

The Criminal Division



FY 2014
Congressional Submission

Table of Contents

	Page No.
I. Overview.....	1
II. Summary of Program Changes.....	10
III. Appropriations Language and Analysis of Appropriations Language	10
IV. Decision Unit Justification.....	11
A. Enforcing Federal Criminal Laws	
1. Program Description.....	11
2. Performance and Resource Tables.....	13
3. Performance, Resources, and Strategies.....	16
V. Program Increases by Item	18
VI. Program Offsets by Item – Not Applicable	
VII. Exhibits	
A. Organizational Chart	
B. Summary of Requirements	
C. Program Increases/Offsets by Decision Unit	
D. Resources by DOJ Strategic Goal/Objective	
E. Justification for Base Adjustments	
F. Crosswalk of 2012 Availability	
G. Crosswalk of 2013 Availability	
H. Summary of Reimbursable Resources	
I. Detail of Permanent Positions by Category	
J. Financial Analysis of Program Changes	
K. Summary of Requirements by Grade	
L. Summary of Requirements by Object Class	

I. Overview for Criminal Division

A. FY 2014 Budget Summary

The Criminal Division requests a total of 814 permanent positions, 703 direct Full-Time Equivalent work years (FTE), and \$182,499,000 in its Salaries and Expenses appropriation for Fiscal Year (FY) 2014. The Division's request will maintain the current level of services while providing funding for necessary resources to combat the growing and evolving cyber threat, the most significant financial and mortgage fraud cases, as well as the increasing threat of transnational intellectual property crime. Electronic copies of the Department of Justice's Congressional Budget Justifications and Capital Asset Plan and Business Case exhibits can be viewed or downloaded from the Internet using the Internet address:

<http://www.justice.gov/02organizations/bpp.htm>.

B. Criminal Division Mission & Program Activities

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.

The 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.

(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 activities 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.

(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.

(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 for the purpose of sustaining democracy and promoting 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.

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 two of its three Strategic Goals: (1) Prevent Terrorism and Promote the Nation’s Security Consistent with the Rule of Law and (2) Prevent Crime, Protect Rights of the American People, and Enforce Federal Law (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
	1.2 Prosecute those involved in terrorist acts
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
	2.2 Prevent and intervene in crimes against vulnerable populations; uphold the rights of, and improve services to, America’s crime victims
	2.3 Combat the threat, trafficking, and use of illegal drugs and the diversion of licit drugs
	2.4 Combat corruption, economic crimes, and international organized crime
	2.5 Promote and protect Americans’ civil rights
Goal Three: Ensure and Support the Fair, Impartial, Efficient, and Transparent Administration of Justice at the Federal, State, Local, Tribal and International Level	3.1 Promote and strengthen relationship and strategies for the administration of justice with state, local, tribal and international law enforcement.

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;
 - **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.

Examples of how the Division’s program activities contribute to achieving its strategic outcomes are provided in the following table:

Key Strategic Priority	Prosecuting & Investigating Activities	Expert Guidance & Advice Activities	Law Enforcement Tool Review Activities	Global Partnership Activities
Ensuring Trust & Confidence in Government Institutions	<ul style="list-style-type: none"> ▪ Prosecuting cases aimed at deterring corruption among elected and other government officials ▪ Supporting United States Attorneys’ Offices (USAOs) by prosecuting cases from which USAOs are recused 	<ul style="list-style-type: none"> ▪ Providing assistance and guidance to USAOs in sensitive cases ▪ Ensuring election crime matters are handled uniformly and fairly 	<ul style="list-style-type: none"> ▪ Using asset forfeiture tools to seize ill-gotten proceeds of crime ▪ Providing oversight to sensitive operations ▪ Utilizing electronic surveillance in sensitive investigations of government officials 	<ul style="list-style-type: none"> ▪ Training foreign countries in anti-corruption strategies ▪ Supporting investigations focused on deterring the corruption of foreign officials
Ensuring the Stability & Security of Domestic & Global Markets	<ul style="list-style-type: none"> ▪ Vigorously prosecuting those who attempt to defraud tax-payers ▪ Conducting sensitive and complex investigations of corrupt corporations operating inside and outside the United States 	<ul style="list-style-type: none"> ▪ Training thousands of foreign officials on intellectual property crimes ▪ Developing national strategies to combat procurement and Medicare fraud 	<ul style="list-style-type: none"> ▪ Developing regulations to address ways to better detect procurement fraud ▪ Providing oversight to ensure fair application of powerful law enforcement tools 	<ul style="list-style-type: none"> ▪ Establishing international working groups to combat money laundering ▪ Creating working relationships with traditionally closed countries
Disrupting & Dismantling Criminal Organizations	<ul style="list-style-type: none"> ▪ Prosecuting wide-ranging criminal organizations using racketeering and other powerful criminal statutes ▪ Coordinating transnational operations relating to violent gangs 	<ul style="list-style-type: none"> ▪ Training USAOs on effectively using the law to prosecute gangs ▪ Creating a coordinated global approach to dismantle drug trafficking organizations 	<ul style="list-style-type: none"> ▪ Providing oversight for the use of electronic surveillance in violent crime and organized crime cases ▪ Assisting in the protection of witnesses 	<ul style="list-style-type: none"> ▪ Improving relations with law enforcement in various countries where gang leaders reside ▪ Implementing the International Organized Crime Strategy

Key Strategic Priority	Prosecuting & Investigating Activities	Expert Guidance & Advice Activities	Law Enforcement Tool Review Activities	Global Partnership Activities
Protecting Children & Vindicating Human Rights	<ul style="list-style-type: none"> ▪ Prosecuting high-profile and dangerous child predators ▪ Investigating potential war criminal harboring illegally in the U.S. 	<ul style="list-style-type: none"> ▪ Training Project Safe Childhood (PSC) field units in prosecution techniques ▪ Advising foreign counterparts on conducting complex investigations 	<ul style="list-style-type: none"> ▪ Overseeing a high-tech lab to assist law enforcement in gathering critical evidence in child exploitation cases ▪ Developing strategies to effectively capture digital evidence 	<ul style="list-style-type: none"> ▪ Working to form international strategies to combat child sexual exploitation ▪ Prosecuting U.S. government agents who have violated human rights while in other countries
Promoting the Rule of Law Internationally	<ul style="list-style-type: none"> ▪ Coordination of bi-lateral investigations ▪ Seeking the extradition of criminal defendants who have fled overseas 	<ul style="list-style-type: none"> ▪ Assisting foreign countries in the development of laws and legal procedures ▪ Training of our foreign counterparts 	<ul style="list-style-type: none"> ▪ Obtaining evidence from or for foreign countries ▪ Supporting trans-national investigations 	<ul style="list-style-type: none"> ▪ Providing direct technical assistance on case-specific matters ▪ Participating in international policy groups
Supporting National Security	<ul style="list-style-type: none"> ▪ Prosecuting cases focused on deterring corruption of foreign officials ▪ Supporting investigations aimed at limiting terrorist mobility 	<ul style="list-style-type: none"> ▪ Participating in government-wide anti-terrorism strategy groups ▪ Providing expert guidance on freezing terrorist assets 	<ul style="list-style-type: none"> ▪ Negotiating Mutual Legal Assistance Treaties to obtain foreign evidence ▪ Securing extradition of terrorist suspects 	<ul style="list-style-type: none"> ▪ Strengthening counter-terrorism ability of foreign counterparts ▪ Working with other countries to disrupt terrorist travel networks

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 & 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 the building management to install electrical light timers and motion detectors in corridors and bathrooms to reduce the use and cost of electricity. The Division has completed this installation in one of its three leased buildings.
- 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)	
Cyber Security	This request will 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.	25	14	\$2,580	18
Financial and Mortgage Fraud	These additional resources will be used by the Criminal Division to prosecute the most significant financial and mortgage fraud cases, coordinate multi-district financial and mortgage fraud cases, and assist U.S. Attorneys Offices (USAOs) in mortgage fraud cases with significant money laundering and asset forfeiture components.	28	14	\$5,000	27
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 four 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	\$3,500	32

III. Appropriations Language and Analysis of Appropriations Language

No changes to appropriations language.

IV. Decision Unit Justification

A. Enforcing Federal Criminal Laws

<i>Enforcing Federal Criminal Laws</i>	Perm. Pos.	FTE	Amount
2012 Enacted	751	748	\$174,000
2013 Continuing Resolution	751	670	\$174,000
2013 Continuing Resolution 0.612% Increase			\$1,065
Base and Technical Adjustments	-1	-1	-\$3,646
2014 Current Services	750	669	\$171,419
2014 Program Increases	64	34	\$11,080
2014 Request	814	703	\$182,499
Total Change 2012-2014	63	-45	\$8,499

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 Unit;
- 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.

2. Performance and Resource Tables

PERFORMANCE AND RESOURCES TABLE											
Decision Unit: Enforcing Federal Criminal Laws											
RESOURCES		Target		Actual		Projected		Changes		Requested (Total)	
		FY 2012		FY 2012		FY 2013 CR		Current Services Adjustments and FY 2014 Program Changes		FY 2014 Request	
Total Costs and FTE (reimbursable FTE are included, but reimbursable costs are not included in the total)		FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
		1,091	\$174,000	954	\$173,061	952	\$175,065	33	\$7,434	985	\$182,499
TYPE/ STRATEGIC OBJECTIVE	PERFORMANCE	FY 2012		FY 2012		FY 2013 CR		Current Services Adjustments and FY 2014 Program Changes		FY 2014 Request	
Program Activity	1. Prosecutions and Investigations	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
		477	\$89,462	458	\$90,319	446	\$93,047	21	\$4,473	467	\$97,520
Workload	Cases Opened	452		461		443		22		465	
Workload	Cases Closed	307		511		322		16		338	
Workload	Cases Pending	1,362		1,156		1,287		127		1,414	
Workload	Appellate Work - Opened	3,410		3,209		3,207		0		3,207	
Workload	Appellate Work - Closed	3,370		3,192		3,198		0		3,198	
Workload	Appellate Work Pending	2,876		2,859		2,833		0		2,833	
Workload	Matters Opened	916		905		901		45		946	
Workload	Matters Closed	791		1,065		890		44		934	
Workload	Matters Pending	2,010		1,687		1,718		12		1,730	

Program Activity	2. Expert Fuidance and Legal Advice	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
		425	\$49,686	353	\$47,813	351	\$47,776	9	\$2,038	360	\$49,814
Workload	Number of Legislative and Policy Analysis Matters Completed	5,181		5,875		5,299		211		5,510	
Workload	Number of Programmatic Coordination Activities	4,058		5,226		7,071		283		7,354	
Workload	Number of Legal Advisory Matters Completed	24,271		39,726		29,959		1,198		31,157	
Workload	Number of Training Sessions/Presentations	3,305		3,845		3,395		135		3,530	
Program Activity	3. Law Enforcement Tools	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
		189	\$34,852	143	\$ 34,929	156	\$34,243	3	\$922	159	\$35,165
Workload	Number of Mandatory Reviews Completed	17,314		19,090		27,432		823		28,255	
Performance Measure: Output	Favorably Resolve Criminal Cases	90%		93%		90%		0		90%	
Performance Measure: Efficiency	Favorably Resolve Civil Cases	80%		N/A		80%		0		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 Unit. 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.

PERFORMANCE MEASURE TABLE

Decision Unit: Enforcing Federal Criminal Laws

Performance Report and Performance Plan Targets		FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012		FY 2013	FY 2014
		Actual	Actual	Actual	Actual	Actual	Target	Actual	Target	Target
OUTPUT Measure	Number of Legislative and Policy Analysis Matters Completed	18,841	14,662	6,683	6,524	7,458	5,181	5,875	5,299	5,510
OUTPUT Measure	Number of Programmatic Coordination Activities	2,019	2,648	2,428	3,509	4,492	4,058	5,226	7,071	7,354
OUTPUT Measure	Number of Legal Advisory Matters Completed	19,651	15,953	16,573	19,039	24,438	24,271	39,726	29,959	31,157
OUTPUT Measure	Number of Training Sessions/Presentations	2,917	2,799	2,194	2,767	3,612	3,305	3,845	3,395	3,530
OUTPUT Measure	Number of Mandatory Reviews Completed	25,052	21,356	22,696	46,125	19,237	17,314	19,090	27,432	28,255
OUTCOME Measure	Favorably resolve Criminal Cases**	97%	95%	97%	90%	96%	90%	93%	90%	90%
OUTCOME Measure	Favorably Resolve Civil Cases**	87%	75%	100%	100%	100%	80%	N/A	80%	80%

N/A = Data unavailable

*** As of Fiscal Year 2007, the workloads of the Counterterrorism and Counterespionage Sections are not included in the Criminal Division.**

**** Denotes inclusion in the DOJ Annual Performance Plan**

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 2012, the Division met both outcome goals and is on track to meet both of them in FY 2013.

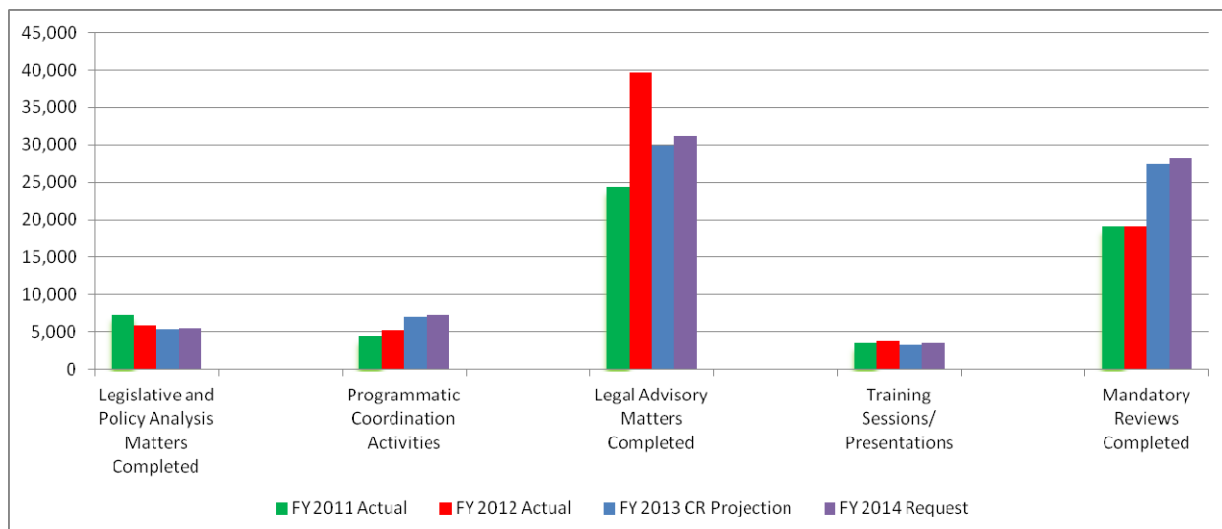
Prosecutions and Investigations Workload

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. The Division exceeded some of the FY 2011 targets set for prosecutions and investigations workload. The Division projects that the prosecutions and investigations workload reflected the following:

- The number of cases and matters opened by the Division increased by approximately 5%;
- The number of cases and matters closed increased by approximately 5%; and,
- The number of appellate work opened and closed will remain the same.

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.



The Division exceeded its FY 2011 targets for four of these five measures, missing only the mandatory reviews completed. With the FY 2014 enhancement request, Division expects to complete about 4% more mandatory reviews.

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 One, Two, and Three.

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 the end of FY 2013, increase by 5 percent over FY 2011 levels, the number of investigations completed per Department of Justice attorney working on financial fraud and healthcare fraud cases; additionally for use in appropriate cases, institute a system for tracking compliance by corporate defendants with the terms of judgments, consent decrees, settlements, deferred prosecution agreements, and nonprosecution agreements.

Vulnerable People: Protect those most in need of help - with special emphasis on child exploitation and civil rights: By September 30, 2013, working with state and local law enforcement agencies, protect potential victims from abuse and exploitation by achieving a 5% increase for 3 sets of key indicators:

- Open investigations concerning non-compliant sex offenders, sexual exploitation of children, human trafficking
- Matters/investigations resolved concerning sexual exploitation of children and human trafficking
- Number of children depicted in child pornography that are identified by the FBI

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

V. Program Increases by Item

Item Name:	<u>Enhancing Cyber Capabilities to Address the Blended Cyber Security Threat</u>
Budget Decision Unit(s):	<u>Enforcing Federal Criminal Laws</u>
Strategic Goal/Objective:	<u>Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law</u> <u>Objective 1.2: Prosecute those involved in terrorist acts</u> <u>Goal 2: Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law</u> <u>Objective 2.4: Combat corruption, economic crimes, and international organized crime</u>
Organizational Program:	<u>Criminal Division</u>
Request Priority:	<u>1 of 3</u>
Program Increase:	Positions <u>25</u> Atty <u>9</u> FTE <u>14</u> Dollars <u>\$2,580,000</u>

Description of Item

The cybercrime threat is growing at a rapid rate. The Criminal Division plays a vital role in combating this threat through direct involvement in prosecutions, support and advocacy for legal tools, international assistance and outreach, and forensic support. In addition to operational support, this enhancement will increase the policy capacity of the Department of Justice as the government continues to grow its interaction and interface with cybersecurity and cyberspace issues. In order to keep pace with the evolving cybercrime threat and the investments being made to investigative agencies, the Division is requesting an increase of **25 positions (9 attorneys), 14 FTE, and \$2,580,000.**

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. Over the last several years, criminal investigators and prosecutors have seen significant increases in the skills and organization of threat actors. In the last year, criminal groups such as Anonymous and LulzSec developed and quickly iterated tools and techniques for damaging computer systems and stealing large quantities of personal data.¹ Financially motivated groups work together closely and easily across national boundaries to steal, exploit, and profit from the large-scale theft of personal data, coalescing in forums where they barter individual skills to create ad hoc criminal networks with a power and reach sometimes approaching that of traditional transnational organized crime

¹ See, e.g., Press Release, U.S. Attorney's Office for the Southern District of N.Y., Six Hackers in the United States and Abroad Charged for Crimes Affecting Over One Million Victims (Mar. 6, 2012), available at <http://www.justice.gov/usao/nys/pressreleases/March12/ackroydetalindictmentpr.pdf>; Matt Peckham, *Anonymous and LulzSec Fire Back at Police with Lethal Data Dump*, TIME TECHLAND (Aug. 8, 2011), <http://techland.time.com/2011/08/08/anonymous-and-lulzsec-fire-back-at-police-with-lethal-data-dump/>.

networks.² Intellectual property and similar proprietary information on which our economy depends are threatened not only by criminals attacking remotely, but also by insiders who can secrete years of research onto a chip the size of a coin in moments.³ And, more recently, actors ranging from nation-states to terrorist groups to criminal organizations have expressed an interest in exploiting the computer networks that control our critical infrastructure—such as the power grid or the water supply—for financial gain or political advantage.⁴

Characteristic of these threats is their blended nature. The tools used to commit serious cyber theft and damage are not only wielded by those with large-scale development resources. Instead, individuals or small groups can steal huge quantities of sensitive data, damage key computer systems, or silence those who disagree with them with widely available tools. Financial gains from these crimes can, in turn, be used to build larger networks and buy protection from foreign government officials. As a result, U.S. investigators working to determine the source and nature of a cyber threat often cannot know at the outset whether an attack was mounted by an individual acting alone, an organized criminal or terrorist group, or a hostile nation.

Addressing this complex threat requires a unified approach, one that incorporates criminal investigation and prosecution tools, civil and national security authorities, trade and economic sanctions, public-private partnerships, and international cooperation. Criminal prosecution, whether in the United States or a partner country, plays a central and critical role in this effort. In addition, while prosecution is not the appropriate approach for every threat that affects the United States, identifying and understanding the threat will very often involve the use of criminal investigative tools and methods. Moreover, other means of addressing threats and cooperatively reducing vulnerabilities—whether undertaken by private groups, system protectors, or the intelligence community—will often require a deep and subtle understanding of law enforcement authorities and criminal prohibitions.

The Criminal Division has long stood at the forefront of addressing these issues, along with its partners across law enforcement, government, and the private sector. As a result of extensive investigation and prosecution of criminal threat actors, often conducted side-by-side with

² See, e.g., Press Release, Dep't of Justice Office of Pub. Affairs, *Online Identity Thief Sentenced in Virginia to 14 Years in Prison for Selling Counterfeit Credit Cards Leading to More than \$3 Million in Losses* (Sept. 9, 2011), available at <http://www.justice.gov/opa/pr/2011/September/11-crm-1163.html>; *Identity Theft: A Victims Bill of Rights: Hearing Before the Subcomm. on Info. Policy, Census, and Nat'l Archives of the H. Comm. on Oversight and Gov't Reform* (June 17, 2009) (statement of Jason M. Weinstein, Deputy Assistant Att'y Gen. of the Crim. Div. of the U.S. Dep't of Justice), available at <http://www.justice.gov/ola/testimony/111-1/2009-06-17-crm-weinstein-identity-theft.pdf>.

³ See, e.g., Insider Threat Team, *Theft of Intellectual Property and Tips for Prevention*, CERT INSIDER THREAT BLOG (July 21, 2011, 1:29 PM), https://www.cert.org/blogs/insider_threat/2011/07/insider_threat_methods_of_exfiltration.html; Peter Lattman, *Former Goldman Programmer Found Guilty of Code Theft*, N.Y. TIMES DEALBOOK, (Dec. 10, 2010, 8:16 PM), <http://dealbook.nytimes.com/2010/12/10/ex-goldman-programmer-is-convicted/>.

⁴ See, e.g., Pierluigi Paganini, *SCADA & Security of Critical Infrastructures*, Infosec Institute (February 22, 2013), <http://resources.infosecinstitute.com/scada-security-of-critical-infrastructures/>; Michael S. Schmidt, *New Interest in Hacking as Threat to Security*, N.Y. TIMES, Mar. 14, 2012, at A16, available at <http://www.nytimes.com/2012/03/14/us/new-interest-in-hacking-as-threat-to-us-security.html>; J. Nicholas Hoover, *Cyber Threats to Critical Infrastructure Spike*, INFO. WEEK (Apr. 19, 2011, 2:08 PM), <http://www.informationweek.com/news/government/security/229401858>. See also, *Executive Order—Improving Critical Infrastructure Cybersecurity* (February 12, 2013), <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

investigators and Assistant United States Attorneys in the field, Division attorneys possess a deep understanding of cyber threats. They provide extensive and authoritative legal advice on the lawful collection of electronic evidence, navigating complex statutes and case law. They have established relationships with international law enforcement agencies, conducted extensive training, and regularly cooperated with international partners to preserve, collect, and exchange electronic evidence and conduct joint investigations when criminal conduct crosses national borders. Supporting this mission, the Division's Cybercrime Laboratory provides essential assistance to prosecutors, agents, and others, helping them understand and better explain technical issues to judges and juries alike.

Meeting this challenge has never been a solitary endeavor, and the Criminal Division has long understood the need to forge key partnerships to address cyber threats. The Division's Computer Crime and Intellectual Property Section (CCIPS) has developed legal expertise and technical acumen that contribute fundamentally to the success of the Department's cyber security efforts.

To extend this expertise nationally, CCIPS has developed, trained, and partnered with Computer Hacking and Intellectual Property (CHIP) Coordinators during the last 17 years, growing a network that now comprises more than 230 Assistant United States Attorneys (at least one in every district). CCIPS engages with and regularly trains key law enforcement partners across the federal government, including the Federal Bureau of Investigation (FBI), U.S. Secret Service, U.S. Postal Inspection Service, and the Inspector General community. Finally, because cybercrimes often span the globe, the Division has forged transnational networks for effective law enforcement cooperation, including a rapid response network aimed at preserving crucial electronic evidence before it vanishes.

In addition to the direct investigation and prosecution of cybercrimes, the Division has provided extensive legal and policy guidance in furtherance of these goals. To enhance the legal and policy landscape to address cybercrime, 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. It has drafted and advocated for revisions to the laws that allow for the collection of electronic evidence to assure that they keep pace with technological advances and that investigators can gain access to the evidence they need. It has developed and reviewed innovative asset seizure mechanisms to disrupt criminal conduct, enhanced collection and analysis of criminal intelligence relating to organized criminals operating online, and provided timely legal advice regarding the application of existing law to new technology.

Finally, since the creation of the National Security Division (NSD) in 2006, the Criminal Division has provided priority assistance and support to NSD's terrorism prosecutions, to intrusion investigations related to espionage, counter-intelligence, and attacks on critical national infrastructures, and to the cooperative development of cybersecurity policy. Recently, NSD, after a careful review, has recognized the need to make substantial changes to its structure and priorities to address the aspects of the cyber threat for which it is primarily responsible. The Criminal Division, principally through CCIPS, is committed to building NSD's expertise through training and ongoing partnerships as it implements these changes. These efforts will require the Criminal Division to assist NSD in its efforts to build needed capability and then to partner with NSD to address the legal, technical, and policy challenges inherent in addressing threats that are,

by their nature, often incapable at the outset of being placed into easily ascertainable criminal or national security categories.

To address these challenges, the Criminal Division must enhance its approach in four key areas.

1. Timely and Accurate Investigations, Prosecutions, and Disruption Efforts

The threats to our nation’s invaluable proprietary and personal information are increasing, and so must our innovation and efforts to deter, disrupt, and prosecute those threat actors. Studies have shown that the number of intrusions continues to increase, and the cost of cybercrime to American businesses and citizens likewise continues to mount.⁵

As a result, the Division’s Computer Crime and Intellectual Property Section has experienced a 19% increase in pending investigations and an 8% increase in pending prosecutions between FY 2010 and FY 2012. Without additional resources, the Division will not be able to keep pace with the growing cyber caseload.

CCIPS Cyber Crime Caseload	FY 2010	FY 2011	FY 2012
Total Investigations Pending	252	357	301
<i>National-security focus</i>	50	71	60
<i>Criminal focus</i>	202	286	240
Total Prosecutions Pending	87	97	95
<i>National-security focus</i>	17	19	19
<i>Criminal focus</i>	70	78	76

A reality of cyber investigations is that it is nearly impossible to forecast where they will begin or end. Consequently, the Division, through CCIPS, provides nation-wide support to investigations, prosecutions, and disruption efforts, helping to ensure that its law enforcement partners receive consistent, quality support whether the investigation’s trail leads to Silicon Valley, rural America, or overseas. As a result, Criminal Division prosecutors have led, or partnered in, some of the country’s most significant data breach and computer intrusion cases, the success of which has required a comprehensive grasp of computer network technology and electronic evidence law and a subtle understanding of the often loosely organized worldwide groups that work together to plan and execute these attacks.

CCIPS prosecutors work in direct cooperation with the CHIP network and investigative agencies to identify and address threat actors, whether they are primarily external—such as criminal groups or foreign actors breaking in and stealing information—or internal, such as insiders misappropriating invaluable research or trade secrets. CCIPS houses prosecutors with a deep understanding of data breaches and computer misuse cases and prosecutors who understand the complexity of intellectual property cases to comprise the nation’s leading resource for deterring, investigating, and punishing the theft of sensitive electronic information. Consequently, every additional prosecutor in CCIPS becomes a force multiplier for the Department, leveraging its

⁵ See, e.g., Salvador Rodriguez, *Cyber Crimes Are More Common and More Costly, Study Finds*, L.A. TIMES, Aug. 3, 2011, <http://articles.latimes.com/2011/aug/03/business/la-fi-cyber-attacks-20110803>; Identity Theft Resource Center, *2012 ITRC Breach Report* (December 26, 2012), <http://www.idtheftcenter.org/ITRC%20Breach%20Report%202012.pdf>.

expertise wherever it is needed to the benefit of all USAOs and the achievement of the Department's cyber crime goals.

For example, in April 2011, CCIPS worked closely with a United States Attorney's Office to implement an innovative approach to disrupting a criminal network that had infected hundreds of thousands of computer systems in order to steal and exploit the computer owners' personal financial data. While the individuals controlling the network resided overseas and were largely outside the direct reach of U.S. law enforcement, prosecutors used a combination of civil and criminal authorities to seize key control servers, shut down the network, and work with private sector partners to help disinfect victims' computer systems. This ground-breaking investigation completely disrupted the ongoing crime.

With additional resources, CCIPS will be able to coordinate more of these ground-breaking investigations and will increase the effectiveness of the Department's efforts to combat the cyber threat.

Furthermore, more and more often, offenders reside outside of the United States, requiring the assistance of foreign law enforcement agents to gather evidence and make arrests. The Criminal Division's Office of International Affairs (OIA) has sole authority within the United States for negotiating mutual legal assistance treaties and securing the cooperation of foreign governments in providing to the U.S. fugitives and foreign electronic evidence. The number of mutual legal assistance requests received has increased nine percent since FY 2010 and 28% during the past six years (since FY 2007). While the number of extradition requests received has relatively remained steady since FY 2007, pending requests have increased by 16%. These trends will only continue and, consequently, require additional resources for OIA to handle their critical workload.

2. Providing Effective Advice on and Advocacy for Legal Tools and Authorities

Beyond its direct prosecutorial role, the Criminal Division plays an essential part in helping to interpret and enforce the rules governing access to electronic evidence. Our nation's laws relating to access to electronic communications are complex, reflecting the numerous interests they balance in determining the appropriate scope of law enforcement and private sector access to communications. Through CCIPS and the Office of Enforcement Operations (OEO), the Criminal Division provides comprehensive and authoritative training, guidance, and review regarding lawful access to electronic evidence for United States law enforcement at the federal, state, and local levels.

During the past six years, OEO's electronic surveillance workload has increased by 21%: in FY 2007, OEO reviewed 2,933 electronic surveillance applications. In FY 2012, OEO reviewed 3,554. Since approximately six percent of the Office's workload is directly related to cyber cases, additional resources are necessary to ensure that OEO is able to handle the surveillance requirements of these cases.

CCIPS provides advice through publications and live training to federal, state, and local law enforcement agencies on searching and seizing electronic evidence. This advice is often based upon direct experience litigating those issues before district and appellate courts across the United States. Because of their lengthy and deep experience with these issues, Division

attorneys are regularly sought by United States Attorney's Offices to litigate electronic evidence issues across the country. The number of cases that involve these issues continues to increase as more investigations use electronic evidence, more defense attorneys come to realize that it is a potential source for suppression motions, and more judges become concerned about government access to electronic data. Additional resources will allow the Division to successfully handle and participate in the most significant litigation.

Few issues in the United States are more closely watched or hotly debated than those relating to government access to electronic information. Whether the question involves the appropriate standard for law enforcement access to location information, the contours of an exception to the wiretap laws, or the application of the Fourth Amendment to an emerging technology, the Criminal Division is deeply engaged in the debate that defines the limits of governmental authority. CCIPS engages with privacy advocacy groups, Congress, and other interested parties to advocate for standards that permit access to or sharing of critical cyber security data while protecting individual privacy to the greatest possible extent. As the requirements of this advocacy increase due to growing public interest in government surveillance, additional resources will be needed to support CCIPS' engagement.

3. Developing International Cooperation and Outreach

Because cybercrime is global in scope, the Criminal Division has long had a robust program for encouraging the development by foreign governments of laws, investigation and prosecution capacity, and political will to address emerging cybercrime threats and capabilities. From the development and maintenance of a 24/7 response capability in more than 50 countries aimed at preserving critical evidence before it is deleted, to its leading role in negotiating the first multilateral convention on cybercrime, to its regular engagement on training, policy, and operational issues with law enforcement partners around the world, the Division has led the fight against transnational cybercrime.

But the problem is only growing. Despite significant advances in law enforcement cooperation and understanding, criminals continue to use gaps and inefficiencies in international law enforcement capabilities to evade detection, attribution, and punishment. Foreign authorities apply data protection regulations in ways that can frustrate investigations. Delays in evidence collection resulting from inexperience, overwork, or inadequate laws can stop investigations almost at their inception. And inadequate international governance of the myriad entities involved in providing Internet connectivity and domain registration has permitted the growth of "data havens" where criminal and other threat actors can commit crimes with relative impunity. Indeed, international discussions over Internet governance have expanded in the International Telecommunications Union and the International Corporation for Assigned Names and Numbers. In order to protect the interests of the Department and the United States Government, Division attorneys will increasingly have to contribute their expertise and advocacy to these debates.

Despite these challenges, the Criminal Division has attempted to perform effective international outreach on cyber issues. 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 continued to improve capacity to address cybercrime around the world. CCIPS attorneys lead efforts to build capacity and law enforcement relationships 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.

Moreover, the State Department is developing plans to address cyber threats more comprehensively. Because these efforts will result in additional interactions with foreign countries and multilateral organizations, as well as new funding for cybercrime training and assistance, they will increase demands on CCIPS and OIA attorneys.

4. Growing a Proven Structure to Address Digital Forensic Capabilities

Underpinning almost every cyber investigation and prosecution is the forensic examination of digital evidence. Over the last two decades, the volume of digital evidence has exploded. This volume has placed a tremendous burden on the Department's prosecutors to learn and understand the myriad complexities at the intersection of computer forensics, cybercrime, and emerging technologies. Due to the fast pace of advancing technologies, federal prosecutors outside of CCIPS often lack the technical knowledge necessary to know what digital evidence to ask for or how to best use digital evidence to further prosecutions.

Law enforcement agencies are overwhelmed with requests for digital forensics. The backlog and processing time for computer forensic analysis can exceed several years, which significantly undermines effective investigations and prosecutions. Even once a full forensic analysis is complete, prosecutors often receive forensic reports that fall far short of meeting their needs.

Prosecutors, who are the ultimate consumers of computer forensic results, must have appropriate and consistent support from digital analysis experts at all stages of a case. Since law enforcement agency support typically diminishes following indictment, prosecutors often lack the appropriate level of support to meet discovery obligations and to understand, identify, and present critical digital evidence. Prosecutors must have digital analysis resources that are committed to the needs of the prosecutor throughout trial preparation, trial, and sentencing.

Department prosecutors routinely need an immediate in-house "go-to" digital forensic expert to:

- assist prosecutors in both early assessment (triage);
- provide digital investigative analysis consultation as necessary for decision-making at critical times throughout the investigation and prosecution;
- review and explain technical analysis reports from law enforcement and defense experts;
- respond to last-minute evidentiary demands created by judges for pre-trial and sentencing hearings;
- assess and consult with prosecutors during trial to rebut shifting defenses; and
- help create demonstrative exhibits, summaries, and presentations that assist the jury's understanding of digital evidence and forensic expert testimony.

The CCIPS Cybercrime Laboratory plays an essential role in assisting investigators and prosecutors – and ultimately judges and juries – in understanding how particular evidence fits

into an overall “story of the case.” This function may be general – for example, the Laboratory’s outreach to judicial authorities to ensure that they have adequate technical foundation and understanding of the role of electronic evidence – or specific to a particular case.

The CCIPS computer forensic model is a tiered and triage-based approach that provides technical and forensic support to litigation, legislative initiatives, and national security activities through consultation, forensic support, and training. The extent of CCIPS Cybercrime Laboratory support varies depending on case need: it can range from simple consultations to hands-on analysis, support, and training of agents or agency forensic personnel in the field (including the use of automated tools on site); from triage exams to full digital investigative analysis; or from pre-trial preparation to trial and post-trial support. Having a Division digital analysis expert – possessing advanced knowledge, skills, and abilities, as well as the capability to provide effective courtroom testimony if needed – sitting with the prosecutor in court could mean the difference between conceding or rebutting inaccurate or misleading defense expert testimony.

Enhancing the CCIPS Cybercrime Laboratory’s resources is therefore necessary to advance prosecutions, meet discovery obligations, develop and evaluate plea offers, and bridge the gap between what law enforcement agencies produce in the course of their normal computer forensic examinations and what is needed for successful prosecutions. Between 2010 and 2011, the Cybercrime Laboratory experienced a 29% increase in requests for forensic support assistance and a 31% increase in forensic consultations. Each additional Cybercrime Laboratory examiner will significantly increase the lab’s capacity for meeting customer demand: one examiner can increase the number of forensic consults provided by more than 50% and the number of trainings provided by 19%. Furthermore, additional examiners will be needed to keep pace with the ever-increasing size of hard drives and the subsequent datasets requiring digital analysis. Within just the *first quarter* of 2012, the lab received over 12 terabytes of data for analysis, which amounts to 85% of the data received in all of 2009 and 41% of the data received in all of 2011. With appropriate resources, the lab could provide the most comprehensive, efficient, and cost-effective digital investigative analysis support to the Department’s prosecutions across the country.

Impact on Performance (Relationship of Increase to Strategic Goals)

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, preserve digital evidence, and meet its mission of protecting national security and public safety against these increasing cyber threats. The Criminal Division has a superb track record: in FY 2011, 100% of its prosecutions had a successful outcome.

However, the Division’s cyber workload is increasing due to the growing nature of the threat and the increase of investigative resources. With the FBI increasing its resources in FY 2014 in support of the Next Generation Cyber Initiative to enhance the technical capabilities of investigative personnel, increase cyber investigations, and improve cyber collection and analysis, the Criminal Division must receive this commensurate increase to ensure that investigations can become successful prosecutions and to ensure that investigations can be adequately supported.

Funding

Base Funding

FY 2012 Enacted				FY 2013 CR				FY 2014 Current Services			
Pos	atty	FTE	\$(000)	Pos	atty	FTE	\$(000)	Pos	atty	FTE	\$(000)
122	79	122	\$28,254	122	79	95	\$28,428	122	79	95	27,891

Personnel Increase Cost Summary

Type of Position	Modular Cost per Position (\$000)	Number of Positions Requested	FY 2014 Request (\$000)	FY 2015 Net Annualization (change from 2014) (\$000)	FY 2016 Net Annualization (change from 2015) (\$000)
Attorney	\$114	9	\$1,026	\$972	\$0
Professional	\$63	9	\$567	\$396	\$441
Expert Professional	\$94	4	\$376	\$340	\$108
Clerical	\$52	3	\$156	\$120	\$0
Total Personnel	n/a	25	\$2,125	\$1,828	\$549

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2014 Request (\$000)	FY 2015 Net Annualization (change from 2014) (\$000)	FY 2016 Net Annualization (change from 2015) (\$000)
International Case Travel	n/a	n/a	\$55	\$55	\$0
Equipment	n/a	n/a	\$400	\$0	\$0
Total Non-Personnel	n/a	n/a	\$455	\$55	\$0

Total Request for this Item

	Pos	Atty	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)	FY 2015 Net Annualization (change from 2014) (\$000)	FY 2016 Net Annualization (change from 2015) (\$000)
Current Services	122	79	95	n/a	n/a	27,891	n/a	n/a
Increases	25	9	14	\$2,125	\$455	\$2,580	\$1,883	\$549
Grand Total	147	88	109	\$2,125	\$455	\$30,471	\$1,883	\$549

Item Name: **Financial and Mortgage Fraud Initiative**

Budget Decision Unit: Enforcing Federal Criminal Laws

Strategic Goal(s) & Objective(s): Goal 2: Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law
Objective 2.4: Combat corruption, economic crimes, and international organized crime

Organizational Program: Criminal Division

Component Ranking of Item: 2 of 3

Program Increase: Positions 28 Atty 16 FTE 14 Dollars \$5,000,000

Description of Item

Losses in financial fraud cases have ranged from millions of dollars to billions of dollars and have resulted in thousands of workers losing their jobs. Mortgage fraud and foreclosure rescue scams routinely involve millions of dollars in losses and multiple defendants, including mortgage brokers, real estate agents, appraisers, closing agents, and false buyers and sellers who receive kickbacks. It is imperative that the Department enforce the laws that protect the integrity of our financial system.

Without the commitment of additional resources, the Department's expanding fraud caseload will outstrip its ability to handle such matters effectively and efficiently. To that end, the FY 2013 President's Budget includes a program enhancement of 28 positions (including 16 attorneys) and \$5,000,000 for the Criminal Division. These resources will enable the Department to hold accountable criminals who perpetrate financial and mortgage fraud, deter future perpetrators of fraud, and recover monies stolen from the U.S. taxpayer.

Justification

The Criminal Division will use its requested resources to prosecute the most significant financial crimes, including mortgage fraud, corporate fraud, and sophisticated investment fraud; coordinate multi-district financial crime cases; and assist U.S. Attorneys' Offices (USAOs) in financial crime cases with significant money laundering and asset forfeiture components.

Financial Institution and Mortgage Fraud

As a result of the financial crisis, a new spotlight has been placed on the importance of prosecuting and deterring mortgage fraud, which injures numerous homeowner victims and prospective home buyers, threatens the financial integrity of banks and financial services firms, and creates risks in the financial system.

The Criminal Division continues to investigate and prosecute numerous mortgage fraud cases across the country, including complex, multi-district mortgage fraud schemes. These cases require significant prosecutorial resources. They are document intensive and multi-jurisdictional. They involve sophisticated techniques used to conceal fraudulent schemes designed to obtain financing. In one case handled by the Criminal Division, 27 individuals have pled guilty and 11 more have been charged, as of January 2013, in a massive six-year mortgage fraud scheme in which conspirators fraudulently gained control of condominium homeowners' associations ("HOA") in the Las Vegas area, so that the HOAs would direct business to a certain law firm and construction company. In another case, Criminal Division prosecutors obtained four guilty pleas in October 2012 relating to a \$27 million scheme perpetrated by executives of American Mortgage Specialists, Inc. ("AMS"), a Phoenix corporation, to defraud BNC National Bank in North Dakota by, among other things, obtaining funds provided by the Bank through a lending arrangement and then falsely reporting to the Bank the value of AMS's secondary mortgage loan sales. In yet another case prosecuted in 2012, the Criminal Division obtained the guilty plea of a former executive at Lender Processing Services, Inc. ("LPS"), for her role in directing LPS's predecessor company to forge and falsify mortgage-related documents to increase the company's production volume, which generated approximately \$60 million in revenues for the company. LPS also entered into a corporate resolution with the Criminal Division and agreed to monetary penalties and forfeiture totaling \$35 million. In addition to its case work, the Criminal Division continues to play a significant role in the inter-agency Residential Mortgage Backed Securities Working Group, which was formed in 2012. To maintain and increase its response to the pervasive use of sophisticated schemes to exploit the mortgage lending market and be a full partner to other agencies, the Criminal Division will need additional prosecutorial resources.

Corporate Fraud

The Criminal Division is conducting complex corporate fraud investigations involving financial services firms impacting the integrity of the financial system. These cases are challenging: they require experienced white collar prosecutors, sophisticated agents and forensic financial accountants, and the support of an experienced paralegal staff to manage the vast inflow of electronic records. Moreover, corporate executives have become increasingly sophisticated in concealing and limiting their communications to make it harder for prosecutors to find incriminating evidence of their misdeeds. This only increases the need for greater electronic forensic analysis of email and phone records. The need for increased resources is highlighted by several recent corporate resolutions involving the Criminal Division, which required the resources of numerous Criminal Division prosecutors. In 2012 and early 2013, the Criminal Division entered into corporate resolutions with Barclays Bank, the Royal Bank of Scotland ("RBS"), and UBS AG, and also entered into guilty pleas with the Japanese subsidiaries of RBS and UBS, for their roles in the global manipulation of reported benchmark interest rates. These resolutions collectively involved the imposition of over \$800 million in monetary penalties and criminal fines. If the Criminal Division is to continue to effectively prosecute corporate fraud in the financial system, it will require increased prosecutorial and paralegal resources.

Sophisticated Investment Frauds

The Criminal Division is investigating and prosecuting large investment fraud schemes (sometimes known as "Ponzi" schemes) that result in injuries to thousands of innocent,

vulnerable investors. Often times, investors are robbed of their life savings in schemes that result in hundreds of millions of dollars in investor losses. These investment fraud schemes are increasingly sophisticated, relying on the use of sham partnerships, corporations and investment vehicles. In addition, these schemes are nationwide and even transnational. In 2012, for example, the Criminal Division obtained the convictions of Robert Allen Stanford and three other individuals for their roles in a massive multi-billion dollar Ponzi scheme involving the fraudulent sale of certificates of deposit issued by the Stanford International Bank to thousands of investors in the United States, Latin America and elsewhere. The scheme involved significant Criminal Division resources, including the involvement of numerous attorneys and paralegals and the retention of a major consulting firm to assist in the challenging task of forensic accounting for the funds obtained from investors. In order to protect Main Street investors from these financial predators, increased investigative and prosecutorial resources are required.

Resources Needed for Effective Support of Prosecutions

Investigators: In-house investigators are necessary to assist prosecutors in investigating financial and mortgage fraud. These investigators would analyze records and databases, identify illicit patterns of activity, seek additional information on suspicious persons and entities, analyze electronic communications among co-conspirators, assist in obtaining electronic evidence from service providers, and assist in preparing for trial by investigating the backgrounds of defense witnesses. As noted above, mortgage and investment fraud schemes prosecuted by the Division are increasingly complex, involving layers of sham partnerships and corporations, use of multiple accounts, and use of electronic communications between individuals. In-house investigators would be able to assist in analyzing and obtaining such evidence.

Forensic Accountants: A large number of the Division's cases involve the use of bank accounts in the name of shell entities that are set up to purposely evade law enforcement and launder funds. As such, the work of forensic accountants is critical in investigating the illicit flow of funds because of the complexity of the financial transactions. Corporate accounting fraud cases also require forensic accountants to analyze the books, ledgers and journal entries of a corporation. Presently, because of the Division's overwhelming case load, many cases do not have adequate financial forensic support, causing significant delays in the investigation and prosecution of these cases.

Paralegals: The financial and mortgage fraud cases prosecuted and investigated by the Criminal Division involve significant electronic and physical records produced from numerous sources. Multi-defendant cases also entail complex discovery obligations. Paralegals are a critical component in the effective prosecution of these cases. The work of the prosecutors is heavily dependent on skilled paralegal support, particularly in complying with the ever increasing discovery obligations being imposed on DOJ prosecutors. Paralegals also assist in drafting subpoena requests and requests for evidence from foreign jurisdictions. Thus, increased paralegal staffing is required to support the work of the Division's attorneys.

Clerical Support: For all the reasons stated above, the Division will also require the support of clerical support personnel. These clerical personnel will support attorneys and other staff in the administrative functions of travel, reimbursements, time keeping, correspondence, photocopying, filing, and other routine administrative matters. By employing three additional clerical support positions, attorneys would be able to focus on their case work.

Litigation Support: Given the change in which documents are electronically stored, criminal investigations and prosecutions now involve an overwhelming volume of documents that must be scanned and reviewed, data that must be shared with multiple agencies, and the use of expert witnesses and consultants to support the government’s efforts. As the Division takes on more investigations and cases, the Division has to expend resources on contracts that far surpass average case costs. To support the requested attorney and support positions and for this initiative to be successful, the Division must also receive additional litigation support resources.

Impact on Performance (Relationship of Increase to Strategic Goals and Priority Goals)

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: *Combat corruption, economic crimes, and international organized crime.*

By expanding the Division’s ability to target mortgage fraud, corporate fraud, and sophisticated investment fraud, the Division will be able to capitalize on its unique expertise and ability. The U.S. Attorneys’ Offices and all law enforcement agencies will also benefit from the funding of this request, because they rely on the Criminal Division’s expertise and support, particularly in multi-district and transnational financial crime cases. For example, in the HOA mortgage fraud case referenced above, the Criminal Division continues to play a leading role in the ongoing investigation and is a partner to national and local law enforcement agencies in that case. The Criminal Division also is increasingly asked by other agencies to play a leading role in the prosecution of complex multi-district and transnational investment fraud investigations, and additional resources are needed to fulfill that leadership role. We anticipate that this additional funding will enable the Division to continue and enhance these important partnerships to the benefit of the entire nation.

Funding

Base Funding

FY 2012 Enacted				FY 2013 CR				FY 2014 Current Services			
Pos	atty	FTE	\$(000)	Pos	atty	FTE	\$(000)	Pos	atty	FTE	\$(000)
268	178	264	\$63,636	268	178	230	\$64,025	268	178	230	\$62,814

Personnel Reduction Cost Summary

Type of Position	Modular Cost per Position (\$000)	Number of Positions Reduced	FY 2014 Request (\$000)	FY 2015 Net Annualization (change from 2014) (\$000)	FY 2016 Net Annualization (change from 2015) (\$000)
Attorney	\$114	16	\$1,824	\$1,728	\$0
Professional	\$63	9	\$567	\$396	\$441
Clerical	\$52	3	\$156	\$120	\$0
Total Personnel	n/a	28	\$2,547	\$2,244	\$441

Non-Personnel Reduction Cost Summary

Non-Personnel Item	Unit	Quantity	FY 2014 Request (\$000)	FY 2015 Net Annualization (change from 2014) (\$000)	FY 2016 Net Annualization (change from 2015) (\$000)
Litigation Support	n/a	n/a	\$2,453	\$2,453	\$0
Total Non-Personnel	n/a	n/a	\$2,453	\$2,453	\$0

Total Request for this Item

	Pos	Atty	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)	FY 2015 Net Annualization (change from 2014) (\$000)	FY 2016 Net Annualization (change from 2015) (\$000)
Current Services	268	178	230	n/a	n/a	\$62,814	n/a	n/a
Increases	28	16	14	\$2,547	2,453	\$5,000	\$4,697	\$441
Grand Total	296	194	244	\$2,547	\$2,453	\$67,814	\$4,697	\$441

Item Name: **Intellectual Property Enforcement**

Budget Decision Unit: Enforcing Federal Criminal Laws

Strategic Goal(s) & Objective(s): Goal 2: Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law
Objective 2.4: Combat corruption, economic crimes, and international organized crime

Organizational Program: Criminal Division

Component Ranking of Item: 3 of 3

Program Increase: Positions 11 Atty 7 FTE 6 Dollars \$3,500,000

Description of Item

The Criminal Division requests an enhancement of 11 positions (including 7 attorneys), 6 FTE, and \$3,500,000 to place four 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.

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 copyright, 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, until March 2011 (when State Department funding expired), Eastern Europe. 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 four important areas (in order of priority) for the placement of International Computer Hacking and Intellectual Property (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 four 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.

Eastern Europe: There is a large amount of intellectual property and cybercrime in Eastern Europe. Romania would serve as strong base of operations for Eastern Europe because of the significant intellectual property and cybercrime activity within the country and because of the close relationship that exists with Romanian law enforcement. This position would build upon the strong foundation created by the State Department-funded IPLEC who was posted in Sofia, Bulgaria until March 2011.

Latin America: South America has a tremendously high concentration of countries facing serious intellectual property challenges. The 2012 U.S. Trade Representative's (USTR) *Special 301 Report* included Argentina, Chile and Venezuela on the *Priority Watch List*; Bolivia, Brazil, Colombia, Ecuador, and Peru on the *Watch List*, and Paraguay subject to monitoring pursuant to Section 306. Likewise, there is extensive cybercrime in the region. However, there is also strong interest from many governments in the region to improve enforcement efforts and electronic evidence collection. Numerous Latin American countries, for example, have indicated interest in becoming Parties to the Budapest Convention on Cybercrime and in receiving practical enforcement assistance from the U.S. An ICHIP/Attaché placed in Brazil or Argentina, for example, would be well positioned to guide the development of regional coordination of intellectual property and cybercrime enforcement efforts. The ICHIP/Attaché would also provide a link between affected U.S. companies and law enforcement officials responsible for intellectual property and cyber enforcement in the region.

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 is 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 (Relationship of Increase to Strategic Goals and Priority Goals):

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: *Combat corruption, economic crimes, and international 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 Computer Hacking and Intellectual Property (CHIP) Network;
- Replace the IPLEC for Eastern Europe, which will no longer be funded by the State Department; and
- Strengthen the DOJ Attaché program’s ability to address transnational organized crime.

Funding

Base Funding

FY 2012 Enacted				FY 2013 CR				FY 2014 Current Services			
Pos	atty	FTE	\$(000)	Pos	atty	FTE	\$(000)	Pos	atty	FTE	\$(000)
20	17	20	\$4,712	22	18	18	\$5,179	22	18	21	5,081

Personnel Increase Cost Summary

Type of Position	Modular Cost per Position (\$000)	Number of Positions Requested	FY 2014 Request (\$000)	FY 2015 Net Annualization (change from 2014) (\$000)	FY 2016 Net Annualization (change from 2015) (\$000)
Foreign Attorney	\$475	4	\$1,900	\$704	\$0
Attorney	\$114	3	\$342	\$324	\$0
Professional	\$63	4	\$252	\$176	\$196
Total Personnel	n/a	11	\$2,494	\$1,204	\$196

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2014 Request (\$000)	FY 2015 Net Annualization (Change from 2014) (\$000)	FY 2016 Net Annualization (Change from 2015) (\$000)
FSN	\$59	4	\$236	\$0	\$0
Travel	n/a	n/a	\$259	\$259	\$0
Training	n/a	n/a	\$511	\$511	\$0
Total Non-Personnel	n/a	n/a	1,006	\$770	\$0

Total Request for this Item

	Pos	Atty	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)	FY 2015 Net Annualization (Change from 2014) (\$000)	FY 2016 Net Annualization (Change from 2015) (\$000)
Current Services	22	18	21	n/a	n/a	\$5,081	n/a	n/a

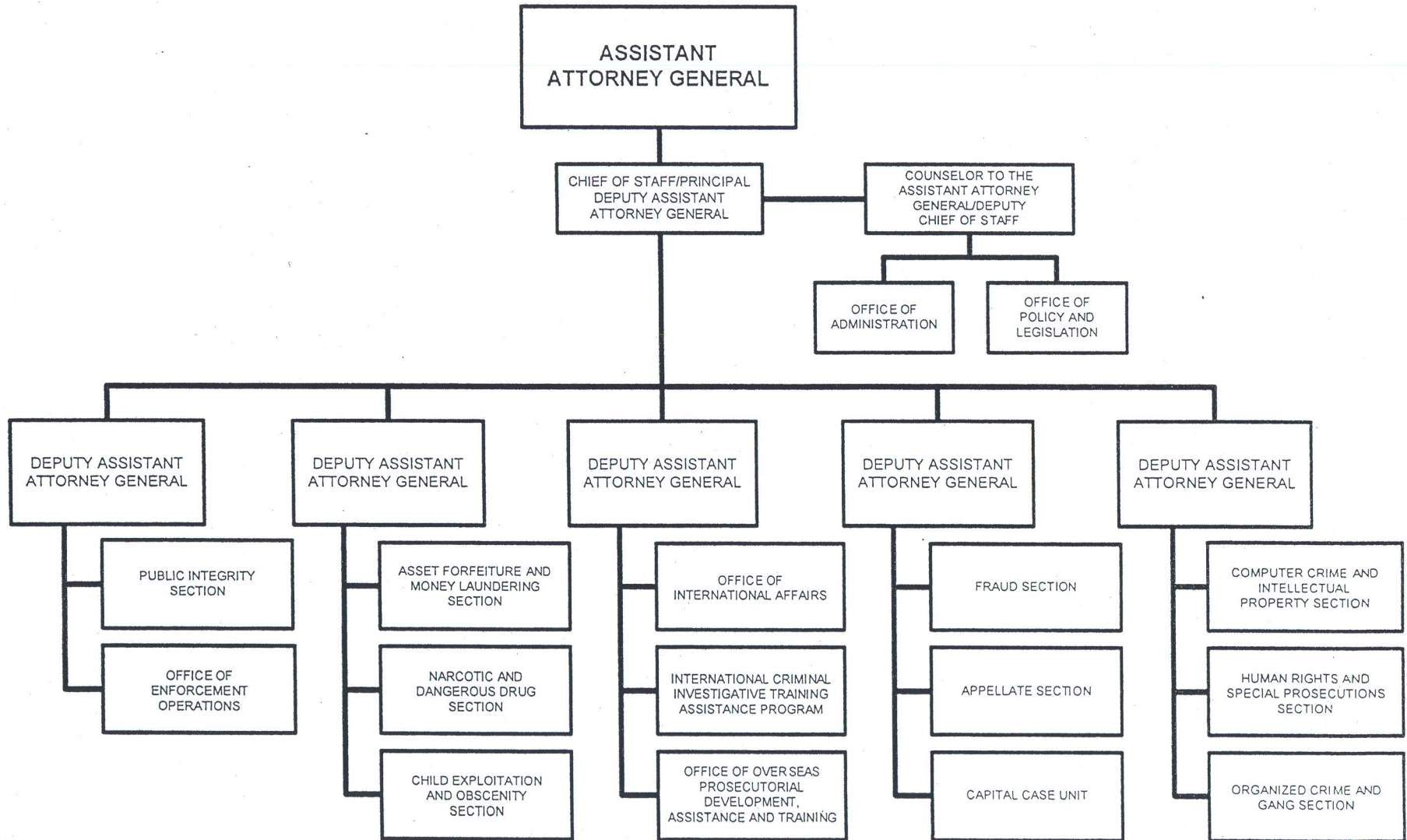
Increases	11	7	6	\$2,494	\$1,006	\$3,500	\$1,974	\$196
Grand Total	33	25	27	\$2,494	\$1,006	\$8,581	\$1,974	\$196

VI. Program Offsets by Item – N/A

VII. Exhibits – Please see attached

A. Organizational Chart

CRIMINAL DIVISION



Approved by

ERIC H. HOLDER, JR.
Attorney General

Date: 10/04/10

B. Summary of Requirements

Summary of Requirements

Criminal Division
Salaries and Expenses
(Dollars in Thousands)

	FY 2014 Request		
	Direct Pos.	Estimate FTE	Amount
2012 Enacted	751	748	174,000
2013 Continuing Resolution			
2013 CR 0.612% Increase			1,065
Total 2013 Continuing Resolution	751	670	175,065
Technical Adjustments			
Adjustment - 2013 CR 0.612%	0	0	-1,065
Total Technical Adjustments	0	0	-1,065
Base Adjustments			
Transfers:			
Transfers - JCON and JCON S/TS	0	0	694
Transfers -Office and Information Policy (OIP)	0	0	-154
Transfers - Office of Tribal Justice (OTJ)	-1	-1	-336
Transfers - Professional Responsibility Advisory Office (PRAO)	0	0	-174
Pay and Benefits	0	0	1,225
Domestic Rent and Facilities	0	0	-1,319
Foreign Expenses	0	0	-2,517
Total Base Adjustments	-1	-1	-2,581
Total Technical and Base Adjustments	-1	-1	-3,646
2014 Current Services	750	669	171,419
Program Changes			
Increases:			
Cyber Security	25	14	2,580
Financial and Mortgage Fraud	28	14	5,000
Intellectual Property	11	6	3,500
Subtotal, Increases	64	34	11,080
Total Program Changes	64	34	11,080
2014 Total Request	814	703	182,499
2012 - 2014 Total Change	63	-45	8,499

Note: The FTE for FY 2012 is actual and for FY 2013 and FY 2014 are estimates.

B. Summary of Requirements

Summary of Requirements

Criminal Division
Salaries and Expenses
(Dollars in Thousands)

Program Activity	2012 Appropriation Enacted			2013 Continuing Resolution *			2014 Technical and Base Adjustments			2014 Current Services		
	Direct Pos.	Actual FTE	Amount	Direct Pos.	Est. FTE	Amount	Direct Pos.	Est. FTE	Amount	Direct Pos.	Est. FTE	Amount
Enforcing Federal Criminal Laws	751	686	174,000	751	670	175,065	-1	-1	-3,646	750	669	171,419
Total Direct	751	686	174,000	751	670	175,065	-1	-1	-3,646	750	669	171,419
Balance Rescission			0			0			0			0
Total Direct with Rescission			174,000			175,065			-3,646			171,419
Reimbursable FTE		268			282			0			282	
Total Direct and Reimb. FTE		954			952			-1			951	
Other FTE:												
LEAP		0			0			0			0	
Overtime		[2]			[2]			0			[2]	
Grand Total, FTE		954			952			-1			951	

Program Activity	2014 Increases			2014 Offsets			2014 Request		
	Direct Pos.	Est. FTE	Amount	Direct Pos.	Est. FTE	Amount	Direct Pos.	Est. FTE	Amount
Enforcing Federal Criminal Laws	64	34	11,080	0	0	0	814	703	182,499
Total Direct	64	34	11,080	0	0	0	814	703	182,499
Balance Rescission			0			0			0
Total Direct with Rescission			11,080			0			182,499
Reimbursable FTE		0			0			282	
Total Direct and Reimb. FTE		34			0			985	
Other FTE:								0	
LEAP		0			0			0	
Overtime		0			0			[2]	
Grand Total, FTE		34			0			985	

*The 2013 Continuing Resolution includes the 0.612% funding provided by the Continuing Appropriations Resolution, 2013 (P.L. 112-175, Section 101(c)).

C. Program Changes by Decision Unit

FY 2014 Program Increases/Offsets by Decision Unit

Criminal Division
Salaries and Expenses
(Dollars in Thousands)

Program Increases	Location of Description by Program Activity	Enforcing Federal Criminal Laws				Total Increases			
		Direct Pos.	Agt./ Atty.	Est. FTE	Amount	Direct Pos.	Agt./ Atty.	Est. FTE	Amount
Cyber Security	Enforcing Federal Criminal Laws	25	9	14	2,580	25	9	14	2,580
Financial and Mortgage Fraud	Enforcing Federal Criminal Laws	28	16	14	5,000	28	16	14	5,000
Intellectual Property	Enforcing Federal Criminal Laws	11	7	6	3,500	11	7	6	3,500
Total Program Increases		64	32	34	11,080	64	32	34	11,080

D. Resources by DOJ Strategic Goal and Strategic Objective

Resources by Department of Justice Strategic Goal/Objective

Criminal Division
Salaries and Expenses
(Dollars in Thousands)

Strategic Goal and Strategic Objective	2012 Appropriation Enacted		2013 Continuing Resolution *		2014 Current Services		2014 Increases		2014 Offsets		2014 Total Request	
	Direct/Reimb FTE	Direct Amount	Direct/Reimb FTE	Direct Amount	Direct/Reimb FTE	Direct Amount	Direct/Reimb FTE	Direct Amount	Direct/Reimb FTE	Direct Amount	Direct/Reimb FTE	Direct Amount
Goal 1 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.	50	8,334	46	6,401	46	6,267	0	0	0	0	46	6,267
1.2 Prosecute those involved in terrorist acts.	83	11,209	28	7,048	28	6,905	3	464	0	0	31	7,369
Subtotal, Goal 1	133	19,543	74	13,449	74	13,172	3	464	0	0	77	13,636
Goal 2 Prevent Crime, Protect the Rights of the American People, and enforce Federal Law												
2.1 Combat the threat, incidence, and prevalence of violent crime.	138	27,130	147	30,815	147	30,159	0	0	0	0	147	30,159
2.2 Prevent and intervene in crimes against vulnerable of violent crim	67	15,906	86	20,639	86	20,205	0	0	0	0	86	20,205
2.3 Combat the threat, trafficking, and use of illegal drugs and the div	222	39,536	208	35,920	207	35,176	0	0	0	0	207	35,176
2.4 Combat corruption, economic crimes, and international organized crime.	365	70,768	360	66,298	360	64,936	31	10,616	0	0	391	75,552
2.5 Promote and protect Americans' civil rights.	29	1,117	8	1,069	8	1,046	0	0	0	0	8	1,046
Subtotal, Goal 2	821	154,457	809	154,741	808	151,522	31	10,616	0	0	839	162,138
Goal 3 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 relationship and strategies for the administration of justice with state, local, tribal and international law enforcement.	0	0	69	6,875	69	6,725	0	0	0	0	69	6,725
Subtotal, Goal 3	0	0	69	6,875	69	6,725	0	0	0	0	69	6,725
TOTAL	954	174,000	952	175,065	951	171,419	34	11,080	0	0	985	182,499

Note: Excludes Balance Rescission and/or Supplemental Appropriations.

*The 2013 Continuing Resolution includes the 0.612% funding provided by the Continuing Appropriations Resolution, 2013 (P.L. 112-175, Section 101 (c)).

E. Justification for Technical and Base Adjustments

Justifications for Technical and Base Adjustments

Criminal Division
Salaries and Expenses
(Dollars in Thousands)

	Direct Pos.	Estimate FTE	Amount
Technical Adjustments			
1 <u>Adjustment - 2013 CR 0.612%:</u> PL 112-175 section 101 (c) provided 0.612% across the board increase above the current rate for the 2013 CR funding level. This adjustment reverses this increase.	0	0	-1,065
Subtotal, Technical Adjustments	0	0	-1,065
Transfers			
1 <u>Transfer of JCON and JCON S/TS to the Criminal Division.</u> A transfer of \$694,000 to the Criminal Division is included in support of the Department's Justice Consolidated Office Network (JCON) and JCON S/TS programs which, will be moved to the Working Capital Fund and provided as a billable service in FY 2013.	0	0	694
2 <u>Transfer to Office of Information Policy (OIP).</u> The component transfers for the Office of Information Policy (OIP) into the General Administration appropriation will centralize appropriated funding and eliminate the current reimbursable financing process. The centralization of the funding is administratively advantageous because it eliminates the paper-intensive reimbursement process. The FY 2013 transfer amounts for OIP are based on the FY 2010 actual costs plus standard inflation per year (the average increase over the past three years) to bridge to FY 2013 amounts. The amount per component is based on the average percentage of total costs paid by that component since 2007.	0	0	-154
3 <u>Transfer to Office of Tribal Justice (OTJ).</u> This request transfers 1 attorney position, 1 FTE, and \$336,000 from the Criminal Division to the Office of Tribal Justice. These funds will be transferred to the General Administration appropriation based on Department guidance.	-1	-1	-336
4 <u>Transfer to Professional Responsibility Advisory Office (PRAO).</u> The component transfers for the Professional Responsibility Advisory Office (PRAO) into the General Administration appropriation will centralize appropriated funding and eliminate the current reimbursable financing process. The centralization of the funding is administratively advantageous because it eliminates the paper-intensive reimbursement process. The FY 2013 transfer amounts for PRAO are based on the FY 2010 actual costs plus standard inflation per year (the average increase over the past three years) to bridge to FY 2013 amounts. The amount per component is based on the average percentage of total costs paid by that component since 2007.	0	0	-174
Subtotal, Transfers	-1	-1	30
Pay and Benefits			
1 <u>2014 Pay Raise:</u> This request provides for a proposed 1 percent pay raise to be effective in January of 2014. The amount request, \$820,000, represents the pay amounts for 3/4 of the fiscal year plus appropriate benefits (\$607,000 for pay and \$213,000 for benefits.)			820
2 <u>Annualization of 2013 Pay Raise:</u> This pay annualization represents first quarter amounts (October through December) of the 2013 pay increase of 0.5% included in the 2013 President's Budget. The amount requested \$142,000, represents the pay amounts for 1/4 of the fiscal year plus appropriate benefits (\$105,000 for pay and \$37,000 for benefits).			142
3 <u>Employee Compensation Fund:</u> The \$17,000 request reflects anticipated changes in payments to the Department of Labor for injury benefits under the Federal Employee Compensation Act.			17

E. Justification for Technical and Base Adjustments

Justifications for Technical and Base Adjustments

Criminal Division
Salaries and Expenses
(Dollars in Thousands)

	Direct Pos.	Estimate FTE	Amount
<p>4 <u>Health Insurance:</u> Effective January 2014, the component's contribution to Federal employees' health insurance increases by XX percent. Applied against the 2013 estimate of \$4,737,000, the additional amount required is \$129,000.</p>			129
<p>5 <u>Retirement:</u> Agency retirement contributions increase as employees under CSRS retire and are replaced by FERS employees. Based on U.S. Department of Justice Agency estimates, we project that the DOJ workforce will convert from CSRS to FERS at a rate of 1.3 percent per year. The requested increase of \$117,000 is necessary to meet our increased retirement obligations as a result of this conversion.</p>			117
Subtotal, Pay and Benefits	0	0	1,225
Domestic Rent and Facilities			
<p>1 <u>General Services Administration (GSA) Rent:</u> GSA will continue to charge rental rates that approximate those charged to commercial tenants for equivalent space and related services. The requested decrease of \$948,000 is required to meet our commitment to GSA. The costs associated with GSA rent were derived through the use of an automated system, which uses the latest inventory data, including rate increases to be effective FY 2014 for each building currently occupied by Department of Justice components, as well as the costs of new space to be occupied. GSA provides data on the rate decrease.</p>			-948
<p>2 <u>Guard Services:</u> This includes Department of Homeland Security (DHS) Federal Protective Service charges, Justice Protective Service charges and other security services across the country. The requested decrease of \$371,000 is required to meet these commitments.</p>			-371
Subtotal, Domestic Rent and Facilities	0	0	-1,319
Foreign Expenses			
<p>1 <u>Education Allowance:</u> For employees stationed abroad, components are obligated to meet the educational expenses incurred by an employee in providing adequate elementary (grades K-8) and secondary (grades 9-12) education for dependent children at post. \$46,000 reflects the decrease in cost to support existing staffing levels.</p>			-46
<p>2 <u>International Cooperative Administrative Support Services (ICASS):</u> Under the ICASS, an annual charge is made by the Department of State for administrative support based on the overseas staff of each federal agency. This request is based on the projected FY 2013 bill for post invoices and other ICASS costs.</p>			2,030
<p>3 <u>Post Allowance - Cost of Living Allowance (COLA):</u> For employees stationed abroad, components are obligated to pay for their COLA. COLA is intended to reimburse certain excess costs and to compensate the employee for serving at a post where the cost of living, excluding the cost of quarters and the cost of education for eligible family members, is substantially higher than in the Washington, D.C. area. \$104,000 reflects the increase in cost to support existing staffing levels.</p>			104

E. Justification for Technical and Base Adjustments

Justifications for Technical and Base Adjustments

Criminal Division
 Salaries and Expenses
 (Dollars in Thousands)

	Direct Pos.	Estimate FTE	Amount
<p>4 Overseas Capital Security Cost Sharing (CSCS): The Department of State (DOS) is in the midst of a multi-year capital security construction program, with a plan to build and maintain new diplomatic and consular compounds that meet security requirements set by the Secure Embassies Construction Act. As authorized by P.L. 108-447 and subsequent acts, "all agencies with personnel overseas subject to chief of mission authority...shall participate and provide funding in advance for their share of costs of providing new, safe, secure U.S. diplomatic facilities, without offsets, on the basis of the total overseas presence of each agency as determined by the Secretary of State." Originally authorized for FY2000-2004, the program has been extended annually by OMB and Congress and has also been expanded beyond new embassy construction to include maintenance and renovation costs of the new facilities also. For the purpose of this program, DOS's personnel totals for DOJ include current and projected staffing. The estimated cost to the Department, as provided by DOS, for FY 2014 is \$79,069,370. The Criminal Division currently has 14 positions overseas, and a funding decrease of \$4,605,000 is requested for this account.</p>			-4,605
Subtotal, Foreign Expenses	0	0	-2,517
TOTAL DIRECT TECHNICAL and BASE ADJUSTMENTS	-1	-1	-3,646

F. Crosswalk of 2012 Availability

Crosswalk of 2012 Availability

Criminal Division
Salaries and Expenses
(Dollars in Thousands)

Program Activity	2012 Appropriation Enacted w/o Balance Rescission			Balance Rescission			Reprogramming/Transfers			Carryover	Recoveries/ Refunds	2012 Availability		
	Direct Pos.	Actual FTE	Amount	Direct Pos.	Actual FTE	Amount	Direct Pos.	Actual FTE	Amount	Amount	Amount	Direct Pos.	Actual FTE	Amount
Enforcing Federal Criminal Laws	751	686	174,000	0	0	0	0	0	-269	4,367	5	751	686	178,103
Total Direct	751	686	174,000	0	0	0	0	0	-269	4,367	5	751	686	178,103
Reimbursable FTE		268			0			0					268	
Total Direct and Reimb. FTE		954			0			0					954	
Other FTE:														
LEAP		0			0			0					0	
Overtime		[2]			0			0					[2]	
Grand Total, FTE		954			0			0					954	

Reprogramming/Transfers

The Criminal Division reprogrammed FARA unobligated balances of \$269,000 to GLA's ALS account.

Carryover:

Funding includes \$269,00 for FARA; \$297,000 for ALS; \$2,600,00 for Afghanistan training; and \$1,201,000 for Deepwater horizon Fraud Task Force.

Recoveries/Refunds:

Funding includes \$5,000 for ALS.

G. Crosswalk of 2013 Availability

Crosswalk of 2013 Availability

Criminal Division
Salaries and Expenses
(Dollars in Thousands)

Program Activity	FY 2013 Continuing Resolution			Supplemental Appropriation Amount	Reprogramming/Transfers			Carryover Amount	Recoveries/ Refunds Amount	2013 Availability		
	Direct Pos.	Estim. FTE	Amount		Direct Pos.	Estim. FTE	Amount			Direct Pos.	Estim. FTE	Amount
Enforcing Federal Criminal Laws	751	670	175,065	0	0	0	424	1	751	670	175,490	
Total Direct	751	670	175,065	0	0	0	424	1	751	670	175,490	
Balance Rescission			0								0	
Total Direct with Rescission			175,065								175,490	
Reimbursable FTE		282				0					282	
Total Direct and Reimb. FTE		952				0					952	
Other FTE:												
LEAP		0				0					0	
Overtime		[2]				0				[2]		
Grand Total, FTE		952				0					952	

Carryover:

Funding includes \$143,000 for ALS and \$281,000 for Deepwater Horizon Fraud Task Force.

Recoveries/Refunds:

Funding includes \$1,000 for ALS

*The 2013 Continuing Resolution includes the 0.612% funding provided by the Continuing Appropriations Resolution, 2013 (P.L. 112-175, Section 101 (c)).

H. Summary of Reimbursable Resources

Summary of Reimbursable Resources

Criminal Division
Salaries and Expenses
(Dollars in Thousands)

Collections by Source	2012 Actual			2013 Planned			2014 Request			Increase/Decrease		
	Reimb. Pos.	Reimb. FTE	Amount	Reimb. Pos.	Reimb. FTE	Amount	Reimb. Pos.	Reimb. FTE	Amount	Reimb. Pos.	Reimb. FTE	Amount
U.S. Department of State	145	146	147,586	183	149	179,265	183	149	188,200	0	0	8,935
Interagency Crime and Drug Enforcement	13	13	2,072	13	13	2,072	13	13	2,086	0	0	14
Asset Forfeiture Fund	78	72	8,484	90	77	31,808	90	77	34,000	0	0	2,192
All Other Sources	40	37	29,298	57	43	29,109	57	43	34,125	0	0	5,016
Budgetary Resources	276	268	187,440	343	282	242,254	343	282	258,411	0	0	16,157

Obligations by Program Activity	2012 Actual			2013 Planned			2014 Request			Increase/Decrease		
	Reimb. Pos.	Reimb. FTE	Amount	Reimb. Pos.	Reimb. FTE	Amount	Reimb. Pos.	Reimb. FTE	Amount	Reimb. Pos.	Reimb. FTE	Amount
U.S. Department of State	145	146	147,586	183	149	179,265	183	149	188,200	0	0	8,935
Interagency Crime and Drug Enforcement	13	13	2,072	13	13	2,072	13	13	2,086	0	0	14
Asset Forfeiture Fund	78	72	8,484	90	77	31,808	90	77	34,000	0	0	2,192
All Other Sources	40	37	29,298	57	43	29,109	57	43	34,125	0	0	5,016
Budgetary Resources	276	268	187,440	343	282	242,254	343	282	258,411	0	0	16,157

I. Detail of Permanent Positions by Category

Detail of Permanent Positions by Category

Criminal Division
Salaries and Expenses
(Dollars in Thousands)

Category	2012 Appropriation Enacted with Balance Rescissions		2013 Continuing Resolution		2014 Request				
	Direct Pos.	Reimb. Pos.	Direct Pos.	Reimb. Pos.	ATBs	Program Increases	Program Offsets	Total Direct Pos.	Total Reimb. Pos.
Miscellaneous Operations (010-099)	1	0	1	0	0	0	0	1	0
Security Specialists (080)	20	0	20	0	0	0	0	20	0
Intelligence Series (132)	1	0	1	0	0	0	0	1	0
Personnel Management (200-299)	10	0	10	0	0	0	0	10	0
Clerical and Office Services (300-399)	148	81	148	81	0	6	0	154	81
Accounting and Budget (500-599)	10	35	10	35	0	4	0	14	35
Attorneys (905)	440	195	440	195	-1	32	0	471	195
Paralegals / Other Law (900-998)	90	25	90	25	0	12	0	102	25
Information & Arts (1000-1099)	1	1	1	1	0	0	0	1	1
Business & Industry (1100-1199)	2	0	2	0	0	0	0	2	0
Library (1400-1499)	4	0	4	0	0	0	0	4	0
Forensic Scientist (1301)	0	4	0	4	0	0	0	0	4
Miscellaneous Inspectors Series (1801-1802)	0	0	0	0	0	3	0	3	0
Travel Services (2101)	0	1	0	1	0	0	0	0	1
Information Technology Mgmt (2210)	24	1	24	1		7	0	31	1
Total	751	343	751	343	-1	64	0	814	343
Headquarters (Washington, D.C.)	737	210	737	210	-1	60	0	796	210
Foreign Field	14	133	14	133	0	4	0	18	133
Total	751	343	751	343	-1	64	0	814	343

J. Financial Analysis of Program Changes

Financial Analysis of Program Changes

Criminal Division
Salaries and Expenses
(Dollars in Thousands)

Grades	Enforcing Federal Criminal Laws						Total Program Changes	
	Cyber Security		Financial and Mortgage Fraud		Intellectual Property		Direct Pos.	Amount
	Direct Pos.	Amount	Direct Pos.	Amount	Direct Pos.	Amount		
GS-14	9	1,372	16	2,439	7	1,530	32	5,341
GS-13	4	517	0	0	0	0	4	517
GS-9	9	602	9	602	4	267	22	1,471
GS-7	3	165	3	165	0	0	6	330
Total Positions and Annual Amount	25	2,656	28	3,206	11	1,797	64	7,659
Lapse (-)	-11	-1,328	-14	-1,603	-5	-898	-30	-3,829
11.5 Other Personnel Compensation		0		0		86		86
Total FTEs and Personnel Compensation	14	1,328	14	1,603	6	985	34	3,916
13.0 Benefits for former personnel		0		0		0		0
21.0 Travel and Transportation of Persons		114		101		298		513
22.0 Transportation of Things		24		27		11		62
23.1 Rental Payments to GSA		0		0		0		0
23.3 Communications, Utilities, and Miscellaneous Charges		64		72		163		299
24.0 Printing and Reproduction		3		3		1		7
25.1 Advisory and Assistance Services		0		0		0		0
25.2 Other Services from Non-Federal Sources		42		65		867		974
25.3 Other Goods and Services from Federal Sources		153		2,624		659		3,436
25.6 Medical Care		2		2		38		42
25.7 Operation and Maintenance of Equipment		0		0		0		0
26.0 Supplies and Materials		52		59		18		129
31.0 Equipment		798		444		405		1,647
31.0 Buildout		0		0		55		55
Total Program Change Requests	14	2,580	14	5,000	6	3,500	34	11,080

K. Summary of Requirements by Grade

Summary of Requirements by Grade

Criminal Division
Salaries and Expenses
(Dollars in Thousands)

Grades and Salary Ranges				2012 Enacted		2013 Continuing Resolution		2014 Request		Increase/Decrease	
				Direct Pos.	Amount	Direct Pos.	Amount	Direct Pos.	Amount	Direct Pos.	Amount
EX	\$	145,700	- 199,700	1	133	1	133	1	135	0	1
SES/SL	\$	119,554	- 179,700	44	6,582	44	6,615	44	6,681	0	66
GS-15	\$	123,758	- 155,500	396	55,282	396	55,558	395	55,969	-1	411
GS-14	\$	105,211	- 136,771	58	7,018	58	7,053	90	11,053	32	4,000
GS-13	\$	89,033	- 115,742	55	5,632	55	5,660	59	6,132	4	472
GS-12	\$	74,872	- 97,333	41	3,530	41	3,548	41	3,583	0	35
GS-11	\$	62,467	- 81,204	55	3,949	55	3,969	55	4,008	0	39
GS-10	\$	56,857	- 73,917	0	0	0	0	0	0	0	0
GS-9	\$	51,630	- 67,114	45	2,669	45	2,682	67	4,033	22	1,351
GS-8	\$	46,745	- 60,765	20	1,076	20	1,081	20	1,092	0	11
GS-7	\$	42,209	- 54,875	21	1,019	21	1,024	27	1,329	6	306
GS-6	\$	37,983	- 49,375	7	306	7	307	7	310	0	3
GS-5	\$	37,075	- 44,293	4	163	4	164	4	165	0	2
GS-4	\$	30,456	- 39,590	4	140	4	141	4	142	0	1
Total, Appropriated Positions				751	87,498	751	87,935	814	94,634	63	6,699
Average SES Salary					149,627		149,627		149,627		
Average GS Salary					112,972		112,972		113,070		
Average GS Grade					13		13		13		

L. Summary of Requirements by Object Class

Summary of Requirements by Object Class

Criminal Division
Salaries and Expenses
(Dollars in Thousands)

Object Class	2012 Actual		2013 Availability *		2014 Request		Increase/Decrease	
	Direct FTE	Amount	Direct FTE	Amount	Direct FTE	Amount	Direct FTE	Amount
11.1 Full-Time Permanent	617	76,751	603	79,056	636	81,622	33	2,566
11.3 Other than Full-Time Permanent	69	6,432	67	8,700	67	8,702	0	2
11.5 Other Personnel Compensation	0	1,188	0	1,250	0	1,336	0	86
<i>Overtime</i>	[2]	0	[2]	0	[2]	0	[2]	0
<i>Other Compensation</i>	0	0	0	0	0	0	0	0
11.8 Special Personal Services Payments	0	1,858	0	1,900	0	1,900	0	0
Total	686	86,229	670	90,906	703	93,560	33	2,654
Other Object Classes								
12.0 Personnel Benefits		23,957		23,390		24,592		1,202
13.0 Benefits for former personnel		18		50		50		0
21.0 Travel and Transportation of Persons		4,008		4,515		5,029		514
22.0 Transportation of Things		1,469		1,124		1,186		62
23.1 Rental Payments to GSA		25,393		26,197		25,254		-943
23.2 Rental Payments to Others		1,531		1,700		1,700		0
23.3 Communications, Utilities, and Miscellaneous Charges		3,475		3,500		3,800		300
24.0 Printing and Reproduction		83		134		141		7
25.1 Advisory and Assistance Services		2,753		5,110		5,111		1
25.2 Other Services from Non-Federal Sources		11,500		13,877		14,709		832
25.3 Other Goods and Services from Federal Sources		8,503		1,500		2,007		507
25.4 Operation and Maintenance of Facilities		0		0		0		0
25.5 Research and Development Contracts		0		0		0		0
25.6 Medical Care		86		91		133		42
25.7 Operation and Maintenance of Equipment		195		200		200		0
25.8 Subsistence and Support of Persons		0		0		0		0
26.0 Supplies and Materials		1,001		1,196		1,325		129
31.0 Equipment		6,121		2,000		3,647		1,647
32.0 Land and Structures		19		0		55		55
41.0 Grants, Subsidies, and Contributions		0		0		0		0
42.0 Insurance Claims and Indemnities		0		0		0		0
Total Obligations		176,341		175,490		182,499		7,009
Unobligated Balance, Start-of-Year		-4,367		-424		0		424
Transfers/Reprogramming		269		0		0		0
Recoveries/Refunds		-5		-1		0		1
Unobligated End-of-Year, Available		424		0		0		0
Unobligated End-of-Year, Expiring		1,338		0		0		0
Total Direct Requirements	0	174,000	0	175,065	0	182,499	0	7,434
Reimbursable FTE								
Full-Time Permanent	268		282		282		0	
23.1 Rental Payments to GSA (Reimbursable)		3,714		2,450		2,499		49
25.3 Other Goods and Services from Federal Sources - DHS Security (Reimbursable)		19		30		31		1

*The 2013 Availability includes the 0.612% funding provided by the Continuing Appropriations Resolution, 2013 (P.L. 112-175, Section 101 (c)).