,323	\$208

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2016 Request (\$000)	FY 2017 Net Annualization (change from 2016) (\$000)	FY 2018 Net Annualization (change from 2017) (\$000)
FSNs	\$60	2	\$120	\$0	\$0
Travel	N/A	N/A	\$228	\$228	\$0
Total Non-Personnel	N/A	N/A	\$348	\$228	\$0

Total Request for this Item

	Pos	Atty	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)	FY 2017 Net Annualization (change from 2016) (\$000)	FY 2018 Net Annualization (change from 2017) (\$000)
Current Services	19	16	15	\$4,833	\$0	\$4,833	\$0	\$0
Increases	11	7	6	\$1,857	\$348	\$2,205	\$1,551	\$208
Grand Total	30	23	21	\$6,690	\$348	\$7,038	\$1,551	\$208