

**FY 2014
Performance Budget
Congressional Submission**



NATIONAL SECURITY DIVISION

U.S. Department of Justice

Table of Contents

I. Overview.....	1
II. Summary of Program Changes	7
III. Appropriations Language and Analysis of Appropriations Language	8
IV. Program Activity Justification	9
National Security Division	
1. Program Description	9
2. Performance Tables	12
3. Performance, Resources, and Strategies	15
V. Program Increases by Item	28
A. Combating Cyber Threats to National Security	28
B. Combating Homegrown Violent Extremist Threats.....	37
C. Intelligence Collection and Oversight.....	39
VI. Program Offsets by Item (Not Applicable)	
VII. Exhibits	
A. Organizational Chart	
B. Summary of Requirements	
C. FY 2014 Program Increases/Offsets by Decision Unit	
D. Resources by DOJ Strategic Goal and Strategic Objective	
E. Justification for Base Adjustments	
F. Crosswalk of 2012 Availability	
G. Crosswalk of 2013 Availability	
H. Summary of Reimbursable Resources (Not Applicable)	
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 National Security Division

A. Introduction

The National Security Division (NSD) is responsible for combating terrorism and other threats to the national security—the Department of Justice’s (DOJ’s) highest priority. To sustain mission needs, NSD requests for FY 2014 a total of 389 positions (including 256 attorneys), 325 FTE, and \$96,240,000. This request includes growth of approximately 8% in positions and 10% in total funding – a total change of 30 positions, 21 FTE, and \$8,708,000.¹

Electronic copies of the Department of Justice’s Congressional Budget Justifications, 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. Background

Earlier this year, NSD engaged in a comprehensive strategic assessment of the Division’s current operations and future requirements. As a result of that assessment, NSD has outlined four areas of new or renewed focus that will guide its operations in the coming years. They are:

- Combating cyber threats to the national security and protecting national security assets;
- Enhancing NSD’s intelligence programs and expanding its intelligence oversight function;
- Continuing to bring an all-tools, integrated approach to NSD’s work, while also adapting to address the changing face of terrorism; and
- Reinvigorating NSD’s development into a mature Division – capable of keeping pace with its national security partners and outpacing the threats this nation faces.

All of the program increases reflected in NSD’s FY 14 request map to these strategic goals and priorities and will ensure that NSD remains best positioned to fulfill the Department’s top priority mission in the face of increasing challenges and a growing and evolving threat. NSD’s assessment of the challenges inherent in fully realizing its goals in these areas are outlined more fully in section I.D. Performance Challenges, below.

Division Structure

The NSD consolidates within a single Division the Department’s primary national security elements outside of the Federal Bureau of Investigation (FBI), which currently are the:

¹ Within the totals outlined above, NSD has included a total of 9 positions, 9 FTE, and \$11,150,000 for Information Technology (IT).

- Office of Intelligence (OI);
- Counterterrorism Section (CTS);
- Counterespionage Section (CES);
- Law and Policy Office (L&P); and
- Office of Justice for Victims of Overseas Terrorism (OVT).

This organizational structure strengthens the effectiveness of the Department's national security efforts by ensuring greater coordination and unity of purpose between prosecutors, law enforcement agencies, intelligence attorneys, and the Intelligence Community (IC).

NSD Major Responsibilities

Intelligence Operations and Litigation

- Ensuring that IC agencies have the legal tools necessary to conduct intelligence operations.
- Representing the United States before the Foreign Intelligence Surveillance Court (FISC) to obtain authorization under the Foreign Intelligence Surveillance Act (FISA) for government agencies to conduct intelligence collection activities;
- Coordinating and supervising intelligence-related litigation matters, including the evaluation and review of requests to use information collected under FISA in criminal and non-criminal proceedings and to disseminate FISA information; and
- Serving as the Department's primary liaison to the Director of National Intelligence and the IC.

Counterterrorism

- Promoting and overseeing a coordinated national counterterrorism enforcement program, through close collaboration with Department leadership, the National Security Branch of the FBI, the IC, and the 94 United States Attorneys' Offices (USAOs);
- Developing national strategies for combating emerging and evolving terrorism threats, including the threat of cyber-based terrorism;
- Overseeing and supporting the Anti-Terrorism Advisory Council (ATAC) program by: 1) collaborating with prosecutors nationwide on terrorism matters, cases, and threat information; 2) maintaining an essential communication network between the Department and USAOs for the rapid transmission of information on terrorism threats and investigative activity; and 3) managing and supporting ATAC activities and initiatives;
- Consulting, advising, and collaborating with prosecutors nationwide on international and domestic terrorism investigations, prosecutions, and appeals, including the use of classified evidence through the application of the Classified Information Procedures Act (CIPA);

- Sharing information with and providing advice to international prosecutors, agents, and investigating magistrates to assist in addressing international threat information and litigation initiatives; and
- Managing DOJ's work on counter-terrorist financing programs, including supporting the process for designating Foreign Terrorist Organizations and Specially Designated Global Terrorists as well as staffing U.S. Government efforts on the Financial Action Task Force.

Counterespionage

- Supporting and supervising the investigation and prosecution of espionage and related cases through coordinated efforts and close collaboration with Department leadership, the FBI, the IC, and the 94 USAOs;
- Developing national strategies for combating the emerging and evolving threat of cyber-based espionage and state-sponsored cyber intrusions;
- Assisting in and overseeing the expansion of investigations and prosecutions into the unlawful export of military and strategic commodities and technology, including by assisting and providing guidance to USAOs in the establishment of Export Control Proliferation Task Forces;
- Coordinating and providing advice in connection with cases involving the unauthorized disclosure of classified information and supporting resulting prosecutions by providing advice and assistance with the application of CIPA; and
- Enforcing the Foreign Agents Registration Act of 1938 (FARA) and related disclosure statutes.

Oversight and Reporting

- Overseeing certain foreign intelligence, counterintelligence, and other national security activities of IC components to ensure compliance with the Constitution, statutes, and Executive Branch policies to protect individual privacy and civil liberties;
- Monitoring certain intelligence and counterintelligence activities of the FBI to ensure conformity with applicable laws and regulations, FISC orders, and Department procedures, including the foreign intelligence and national security investigation provisions of the Attorney General's Guidelines for Domestic FBI Operations; and
- Fulfilling statutory, Congressional, and judicial reporting requirements related to intelligence, counterintelligence, and other national security activities.

Policy and Other Legal Issues

- Handling appeals in cases involving national security-related prosecutions, and providing views on appellate issues that may impact national security in other civil, criminal, and military commissions cases;
- Providing legal and policy advice on the national security aspects of cybersecurity policy and cyber-related operational activities;
- Providing advice and support on national security issues that arise in an international context, including assisting in bilateral and multilateral engagements with foreign governments and working to build counterterrorism capacities of foreign governments and enhancing international cooperation;
- Providing advice and support on legislative matters involving national security issues, including developing and commenting on legislation, supporting Departmental engagements with members of Congress and Congressional staff, and preparing testimony for senior Division/Department leadership;
- Providing legal assistance and advice on matters arising under national security laws and policies, and overseeing the development, coordination, and implementation of Department-wide policies with regard to intelligence, counterintelligence, counterterrorism, and other national security matters; handling issues related to classification and declassification of records, records management, and freedom of information requests and related litigation; and
- Developing a training curriculum for prosecutors and investigators on cutting-edge tactics, substantive law, and relevant policies and procedures.

Foreign Investment

- Performing the Department's staff-level work on the Committee on Foreign Investment in the United States (CFIUS), which reviews foreign acquisitions of domestic entities that might affect national security and makes recommendations to the President on whether such transactions are a threat;
- Tracking and monitoring certain transactions that have been approved, including those subject to mitigation agreements, and identifying unreported transactions that might merit CFIUS review;
- Responding to Federal Communication Commission (FCC) requests for the Department's views relating to the national security implications of certain transactions relating to FCC licenses; and
- Tracking and monitoring certain transactions that have been approved pursuant to this process.

Victims of Terrorism

- Through NSD's OVT, prioritizing within the Department the investigation and prosecution of terrorist attacks that have resulted in the deaths and/or injuries of American citizens overseas; and
- Ensuring that the rights of victims and their families are honored and respected, and that victims and their families are supported and informed during the criminal justice process.

NSD Recent Accomplishments (unclassified selections only)

- Conducted a top-to-bottom review of existing efforts to combat cyber threats to the national security (i.e., cyber-based terrorism, cyber-based espionage, and other state-sponsored cyber intrusions) to develop a baseline and chart a strategic vision for the future.
- Established a National Security Cyber Specialist Network to coordinate the Division's work to combat cyber threats to the national security, and to work with other components and the USAOs to ensure that the Department takes an all-tools approach to the problem.
- Selected a liaison to the FBI's National Cyber Investigative Joint Task Force to assist with intelligence-related issues and facilitate exploration of prosecution options.
- Filed 1,745 FISA applications with the FISC in 2011.
- Designated 166 international terrorism events to allow for U.S. victim compensation and reimbursement under the International Terrorism Victim Expense Reimbursement Program (ITVERP).
- Combated the growing threat posed by the illegal foreign acquisition of controlled U.S. military and strategic technologies through the National Export Enforcement Initiative.
- Continued to lead the nation's counterterrorism enforcement program through collaboration with Department leadership, the FBI, the IC, and the USAOs.
- Successfully investigated and prosecuted national security threat actors – specific examples detailed below.
- Managed an increased workload associated with the CFIUS.
- Established a Joint Task Force with the Department of State to be activated in the event of a terrorist incident against American citizens overseas.

C. Full Program Costs

The NSD has a single decision unit. Its program activities include intelligence, counterterrorism, and counterespionage, which are related to DOJ Strategic Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law, and its three Objectives. The costs by program activity include the activity's base funding plus an allocation of management, administration, and L&P overhead costs. The overhead cost is allocated based on the percentage of the total cost comprised by each of the three program activities.

D. Performance Challenges

Protecting the nation's security is the top priority for the Department, and NSD's work is critical to that mission. However, as the threats facing this nation continue to grow and evolve, the challenges NSD must overcome also continue to increase. These challenges include:

1. the recent recognition of an explosive growth of cyber threats to the national security;
2. the changing face of terrorism and the risks posed by homegrown violent extremists;
3. an increasing workload in intelligence operations, litigation, and oversight; and
4. difficulties inherent in supporting the development of a young Division in an ever-changing environment.

Among the most significant challenges that NSD faces is the rapid expansion and evolution of cyber threats to the national security. Representatives from the IC have assessed that the cyber threat may soon surpass that of traditional terrorism, and NSD must be prepared to take lessons learned over the past decade and adapt them to this new threat. Cyber threats, which are highly technical in nature, require time-intensive and complex investigative and prosecutorial work, particularly given their novelty, the difficulties of attribution, challenges presented by electronic evidence, the speed and global span of cyber activity, and the balance between prosecutorial and intelligence-related interests in any given case. To meet this growing threat head on, NSD must equip its personnel with cyber-related skills through additional training while recruiting and hiring individuals with cyber skills who can dedicate themselves full-time to these issues immediately. The window of opportunity for getting ahead of this threat is narrow; closing the gap between our present capabilities and our anticipated needs in the near future will require significant resources and commitment.

The threat posed by terrorism has also evolved, having grown and splintered in recent years. Lone wolves and homegrown violent extremists have grown in national prominence, and identifying and disrupting these isolated actors and their operations pose distinct challenges for investigators and prosecutors.

Given the complexity—and range—of the Department's national security prosecutions and investigations, NSD has seen steady growth in the number of FISA applications filed before the FISC, in requests for assistance in criminal litigation involving FISA-derived information, and in reporting obligations pertaining to national security activities – which ensure that congressional oversight committees are fully informed regarding such activities. This growth has outpaced attrition and has brought workloads, which are unlikely to diminish in the foreseeable future, to historic highs.

E. Environmental Accountability

NSD is committed to environmental wellness and participates in DOJ's green programs.

II. Summary of Program Changes

Item Name	Description				Page
		Pos.	FTE	Dollars (\$000)	
Combating Cyber Threats to National Security	Requesting additional resources for NSD's work related to combating cyber threats to national security.	26	13	\$3,468	28
Combating Homegrown Violent Extremist Threats	Requesting additional resources for NSD's work related to combating homegrown violent extremist threats.	2	1	320	37
Intelligence Collection and Oversight	Requesting additional resources for NSD's work related to intelligence collection and oversight.	2	1	320	39
TOTAL, NSD		30	15	\$4,108	

III. Appropriations Language and Analysis of Appropriations Language

Appropriations Language

SALARIES AND EXPENSES, NATIONAL SECURITY DIVISION

For expenses necessary to carry out the activities of the National Security Division, \$96,240,000, of which not to exceed \$5,000,000 for information technology systems shall remain available until expended: Provided, That notwithstanding section 205 of this Act, upon a determination by the Attorney General that emergent circumstances require additional funding for the activities of the National Security Division, the Attorney General may transfer such amounts to this heading from available appropriations for the current fiscal year for the Department of Justice, as may be necessary to respond to such circumstances: Provided further, That any transfer pursuant to the preceding proviso shall be treated as a reprogramming under section 505 of this Act and shall not be available for obligation or expenditure except in compliance with the procedures set forth in that section.

Analysis of Appropriations Language

Only dollar amount changed. No substantive language changes proposed.

IV. Decision Unit Justification

National Security Division

<i>National Security Division</i>	Perm. Pos.	FTE	Amount
2012 Enacted	359	298	\$87,000,000
2012 Prior Year Balance Rescissions	0	0	0
2012 Enacted w/Rescissions	359	298	87,000,000
2013 Continuing Resolution	359	304	87,532,000
Adjustments to Base and Technical Adjustments	0	6	4,600,000
2014 Current Services	359	310	92,132,000
2014 Program Increases	30	15	4,108,000
2014 Program Offsets	0	0	0
2014 Request	389	325	96,240,000
Total Change 2013-2014	30	21	\$8,708,000

<i>National Security Division Technology Breakout (of Decision Unit Total)</i>	Perm. Pos.	FTE	Amount
2012 Enacted	9	9	\$12,055,000
2012 Prior Year Balance Rescissions	0	0	0
2012 Enacted w/Rescissions	9	9	12,055,000
2013 Continuing Resolution	9	9	12,444,000
Adjustments to Base and Technical Adjustments	0	0	0
2014 Current Services	9	9	11,150,000
2014 Program Decreases	0	0	(1,294,000)
2014 Program Offsets	0	0	0
2014 Request	9	9	11,150,000
Total Change 2013-2014	0	0	(\$1,294,000)

1. Program Description

The National Security Division (NSD) is responsible for overseeing terrorism investigations and prosecutions; handling counterespionage cases and matters; protecting critical national assets from national security threats, and assisting the Attorney General and other senior Department and Executive Branch officials in ensuring that the national security-related activities of the United States are consistent with relevant law.

In coordination with the FBI, the IC, and the USAOs, NSD's primary operational functions are to prevent acts of terrorism and espionage from being perpetrated in the United States by foreign powers and to facilitate the collection of information regarding the activities of foreign agents and powers. The NSD also advises the Attorney General on all matters relating to the national

security activities of the United States, and develops strategies for emerging national security threats – including cyber threats to the national security.

On the intelligence front, NSD administers the U.S. Government’s national security program for conducting electronic surveillance and physical search of foreign powers and agents of foreign powers pursuant to FISA, and conducts oversight of certain activities of the IC components and the FBI’s foreign intelligence and counterintelligence investigations pursuant to the Attorney General’s guidelines for such investigations. NSD prepares and files all applications for electronic surveillance and physical search under FISA, represents the government before the Foreign Intelligence Surveillance Court (FISC), and – when evidence obtained under FISA is proposed to be used in a criminal proceeding – NSD obtains the necessary authorization for the Attorney General to take appropriate actions to safeguard national security. NSD also works closely with the Congressional Intelligence Committees to ensure they are apprised of Departmental views on national security and intelligence policy and are appropriately informed regarding operational intelligence and counterintelligence activities.

In addition, NSD advises a range of government agencies on matters of national security law and policy, participates in the development of national security and intelligence policy through the National Security Council-led Interagency Policy Committee and Deputies’ Committee process, and represents the DOJ on a variety of interagency committees such as the Director of National Intelligence’s FISA Working Group and the National Counterintelligence Policy Board. NSD comments on and coordinates other agencies’ views regarding proposed legislation affecting intelligence matters, and advises the Attorney General and various client agencies, including the Central Intelligence Agency, the FBI, and the Defense and State Departments concerning questions of law, regulations, and guidelines as well as the legality of domestic and overseas intelligence operations.

NSD also serves as the staff-level DOJ representative on the CFIUS, which reviews foreign acquisitions of domestic entities affecting national security. In this role, NSD evaluates information relating to the structure of the transaction, any foreign government ownership or control, threat assessments provided by the IC, vulnerabilities resulting from the transaction, and ultimately the national security risks, if any, of allowing the transaction to proceed as proposed or subject to conditions. In addition, NSD tracks and monitors transactions that have been approved subject to mitigation agreements and seeks to identify unreported transactions that may require CFIUS review. On behalf of the Department, NSD also responds to FCC requests for Executive Branch determinations relating to the national security implications of certain transactions that involve FCC licenses. NSD reviews such license applications to determine if a proposed communication provider’s foreign ownership, control, or influence poses a risk to national security, infrastructure protection, law enforcement interests, or other public safety concerns sufficient to merit mitigating measures or opposition to the transaction.

Finally, OVT ensures that the investigation and prosecution of terrorist attacks against American citizens overseas are a high priority within the Department of Justice. Among other things, OVT is responsible for monitoring the investigation and prosecution of terrorist attacks against

Americans abroad, working with other Justice Department components to ensure that the rights of victims of such attacks are honored and respected, establishing a Joint Task Force with the Department of State to be activated in the event of a terrorist incident against American citizens overseas, responding to Congressional and citizen inquires on the Department's response to such attacks, compiling pertinent data and statistics, and filing any necessary reports with Congress.

2. Performance Tables

PERFORMANCE AND RESOURCES TABLE											
Decision Unit: National Security Division											
DOJ Strategic Goal/Objective: 1.1 Prevent, disrupt, and defeat terrorist operations before they occur; 1.2 Prosecute those involved in terrorist acts; and 1.3 Combat espionage against the United States.											
WORKLOAD/ RESOURCES		Target		Actual		Projected		Changes		Requested (Total)	
		FY 2012		FY 2012		FY 2013		Current Services Adjustments and FY 2014 Program Changes		FY 2014 Request	
Workload ¹											
Cases Opened	124		105		107		5		112		
Cases Closed	102		99		102		5		107		
Matters Opened	35,499		61,313		68,499		10,025		78,524		
Matters Closed	35,392		61,342		68,392		10,019		78,411		
FISA Applications Filed ²	CY 2012: 2,000		Not available. This information is classified at this time.		CY 2012: 2,000		0		CY 2012: 2,200		
National Security Reviews of Foreign Acquisitions ³	CY: 200		CY: 205		CY: 200		0		CY: 200		
Total Costs and FTE (reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	
	298	87,000	304	87,532	304	87,532	21	8,708	325	96,240	
		FY 2012		FY 2012		FY 2013		Current Services Adjustments and FY 2014 Program Changes		FY 2014 Request	
Program Activity	Intelligence	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
		192	61,123	192	61,123	195	61,497	12	5,226	207	66,723
Output Measure	Intelligence Community Oversight Reviews ⁴	CY: 82		CY: 99		CY: 82		7		CY: 89	
Output Measure (measure discontinued beginning FY 2013)	Percent Increase in the Number of US Victims of Overseas Terrorism Identified Since Program Inception (Baseline: 50) ⁵	5.8% (increase of 59, from 1,024 to 1,083)		8.4% (increase of 86, from 1,024 to 1,110)		NA		NA		NA	
Efficiency Measure	Percentage of OVT responses to victims within 3 business days of victim request for information from OVT ⁶	80%		89%		80%		0%		80%	
Outcome Measure (new measure beginning FY 2013)	Percentage of referrals for assistance received by OVT successfully resolved	NA		NA		95%		0%		95%	

¹Workload measures are not performance targets, rather they are estimates to be used for resource planning. In addition, these measures do not take into consideration potential policy changes.

²FISA applications filed data is based on historical averages and do not represent actual data, which remains classified until the public report is submitted to the Administrative Office of the US Courts and the Congress in April for the preceding calendar year.

³Beginning FY 2012, this measure will be tracked on a calendar year basis rather than a fiscal year basis (similar to other agencies in CFIUS and Team Telecom) for ease of reporting.

⁴This measure is tracked on a calendar year basis for ease of reporting.

⁵ After a thorough review completed during FY 2013, 32 victims identified during FY 2011 have been deleted from the database. The FY 2011 actual increase in victims identified is 493 with a cumulative total of 1,042. The FY 2012 baseline has been revised.

⁶ The title of this measure has been modified from "Percentage of victims provided with service and/or compensation information within 3 business days of identification" to "Percentage of OVT responses to victims within 3 business days of victim request for information from OVT" for clarity.

PERFORMANCE AND RESOURCES TABLE

Decision Unit: National Security Division

DOJ Strategic Goal/Objective: 1.1 Prevent, disrupt, and defeat terrorist operations before they occur; 1.2 Prosecute those involved in terrorist acts; and 1.3 Combat espionage against the United States.

WORKLOAD/ RESOURCES		Target		Actual		Projected		Changes		Requested (Total)	
		FY 2012		FY 2012		FY 2013		Current Services Adjustments and FY 2014 Program Changes		FY 2014 Request	
Program Activity	Counterterrorism	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
		73	17,498	73	17,498	75	17,605	3	1,764	78	19,369
Outcome Measure	Percentage of CT defendants whose cases were favorably resolved ⁶	90%		98%		90%		0		90%	
Outcome Measure	Percentage of CT cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	99%		100%		99%		0		99%	
Program Activity	Counterespionage	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
		33	8,379	33	8,379	34	8,430	6	1,718	40	10,148
Outcome Measure	Percentage of CE defendants whose cases were favorably resolved ⁷	90%		100%		90%		0		90%	
Outcome Measure	Percentage of CE cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	99%		100%		99%		0		99%	
Output Measure	FARA Inspections	15		15		15		0		15	
Output Measure	High priority national security reviews completed ⁸	30		37		30		0		30	

⁶ The title of this measure has been modified from "Percentage of CT cases favorably resolved" to "Percentage of CT defendants whose cases were favorably resolved" for clarity.

⁷ The title of this measure has been modified from "Percentage of CE cases favorably resolved" to "Percentage of CE defendants whose cases were favorably resolved" for clarity.

⁸ Beginning FY 2012, this measure is tracked on a calendar year basis rather than a fiscal year basis (similar to other agencies in CFIUS and Team Telecom) for ease of reporting.

PERFORMANCE MEASURE TABLE

Decision Unit: National Security Division

Performance Report and Performance Plan Targets		FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012		FY 2013	FY 2014
		Actual	Actual	Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Performance Measure	Intelligence Community Oversight Reviews ¹	N/A	N/A	N/A	N/A	NA	CY: 92	CY: 82	CY: 99	CY: 82	CY: 89
Output Measure (discontinued beginning FY 2013)	Percent Increase in the Number of U.S. Victims of Overseas Terrorism Identified Since Program Inception (Baseline: 50)	N/A	N/A	Baseline - 50	384% (increase of 192, from 50 to 242) ²	119% (increase of 289, from 242 to 531) ³	93% (increase of 493, from 531 to 1,024) ⁴	5.8% (increase of 59, from 1,024 to 1,083) ⁵	8.4% (increase of 86, from 1,024 to 1,110)	NA	NA
Efficiency Measure	Percentage of OVT responses to victims within 3 business days of victim request for information from OVT ⁵	N/A	N/A	N/A	80%	95%	90%	80%	89%	80%	80%
Outcome Measure (new beginning FY 2013)	Percentage of referrals for assistance received by OVT successfully resolved	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	95%	95%
Outcome Measure	Percentage of CT defendants whose cases were favorably resolved ⁶	N/A	98%	97%	100%	100%	98%	90%	98%	90%	90%
Outcome Measure	Percentage of CT cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	N/A	N/A	100%	100%	100%	100%	99%	100%	99%	99%
Outcome Measure	Percentage of CE defendants whose cases were favorably resolved ⁷	N/A	96%	92%	98%	94%	98%	90%	100%	90%	90%
Performance Measure	FARA inspections completed	N/A	0	13	14	15	15	15	15	15	15
Performance Measure	High priority national security reviews completed ⁸	N/A	N/A	N/A	27	28	29	CY: 30	CY: 37	CY: 30	CY: 30
Outcome Measure	Percentage of CE cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	N/A	N/A	100%	100%	100%	100%	99%	100%	99%	99%

¹ This measure is tracked on a calendar year basis for ease of reporting.

² The FY 2009 actual for this measure was previously reported as 400% (increase of 200, from 50 to 250). However, during a recent audit by the Office of the Inspector General, it was determined that seven of the FY 2009 victims identified should have been included in FY 2010. Additionally, one FY 2009 victim identified has been removed from the database, and therefore the FY 2009 actual has decreased by eight victims identified overall to 192 victims identified.

³ The FY 2010 baseline decreased from 250 as it was reported in the FY 2013 Congressional Budget to 242 as discussed above.

⁴ After a thorough review completed during FY 2013, 32 victims identified during FY 2011 have been deleted from the database. The FY 2011 increase in victims identified is 493 with a cumulative total of 1,042, not 525 with a cumulative total of 1,056 as it was reported in the FY 2013 Budget.

⁵ The FY 2012 baseline has been revised to reflect the 32 victims who have been deleted from the database as discussed above.

⁶ The title of this measure has been modified from "Percentage of victims provided with service and/or compensation information within 3 business days of identification" to "Percentage of OVT responses to victims within 3 business days of victim request for information from OVT" for clarity.

⁷ The title of this measure has been modified from "Percentage of CT cases favorably resolved" to "Percentage of CT defendants whose cases were favorably resolved" for clarity.

⁸ The title of this measure has been modified from "Percentage of CE cases favorably resolved" to "Percentage of CE defendants whose cases were favorably resolved" for clarity.

⁹ Beginning FY 2012, this measure is tracked on a calendar year basis rather than a fiscal year basis (similar to other agencies in CFIUS and Team Telecom) for ease of reporting.

3. Performance, Resources, and Strategies

For performance reporting purposes, resources for NSD are included under DOJ Strategic Goal 1: Prevent Terrorism and Promote the Nation’s Security Consistent with the Rule of Law. Within this Goal, NSD resources address all three Objectives:

- 1.1 Prevent, disrupt, and defeat terrorist operations before they occur;
- 1.2 Prosecute those involved in terrorist acts; and
- 1.3 Combat espionage against the United States.

Based on these three objectives, performance resources are allocated to three program activities: Intelligence, Counterterrorism, and Counterespionage.

a. Performance Plan and Report for Outcomes

Intelligence Performance Report

Measure: **Intelligence Community Oversight Reviews**

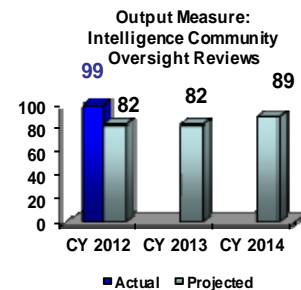
CY 2012 Target: 82

CY 2012 Actual: 99

CY 2013 Target: 82

CY 2014 Target: 89

Discussion: This measure is tracked on a calendar year basis for ease of reporting. It was incorrectly reported in fiscal years before.



Data Definition: NSD attorneys are responsible for conducting oversight of certain activities of IC components. The oversight process involves numerous site visits to review intelligence collection activities and compliance with the Constitution, statutes, AG Guidelines, and relevant Court orders. Such oversight reviews require advance preparation, significant on-site time, and follow-up and report drafting resources. These oversight reviews cover many diverse intelligence collection programs. FISA Minimization Reviews and National Security Reviews will be counted as part of Intelligence Community Oversight Reviews.

Data Collection and Storage: The information collected during each review is compiled into a report, which is then provided to the reviewed Agency. Generally, the information collected during each review, as well as the review reports, are stored on a classified database. However, some of the data collected for each review is stored manually.

Data Validation and Verification: Reports are reviewed by NSD management, and in certain instances reviewed by agencies, before being released.

Data Limitations: None identified at this time.

Measure: Percent Increase in the Number of U.S. Victims of Overseas Terrorism Identified Since Program Inception (Baseline: 50)

FY 2012 Target: 5.8% (Increase from 1,024 to 1,083)

FY 2012 Actual: 8.4% (Increase from 1,024 to 1,110)

FY 2013 Target: Not Applicable

FY 2014 Target: Not Applicable

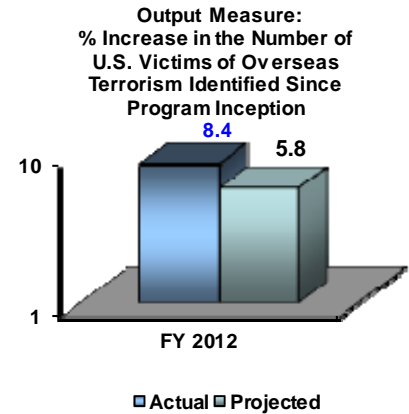
Discussion: This measure will be discontinued in FY 2013 because it is no longer an effective indicator of program performance. Additionally, after a thorough review completed during FY 2013, 32 victims identified during FY 2011 have been deleted from the database. The FY 2012 baseline has been revised accordingly.

Data Definition: Victims: American citizens who are the victims of terrorism outside the borders of the U.S.

Data Collection and Storage: Data is collected and stored in an electronic database.

Data Validation and Verification: Data is validated by management and staff.

Data Limitations: None.



Measure: Percentage of OVT Responses to Victims within 3 Business Days of Victim Request for Information from OVT

FY 2012 Target: 80%

FY 2012 Actual: 89%

FY 2013 Target: 80%

FY 2014 Target: 80%

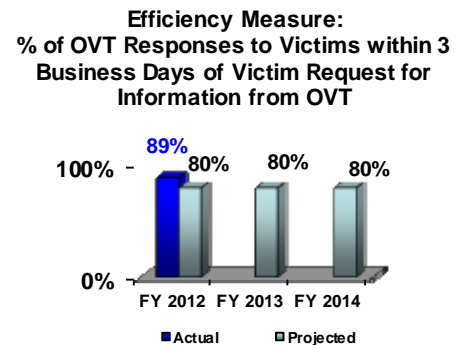
Discussion: The title of this measure has been modified from "Percentage of Victims Provided with Service and/or Compensation Information within 3 Business days of Identification" to "Percentage of OVT Responses to Victims within 3 Business Days of Victim Request for Information from OVT" for clarity.

Data Definition: Victims: American citizens who are the victims of terrorism outside the borders of the U.S. This measure reflects OVT's efficiency in providing information to victims after they have contacted OVT.

Data Collection and Storage: Data is collected and storage in an electronic database.

Data Validation and Verification: Data is validated by management and staff.

Data Limitations: None.



Measure: Percentage of Referrals for Assistance Received by OVT Successfully Resolved

FY 2012 Target: NA

FY 2012 Actual: NA

FY 2013 Target: 95%

FY 2014 Target: 95%

Discussion: New measure beginning FY 2013.

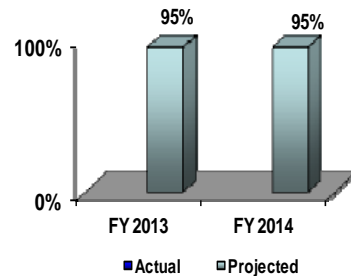
Data Definition: This measure counts the percentage of referrals received during the fiscal year that are successfully resolved through the provision of a set group of services. OVT is monitoring two types of referrals. First are newly identified victims. Second are referrals of already existing victims when criminal justice proceedings are initiated for each defendant in a domestic or foreign criminal justice system. Most referrals come from the FBI's Office for Victim Assistance which will inform OVT when foreign criminal justice proceedings have been initiated. Another source for information is the Counterterrorism Section which will inform OVT about foreign and domestic terrorism trials with U.S. victims. In some situations referrals may come from the State Department or other victims.

Data Collection and Storage: For each new victim referred to OVT for assistance, OVT creates a paper file to document OVT efforts. The file contains a checklist of services that OVT can either provide, make a referral for another agency to provide, or which cannot be provided for a legitimate reason (such as it would involve divulging National Security information, or a criminal justice proceeding is not ongoing at the time). On a quarterly basis the paper files are reviewed and analyzed to determine whether the checklist services have been successfully addressed as indicated in the previous sentence. For referrals based on new criminal justice proceedings, OVT takes an existing victim file and creates a new checklist for the new criminal justice proceeding.

Data Validation and Verification: OVT will review the paper files on a quarterly basis. The information in the paper files will then be loaded into an automated Victim/Attack Tracking Tool (VATT) so that the information can be easily accessed.

Data Limitations: Some criminal justice proceedings and corresponding support efforts will span several years, but OVT's efforts will only be reported in the year in which the criminal justice proceeding was initiated.

% of Referrals for Assistance Received by OVT Successfully Resolved



Counterterrorism (CT) Performance Report

Measure: Percentage of CT Defendants Whose Cases Were Favorably Resolved

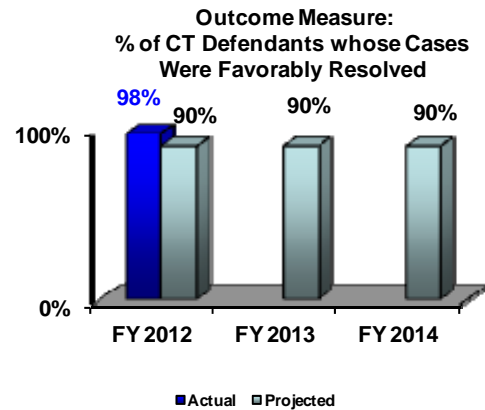
FY 2012 Target: 90%

FY 2012 Actual: 98%

FY 2013 Target: 90%

FY 2014 Target: 90%

Discussion: NSD has modified the title of this measure from “Percentage of CT Cases Favorably Resolved” to “Percentage of CT Defendants Whose Cases Were Favorably Resolved” for clarity.



Data Definition: Cases Favorably Resolved include those cases closed during the fiscal year that resulted in court judgments favorable to the government.

Data Collection and Storage: Attorneys provide data which is stored in the ACTS database.

Data Validation and Verification: Data validation and verification is accomplished via quarterly review by CTS Chief.

Data Limitations: None identified at this time.

Select Recent Counterterrorism Section Prosecutions:

New York Subway Bomb Plot / U.S. v. Medunjanin, et al. - On May 2, 2012, Adis Medunjanin, a Queens, N.Y., resident who joined al-Qaeda and plotted to commit a suicide terrorist attack in New York City, was convicted of multiple federal terrorism offenses in the Eastern District of New York. As of May 10, 2012, seven defendants, including Medunjanin, Najibullah Zazi, Amanullah Zazi, and Zarein Ahmedzay, had been convicted in connection with the New York City bombing plot and related charges. On November 16, 2012, the court sentenced Medunjanin to life imprisonment. Ahmedzay and Najibullah Zazi, who each face a maximum sentence of life imprisonment, are scheduled to be sentenced on May 10, 2013, and September 27, 2013, respectively.

Christmas Day 2009 Underwear Bomb Plot / U.S. v. Abdulmutallab -- On February 16, 2012, Umar Farouk Abdulmutallab, the so-called “underwear bomber,” was sentenced in the Eastern District of Michigan to life in prison as a result of his October 12, 2011 guilty plea to all eight counts of an indictment charging him for his role in the attempted Christmas Day 2009 bombing of Northwest Airlines flight 253. In August 2009, Abdulmutallab traveled to Yemen for the purpose of becoming involved in violent “jihad” on behalf of al-Qaeda. There, he met with and conspired with members of al-Qaeda in the Arabian Peninsula (AQAP), including the late Anwar

Awlaki, to bomb a U.S. aircraft over U.S. soil. According to court papers filed in the case, while in Yemen, Abdulmutallab received an explosive device constructed by alleged AQAP bomb-maker, Ibrahim al Asiri, for his suicide mission. After being trained in the use of the bomb, Abdulmutallab provided a statement for a martyrdom video that was filmed by AQAP. Abdulmutallab then traveled with the bomb concealed in his underwear from Yemen to Africa and then to the Netherlands, where he boarded Flight 253 on Christmas Day 2009. The bomb contained PETN and TATP, two high explosives. As Flight 253 descended into Detroit Metropolitan Airport, Abdulmutallab detonated the bomb, which resulted in a fire, but did not fully explode.

U.S. v. Waad Ramadan Alwan, et al. – On May 26, 2011, Waad Ramadan Alwan was indicted by a grand jury in Bowling Green, Kentucky, on 23 charges, including conspiracy to kill U.S. nationals abroad, conspiracy to use a weapon of mass destruction against U.S. nationals abroad, distributing information on the manufacture and use of improvised explosive devices (IEDs), attempting to provide material support to terrorists and to al-Qaeda in Iraq and conspiracy to transfer, possess, and export Stinger missiles. Alwan’s co-defendant, Mohanad Shareef Hammadi, was charged in the same indictment with five counts of attempting to provide material support to terrorists, in violation of 18 U.S.C. §2339A; four counts of attempting to provide material support to a foreign terrorist organization (al Qaeda in Iraq), in violation of 18 U.S.C. § 2339B; and one count of conspiracy to transfer, possess or export a device designed or intended to launch or guide a rocket or missile, in violation of 18 U.S.C. § 2332g. On February 15, 2012, a superseding indictment against Hammadi was filed adding two counts of making false statements in immigration matters, in violation of 18 U.S.C. § 1546(a). On December 16, 2011, Alwan pled guilty to all of the charges in the indictment. On August 21, 2012, Hammadi entered a guilty plea to all twelve counts of the superseding indictment. Alwan was sentenced to life imprisonment and Hammadi was sentenced to 40 years’ imprisonment.

U.S. v. Khalid Aldawsari – On March 9, 2011, Khalid Aldawsari, a citizen of Saudi Arabia and a resident of Lubbock, Texas, was charged by indictment with one count of attempting to use a weapon of mass destruction, in violation of 18 U.S.C. § 2332a(a)(2)(A) and (D). Aldawsari was arrested on February 23, 2011, based on a criminal complaint. An FBI investigation uncovered Aldawsari’s plan to purchase concentrated chemicals and equipment necessary to make an Improvised Explosive Device (IED) for use against persons and infrastructure in the United States. Furthermore, he allegedly also conducted online research on several potential targets including the Dallas residence of former President George W. Bush. Aldawsari was convicted on June 27, 2012. On November 13, 2012, Aldawsari was sentenced to life imprisonment.

U.S. v. Arbabsiar, et al. – Arbabsiar was arrested on September 29, 2011, at John F. Kennedy International Airport in Queens, New York. On October 7, 2012, Arbabsiar pled guilty before U.S. District Judge John F. Keenan, to a superseding information that charges him with three counts. Count one charges Arbabsiar with traveling in foreign commerce and using interstate and foreign commerce facilities in the commission of murder-for-hire, in violation of 18 U.S.C. § 1958; count two charges him with conspiracy to do count one, in violation of

18 U.S.C. § 1958; and count three charges him with conspiracy to commit an act of terrorism transcending national boundaries, in violation of 18 U.S.C. § 371. Arbabsiar faces a maximum potential sentence of 25 years in prison. Arbabsiar is scheduled to be sentenced on March 26, 2013.

U.S. v. Warsame - On June 30, 2011, Ahmed Abdulkadir Warsame, an accused al-Shabaab commander, was indicted in the Southern District of New York on charges of providing material support to al-Shabaab and Al-Qaeda in the Arabian Peninsula (AQAP), as well as weapons violations, conspiracy to teach and demonstrate the making of explosives, receiving explosives training from AQAP, and other violations. Warsame was captured in the Gulf region by the United States military on April 19, 2011 and was questioned for intelligence purposes for more than two months. Warsame was brought to the Southern District of New York for prosecution and arraigned on July 5, 2011. According to the indictment, between 2007 and April 2011, Warsame conspired to provide and provided material support to al-Shabaab, resulting in the death of at least one person. Warsame allegedly fought on behalf of al-Shabaab in Somalia in 2009 and provided other forms of support to the terrorist organization including explosives, weapons, communications equipment, expert advice, and assistance and training. The indictment further alleges that between 2009 and April 2011, Warsame conspired to provide and provided material support to AQAP, in the form of money, training, communications equipment, facilities, and personnel. While in Yemen in 2010 and 2011, he allegedly possessed and used grenades and an AK-47 semi-automatic assault weapon in crimes of violence. According to the charges, Warsame also worked to broker a weapons deal with AQAP on behalf of al-Shabaab.

U.S. v. Naser Jason Abdo – Naser Jason Abdo was arrested on July 28, 2011, by local authorities in Killeen, Texas, after he was found in possession of bomb-making materials and a gun. Abdo had planned an attack on U.S. soldiers at a restaurant outside Fort Hood in Texas and planned to use explosive devices to kill soldiers and then use a handgun to kill any survivors. He was charged by indictment with: (1) attempted use of a weapon of mass destruction, in violation of 18 U.S.C. § 2332a(a)(2)(D) (one count); (2) attempted murder of officers and employees of the United States, in violation of 18 U.S.C. § 1114(3) (one count); and (3) possession of a weapon in furtherance of a federal crime of violence, in violation of 18 U.S.C. § 924(c)(1)(A) (four counts). On May 24, 2012, he was convicted on all counts. On August 10, 2012, he was sentenced to life in prison.

Measure: Percentage of CT Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process

FY 2012 Target: 99%
FY 2012 Actual: 100%
FY 2013 Target: 99%
FY 2014 Target: 99%

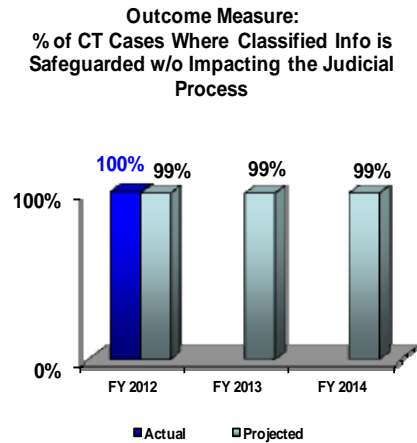
Discussion: No discussion required.

Data Definition: Classified information - information that has been determined by the United States Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data as defined by the Atomic Energy Act of 1954. Safeguarded - that the confidentiality of the classified information is maintained because the Government has proposed redactions, substitutions or summarizations pursuant to CIPA which the Court has accepted. Impact on the judicial process - that the Court does not exclude certain evidence, dismiss particular counts of the indictment, or dismiss the indictment as a remedy for the Government’s insistence that certain classified information not be disclosed at trial.

Data Collection and Storage: Data collection and storage is manual.

Data Validation and Verification: Data validation and verification is accomplished via quarterly review by CTS Chief.

Data Limitations: None identified at this time.

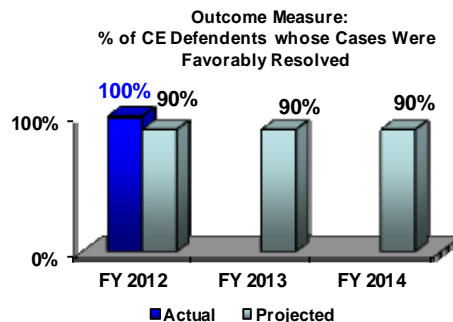


Counterespionage (CE) Performance Report

Measure: Percentage of CE Defendants Whose Cases Were Favorably Resolved

FY 2012 Target: 90%
FY 2012 Actual: 100%
FY 2013 Target: 90%
FY 2014 Target: 90%

Discussion: NSD has modified the title of this measure from “Percentage of CE Cases Favorably Resolved” to “Percentage of CE Defendants Whose Cases Were Favorably Resolved” for clarity.



Data Definition: Cases Favorably Resolved include those cases closed during the fiscal year that resulted in court judgments favorable to the government.

Data Collection and Storage: Attorneys provide data which is stored in the ACTS database.

Data Validation and Verification: Quarterly review of database records and data updates from CES attorneys in order to insure that records are current and accurate.

Data Limitations: Reporting lags.

Select Recent Counterespionage Prosecutions

Former U.S. Consulate Guard Pleads Guilty to Spying / U.S. v. Underwood –

On August 30, 2012, Bryan Underwood, a former contract guard working at a U.S. Consulate in China, pleaded guilty to attempting to communicate national defense information to a foreign government. On September 28, 2011, Underwood had been charged in a superseding indictment in the District of Columbia with attempting to communicate national defense information to the People's Republic of China (PRC), making false statements, and failing to appear in court pursuant to his conditions of release. Underwood was first charged with making false statements and was arrested on September 1, 2011. The following day, he failed to appear at a status hearing in court. The FBI located Underwood in Los Angeles and arrested him on September 24, 2011. According to the superseding indictment, Underwood attempted to communicate photographs and other national defense information to representatives of the PRC from about March 1, 2011 to about August 5, 2011. Underwood is scheduled to be sentenced on March 5, 2013.

Virginia Man Sentenced for Acting as Illegal Agent of Syria / U.S. v. Soueid – On July 20, 2012, Mohamad Soueid was sentenced to 18 months in prison after being convicted of unlawfully acting as an agent of a foreign government. On October 11, 2011, Soueid had been arrested for his alleged role in a conspiracy to collect video and audio recordings and other information about individuals in the United States and Syria who were protesting the Government of Syria and to provide these materials to Syrian intelligence agencies in order to silence, intimidate, and potentially harm the protestors. Soueid, a Syrian-born naturalized U.S. citizen, was charged by a federal grand jury on October 5, 2011, in the Eastern District of Virginia with conspiring to act and acting as an agent of the Syrian Government in the United States without notifying the Attorney General as required by law; two counts of providing false statements to federal law enforcement; and two counts of providing false statements on a firearms purchase form.

Former CIA Officer Pleads Guilty to Disclosing Classified Information / U.S. v. Kiriakou – On April 5, 2012, former CIA officer John Kiriakou was indicted for allegedly disclosing classified information to journalists, including the name of a covert CIA officer and information revealing the role of another CIA employee in classified activities. Kiriakou was charged in a five-count indictment returned by a federal grand jury in the Eastern District of Virginia, after he was initially charged in a criminal complaint and arrested in January 2012. The indictment charged Kiriakou with one count of violating the Intelligence Identities Protection Act for allegedly illegally disclosing the identity of a covert officer, and with three counts of violating the Espionage Act for allegedly illegally disclosing national defense information to individuals not authorized to receive it. The indictment also charged Kirakou with one count of making false

statements for allegedly lying to the CIA Publications Review Board in an unsuccessful attempt to trick the CIA into allowing him to include classified information in a book he was seeking to publish. On October 23, 2012, Kiriakou pleaded guilty to Count One of the indictment – intentionally disclosing information identifying a covert officer.

Scientist Sentenced for Attempted Espionage / U.S. v. Nozette – On March 21, 2012, Stewart David Nozette, a scientist who once worked for the White House’s National Space Council and other federal agencies, was sentenced in the District of Columbia to 13 years in prison for attempted espionage, conspiracy to defraud the United States, and tax evasion. The sentence covered charges in two cases. In one, Nozette pleaded guilty to attempted espionage for providing classified information to a person he believed to be an Israeli intelligence officer. In the other, he pleaded guilty to fraud and tax charges. From 1989 through 2006, Nozette held security clearances as high as TOP SECRET. On September 3, 2009, Nozette was contacted by an individual purporting to be an Israeli intelligence officer, but who was actually an FBI undercover employee. That day, Nozette informed the undercover employee that he would provide classified information for money and a foreign passport to a country without extradition to the United States. A series of contacts followed over the next several weeks, including meetings and exchanges in which Nozette took \$10,000 in cash left by the FBI at pre-arranged drop-off sites and provided classified information relating to the national defense.

Ten Defendants Charged in Economic Espionage Case / U.S. v. Liew et al. – On March 2, 2012, former DuPont scientist Tze Chao pleaded guilty in the Northern District of California to conspiracy to commit economic espionage, admitting that he provided trade secrets on DuPont’s proprietary titanium dioxide (TiO₂) process to companies controlled by the government of the People’s Republic of China (PRC). On February 7, 2012, a grand jury in San Francisco returned a superseding indictment charging Chao and four other individuals, as well as five companies, with economic espionage and theft of trade secrets for their roles in a long-running effort to obtain U.S. trade secrets from DuPont for companies controlled by the PRC. According to the indictment, the PRC government identified as a priority the development of TiO₂ production capabilities. TiO₂ is a commercially valuable white pigment with numerous uses. To achieve that goal, companies controlled by the PRC government, specifically the Pangang Group companies, and employees of those companies allegedly attempted to illegally obtain TiO₂ technology developed by DuPont. The Pangang Group companies were allegedly aided in their efforts by individuals in the United States who had obtained TiO₂ trade secrets and were willing to sell them for significant sums of money.

Select Recent Counterproliferation Prosecutions

TOW Missile Components to Iran / U.S. v. Baniameri et al. – On July 26, 2012, Andro Telemi, a naturalized U.S. citizen from Iran who resided in California, pleaded guilty in the Northern District of Illinois to one count of attempting to illegally export defense articles in connection with his efforts to export TOW and TOW2 missile components to Iran. Telemi was indicted in December 2009, along with Davoud Baniameri, an Iranian citizen who lived in Woodland Hills, California. A superseding indictment returned in July 2010 charged Telemi, Baniameri and Syed

Majid Mousavi, an Iranian citizen living in Iran. According to court documents, sometime before Oct. 2008, Mousavi, based in Iran, contacted Baniameri in California and requested that he purchase Marconi radio test sets for illegal export from the United States to Iran. Baniameri purchased these sets from an Illinois company and later exported them to Iran via Dubai. Mousavi also requested that Baniameri purchase and export to Iran, via Dubai, ten connector adaptors for the TOW and TOW2 missile system, which are used on the U.S. Army's Bradley fighting vehicle and the U.S. Marine Corp's AH-1W Cobra attack helicopter. Baniameri later negotiated the purchase of these items from an Illinois company and directed Telemi to assist him in this effort and to take possession of the items. To facilitate the export of these goods, Baniameri arranged to fly to Iran, but he was arrested before leaving the country. On May 31, 2011, Baniameri pleaded guilty to conspiracy to illegally export goods and technology to Iran and attempting to illegally export defense articles in connection with the TOW missile components and radio test sets. On August 12, 2011, Baniameri was sentenced to 51 months in prison. On July 26, 2012, Telemi pleaded guilty to attempting to export defense articles without a license. Telemi was sentenced to 5 years' probation.

Materials for Gas Centrifuges and Nuclear-Related Goods to Iran / U.S. v. Khaki et al. – On July 12, 2012, a grand jury in the District of Columbia returned a superseding indictment charging Parviz Khaki, a citizen of Iran, and Zongcheng Yi, a resident of China, for their alleged efforts to obtain and illegally export to Iran U.S.-origin materials used to construct, operate and maintain gas centrifuges to enrich uranium, including maraging steel, aluminum alloys, mass spectrometers, vacuum pumps and other items. Khaki was also accused of conspiring to procure radioactive source materials from the United States for customers in Iran. The indictment charges Khaki and Yi each with conspiracy to violate the International Emergency Economic Powers Act (IEEPA), conspiracy to defraud the United States, smuggling, illegally exporting U.S. goods to Iran in violation of IEEPA, and conspiracy to commit money laundering. Khaki was arrested on May 24, 2012, by authorities in the Philippines in connection with a U.S. provisional arrest request stemming from an indictment in the District of Columbia. The United States has requested Khaki's extradition. Yi, who is purported to be the managing director of Monalila Co. LTD, a toy company in Guangzhou City, China, remains at large. From around October 2008 through January 2011, Khaki, Yi and others allegedly conspired to cause the export of goods from the United States to Iran without a Treasury Department license. In carrying out the conspiracy, Khaki directed Yi and others to contact U.S. companies about purchasing U.S.-origin goods. Yi and other conspirators then purchased goods from various U.S. companies and had the goods exported from the United States through China and Hong Kong to Khaki and others in Iran. Yi and others made false statements to U.S. companies on behalf of Khaki to conceal that Iran was the final destination and end-user of the goods.

Military Software for China's Attack Helicopter / U.S. v. UTC et al. -- On June 28, 2012, in the District of Connecticut, Pratt & Whitney Canada Corp. (PWC), a Canadian subsidiary of Connecticut-based defense contractor United Technologies Corp. (UTC), pleaded guilty to violating the Arms Export Control Act and making false statements in connection with its illegal export to China of U.S.-origin military software that was used in the development of China's first modern military attack helicopter, the Z-10. In addition, UTC, its U.S.-based subsidiary

Hamilton Sundstrand Corp. (HSC), and PWC all agreed to pay more than \$75 million as part of a global settlement with the Justice Department and the State Department in connection with various export violations, including those related to the Z-10, and for making false and belated disclosures to the U.S. government about the illegal exports for the Z-10. A three-count criminal information was filed against the companies. Count one charged PWC with violating the Arms Export Control Act for the illegal export of defense articles to China for the Z-10 helicopter. Specifically, PWC knowingly and willfully caused HSC military software used to test and operate PWC engines to be exported to China for the Z-10 without any U.S. export license. Count two charged PWC, UTC, and HSC with making false statements about these illegal exports to the State Department in their belated disclosures, which did not begin until 2006. Count three charged PWC and HSC for their failure to timely inform the State Department of the unlawful export of defense articles to China, an embargoed nation, as required by U.S. export regulations. This is the first case in which the provisions in count three have been enforced criminally. While PWC pleaded guilty to counts one and two, prosecution of PWC, UTC, and HSC on the other charges is deferred for two years, provided that the companies abide by the terms of a deferred prosecution agreement with the Justice Department. In connection with the global settlement with the Justice and State Departments, PWC, UTC, and HSC agreed to pay more than \$75 million in penalties, subject themselves to independent monitoring for several years, and be required to comply with an extensive training and remedial action program to strengthen their export compliance.

Radiation-Hardened Circuits to China / U.S. v. He – On February 3, 2012, Chinese citizen and former California Department of Transportation (Caltrans) engineer Philip Chaohui He appeared in federal court in the District of Colorado after his arrest in San Francisco in connection with his alleged efforts to export defense articles to China without a State Department license, specifically more than 300 space-qualified and radiation-hardened computer circuits used in satellite communications with a total value of nearly \$550,000. An indictment charged He with conspiracy to violate the Arms Export Control Act (AECA) and to smuggle goods; attempted violation of AECA; and smuggling. According to the charges, He arranged for the purchase of more than 300 radiation-hardened circuits from Aeroflex, a Colorado manufacturer, in May 2011. He arranged for the purchase after a co-conspirator sent him wire transfers totaling nearly \$490,000 from a bank in China. He then provided false certification to Aeroflex that the items would remain in the United States. In December 2011, He drove to the Port of Long Beach and met with two men in front of a docked Chinese-flagged ship that was registered to a subsidiary of a China state-owned corporation. The ship recently had arrived from Shanghai and was scheduled to return on December 15, 2011. He was arrested on December 11, 2011 at the Port. He allegedly had concealed 200 circuits in infant formula containers in the trunk of his vehicle.

Components for IEDs to Iran and Iraq / U.S. v. Larijani et al. – On October 25, 2011, prosecutors in the District of Columbia unsealed an indictment which charged five individuals and four of their companies with various violations, including conspiracy to defraud the United States, smuggling, illegal export of goods to Iran, illegal export of defense articles, false statements and obstruction of justice. The charged defendants are Iranian national Hossein

Larijani, and his companies Paya Electronics Complex, based in Iran, and Opto Electronics Pte, Ltd., based in Singapore; Wong Yuh Lan, an agent of Opto Electronics who was allegedly supervised by Larijani from Iran; NEL Electronics Pte. Ltd., a company in Singapore, along with NEL's owner and director, Lim Yong Nam; Corezing International Pte. Ltd., a company in Singapore that maintained offices in China; as well as Lim Kow Seng, an agent of Corezing, and Hia Soo Gan Benson, a manager, director and agent of Corezing. On October 24, 2011, authorities in Singapore arrested Wong, Nam, Seng and Hia pursuant to a U.S. extradition request. Larijani remains a fugitive in Iran. The indictment alleges that, between June 2007 and February 2008, the defendants fraudulently purchased and caused 6,000 radio frequency modules to be illegally exported from Minnesota through Singapore to Iran. The alleged recipient of all 6,000 modules in Iran was Larijani. The indictment alleges that Coalition forces found no less than 16 of these 6,000 modules in Iraq where they were being used as part of the remote detonation devices of unexploded IEDs. The indictment further charged Seng, Hia, and Corezing with a separate fraud conspiracy involving the illegal export of two types of military antenna from the United States. In February 2012, a Singapore court ruled that the four suspects held in Singapore may be extradited to the United States to face prosecution for their alleged roles in conspiracies to defraud the United States. The litigation over extradition continues, after another court in Singapore in August 2012 found that only two of the suspects could be extradited.

Measure: Percentage of CE Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process

FY 2012 Target: 99%

FY 2012 Actual: 100%

FY 2013 Target: 99%

FY 2014 Target: 99%

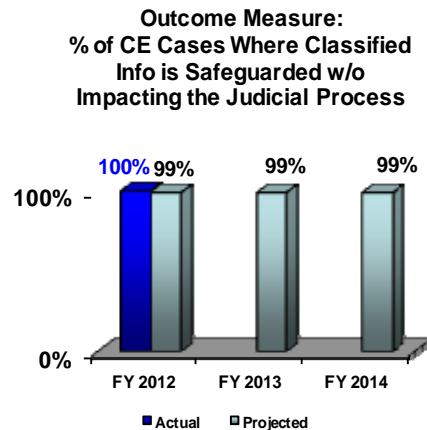
Discussion: No discussion required.

Data Definition: Classified information - information that has been determined by the United State Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data as defined by the Atomic Energy Act of 1954. Safeguarded - that the confidentiality of the classified information is maintained because the Government has proposed redactions, substitutions or summarizations pursuant to CIPA which the Court has accepted. Impact on the judicial process - that the Court does not exclude certain evidence, dismiss particular counts of the indictment, or dismiss the indictment as a remedy for the Government's insistence that certain classified information not be disclosed at trial.

Data Collection and Storage: CES attorneys provide data concerning CIPA matters handled in their cases as well as the status or outcome of the matters, which are then entered into the ACTS database.

Data Validation and Verification: Quarterly review of database records and data updates from CES attorneys in order to insure that records are current and accurate.

Data Limitations: Reporting lags.



Measure: Targeted FARA Inspections Completed

FY 2012 Target: 15

FY 2012 Actual: 15

FY 2013 Target: 15

FY 2014 Target: 15

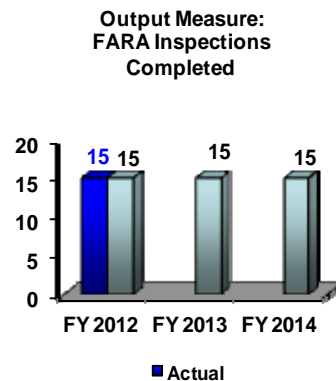
Discussion: No discussion required.

Data Definition: Targeted FARA Inspections are conducted routinely. There can also be additional inspections completed based on potential non-compliance issues. Inspections are just one tool used by the Unit to bring registrants into compliance with FARA.

Data Collection and Storage: Inspection reports are prepared by FARA Unit personnel and stored in manual files.

Data Validation and Verification: Inspection reports are reviewed by the FARA Unit Chief.

Data Limitations: None identified at this time



Measure: High Priority National Security Reviews Completed

CY 2012 Target: 30

CY 2012 Actual: 37

CY 2013 Target: 30

CY 2014 Target: 30

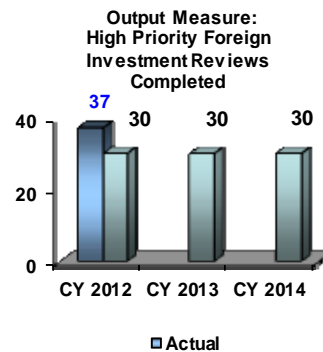
Discussion: Beginning FY 2012, this measure will be tracked on a calendar year basis rather than a fiscal year basis (similar to other agencies in CFIUS and Team Telecom) for ease of reporting.

Data Definition: High Priority National Security Reviews include (1) CFIUS case reviews of transactions in which DOJ is a co-lead agency in CFIUS due to the potential impact on DOJ equities; (2) CFIUS case reviews which result in a mitigation agreement to which DOJ is a signatory; (3) Team Telecom case reviews which result in a mitigation agreement to which DOJ is a signatory; and (4) mitigation monitoring site visits.

Data Collection and Storage: Data is collected manually and stored in generic files; however management is reviewing the possibility of utilizing a modified automated tracking system.

Data Validation and Verification: Data is validated and verified by management.

Data Limitations: Given the expanding nature of the program area – a more centralized data system is desired.



V. Program Increases by Item

A. Item Name: **Combating Cyber Threats to National Security**

Budget Decision Unit: National Security Division

Strategic Goal & Objective: Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law
Objective 1.1 Prevent, disrupt, and defeat terrorist operations before they occur
Objective 1.2 Prosecute those involved in terrorist acts
Objective 1.3 Combat espionage against the United States

Organizational Program: Counterespionage, Foreign Investment Review, Counterterrorism, Intelligence, Law and Policy, Information Technology

Component Ranking of Item: 1 of 3

Program Increase: Positions 26 Atty 16 FTE 13 Dollars \$3,468,000

Description of Item

The National Security Division (NSD) requests a total of 26 positions, including sixteen attorneys and ten non-attorneys, to support the growing area of combating cyber threats to national security. These requested positions are detailed below.

Justification

One of the most significant national security threat evolutions in recent years has been the growth of cyber threats to the national security. Attacks against America's digital infrastructure were once the near-exclusive purview of ordinary criminals; however, nation states and terrorists are increasingly looking for opportunities to exploit this critical national asset. Just last month, al Qaeda released a six-minute video instructing its followers that "the U.S. is vulnerable to cyberattacks in the same way airline security was vulnerable in 2001 before the terrorist attacks of September 11," and calling on individuals "with expertise in this domain to target the websites and information systems of big companies and government agencies."² And late last year, the National Counterintelligence Executive issued a report entitled "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011," in which it stated that entities within China and Russia are

² "Al Qaeda video calling for cyberattacks on Western targets raises alarm in Congress," Fox News, (May 22, 2012), available at <http://www.foxnews.com/politics/2012/05/22/al-qaeda-video-calling-for-cyberattacks-on-western-targets-raises-alarm-in/#ixzz1x8MO0D6f>.

“responsible for extensive illicit intrusions” into our networks and the “theft of US intellectual property.”³

In 2009, President Obama acknowledged that cybersecurity threats have become “one of the most serious national security, public safety, and economic challenges we face as a nation,”⁴ and the U.S. National Security Strategy identified protecting America’s cyber infrastructure as a key national security priority. More recently, leaders from across the IC have assessed that the cyber threat will soon become the number one threat facing this country.⁵

Because cyber-based terrorism, cyber-based espionage, and other state-sponsored cyber intrusions threaten national security, NSD is involved in the full range of U.S. cyber and cybersecurity efforts, including cyber threat prevention, detection, investigation, and prosecutions, cybersecurity program development and oversight, cybersecurity vulnerability management, and cyber policy development. To keep pace with the unique challenges of this evolving threat, NSD will need to recruit, hire, and train additional cyber specialists.

This request is broken out by NSD section/office below.

Counterespionage

Program Increase: Positions 3 Atty 2 FTE 2 Dollars \$440,000

The Counterespionage Section (CES) requests two attorneys and one intelligence research specialist to support combating cyber threats to national security.

Attorneys

Two attorneys are requested to manage the rapid growth anticipated in cyber-related cases and investigations in the coming years. As technology becomes more advanced, cyber threats are likely to increase and result in more referrals from USAOs around the country. Additionally, as NSD’s National Security Cyber Specialist Network further develops, and its plan to staff Threat Focus Cells is implemented, CES anticipates an increase in the number of cyber investigations and possible prosecutions. CES also anticipates additional prosecutions due to new statutory tools and revisions to existing statutes that cover cyber threats.

³ Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, at i (Oct. 2011), available at http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf [hereinafter “ONCIX Report”].

⁴ President Barack Obama, Remarks on Securing our Nation’s Cyber Infrastructure (May 29, 2009), available at <http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>.

⁵ See Remarks of Director of National Intelligence James Clapper and FBI Director Robert S. Mueller, III Before the House Permanent Select Committee on Intelligence (HPSCI), February 10, 2012.

Intelligence Research Specialist

One intelligence research specialist is requested to assist in cyber case development. A significant part of the cyber threat evolution has involved the unlawful extraction of U.S. trade secrets and national defense information by state and non-state actors. The vast majority of reporting pertaining to these types of intrusions resides in classified databases maintained by the IC, and in many instances, it never gets disseminated to DOJ attorneys in a position to potentially develop criminal charges. An intelligence research specialist's knowledge and ability to access and cull cyber-related reporting among the vast array of data sources will be paramount to CES's efforts to generate new cases in this area. An intelligence research specialist could also provide direct analytic support to investigations already underway. Cyber investigations are typically complex, and an intelligence research specialist can spend the required time researching technical details within the case to develop products such as assessments and link charts that lay out the full scope of the illegal activity. Finally, an intelligence research specialist can work closely with personnel assigned to the FBI's National Cyber Investigative Joint Task Force and other IC cyber working groups to deconflict potential matters.

Foreign Investment Review

Program Increase: Positions 4 Atty 3 FTE 2 Dollars \$617,000

The Foreign Investment Review Staff (FIRS) requests the three attorneys and one cyber auditor to support combating cyber threats to national security.

Attorneys

Three attorneys are requested to assist with the review of foreign acquisitions as they relate to cyber threats to the national security. As a member of CFIUS, FIRS is responsible for reviewing foreign acquisitions of United States companies in order to identify any national security concerns arising from such transactions. The primary DOJ CFIUS equities are protecting the nation's telecommunications system and preventing espionage by foreign corporations or sovereign states through hardening of corporate cyber defenses and security policies. FIRS also addresses these equities through its participation in Team Telecom, an ad hoc interagency body that reviews international telecommunications licenses referred by the FCC. Through its cooperation with the FBI and the National Security Agency, FIRS assists the IC in gleaning valuable foreign intelligence information from CFIUS filings and FCC license applications and promotes the dissemination of that information throughout the IC. Once FIRS identifies national security concerns, often related to either cybersecurity or intelligence collection, through either the CFIUS or Team Telecom process, FIRS often enters into a National Security Agreement with the foreign company to ensure that any national security concerns are addressed through enhanced cyber protections and personnel security policies. Currently, FIRS is responsible for monitoring corporate compliance with nearly 100 such agreements. The requested attorneys would have responsibility for overseeing this compliance program, identifying vulnerabilities that must be addressed, and ensuring that DOJ implements appropriate monitoring strategies to ensure that these agreements serve the purpose for which they were designed.

Cyber Auditor

One cyber auditor is requested to help design and monitor mitigation compliance regimes as part of FIRS' vital operations related to cyber-security and intelligence collection. The cyber auditor would work with FIRS attorneys to manage the corporate compliance program.

Counterterrorism

Program Increase: Positions 3 Atty 2 FTE 2 Dollars \$440,000

The Counterterrorism Section (CTS) requests two attorneys and one intelligence research specialist to support combating cyber threats to national security.

Attorneys

CTS requests two attorneys to continue to address the increasing cyber threat posed by the use of the internet and technology by terrorists. CTS attorneys regularly review and provide guidance on the rapidly growing number of terrorism cases that involve cyber activity. CTS also anticipates an increase in the number of investigations and prosecutions of cyber-based terrorism in which its attorneys must play an integral role. To ensure that Department attorneys continue to be prepared to handle new and emerging cyber threats, and to disrupt potential cyber-based terrorist operations, CTS requires these resources to handle investigations and prosecutions, conduct nationwide training on cyber-related topics, and regularly participate in interagency and private industry cybersecurity meetings and initiatives.

Intelligence Research Specialist

One intelligence research specialist is requested to assist with cyber-based terrorism cases and investigations. The intelligence research specialist will review and analyze large amounts of intelligence data and enable CTS attorneys to be proactive in developing leads, investigative plans and strategies in close coordination with investigative agents and terrorism prosecutors. In today's threat environment, having the right information at the right time is essential to protecting national security. In addition, having an additional intelligence specialist will enhance CTS's ability to absorb the increasing volume of intelligence material and threat information that is sent from the FBI and other agencies. An intelligence specialist at CTS would serve as the initial point of contact for intelligence material and threat information, and could establish lines of communication with the reporting agencies to obtain supplemental information when needed. The intelligence research specialist could also generate meaningful intelligence summaries, create link analyses, and cull information in reports that highlights items of particular significance to matters within CTS.

Office of Intelligence

Program Increase: Positions 12 Atty 8 FTE 6 Dollars \$1,588,000

OI requests eight attorneys and four non-attorney positions to support combating cyber threats to national security in the areas of Intelligence Operations, Oversight, and Litigation.

Operations Attorneys

Four operations attorneys are requested to support OI's cyber efforts. OI expects to see considerable growth in the cyber area. In accordance with the growing threat and increased prioritization, the Operations Section anticipates dedicating an increasing number of resources to work on cyber-related matters and to become cyber experts. OI also expects to play a larger role in the Division's efforts to coordinate cyber-related efforts within the Department and across the Government. This has to be done in a way that does not adversely affect staffing for other national security priorities.

Oversight Attorneys

Two oversight attorneys are requested to support OI's cyber efforts. OI has continued to develop its oversight capabilities and programs to help the operations components of the IC on a programmatic basis and to increase assurance that operational activities are executed in compliance with governing rules. OI anticipates that these resources will enable OI attorneys to better help these agencies avoid mistakes that could lead to significant compliance problems, including compliance incidents subject to reporting requirements to the FISC or, potentially, the Intelligence Oversight Board and Congress. Additionally, OI has experienced a steady and significant increase in the requirements necessary to satisfy its role in the oversight of certain activities of IC agencies brought about by the FISA Amendments Act of 2008. OI's Oversight Section plays an important part in these efforts, which includes regular reviews at these agencies and the preparation of reports for Congress and the FISC. This enhanced oversight role is expected to continue to grow in the future. For example, NSD's OI Oversight Section, with the Office of the Director of National Intelligence (ODNI), executes responsibility for oversight of Section 702 of FISA. Section 702 permits the Attorney General and the Director of National Intelligence to jointly authorize the targeting of non-United States persons reasonably believed to be outside the United States to acquire foreign intelligence information. This targeting must comply with the FISC-approved targeting procedures and the acquisition, retention, and dissemination of any Section 702-acquired information must comply with FISC-approved minimization procedures. OI also reports its findings to Congress, including preparing lengthy and detailed semi-annual summaries. In addition to Section 702 oversight, OI is planning oversight of IC use of other FISA Amendments Act provisions.

Finally, as the IC expands its use and sharing of intelligence obtained through FISA authorities, OI's oversight responsibilities expand as a corollary. Accordingly, OI's Oversight Section has, and will continue, to expand the number of IC oversight reviews it conducts. These reviews are aimed primarily at ensuring that FISA-derived information is being handled in accordance with FISC-approved minimization procedures and that what is retained and disseminated by the

government is limited to foreign intelligence information. These reviews are becoming increasingly complex and time-consuming because of a growing interest shared by the Department, the FISC and Congress in how FISA-derived information is being marked, used, retained and disseminated by the government.

Fulfillment of these complex oversight responsibilities is one of OI's and NSD's most important functions. To properly discharge this function involves significant increased oversight and compliance responsibilities, which, in turn, requires increased staff resources in the OI Oversight Section to achieve.

Litigation Attorneys

Two litigation attorneys are requested to support OI's cyber efforts. OI's responsibilities in overseeing the use of FISA obtained or derived information in criminal, civil, and administrative proceedings has increased dramatically since 2001. There was a 144 percent increase in the number of FISA use requests processed by the Litigation Section compared to the previous calendar year. The Litigation Section attorneys not only process use requests and make recommendations to the Attorney General, but, once authorization has been granted, the attorneys have a significant role in drafting responses to defense motions to disclose FISA applications, orders, and other materials filed with the Foreign Intelligence Surveillance Court and to suppress information obtained or derived from FISC-authorized electronic surveillance and physical search. In calendar year 2011, there was a 300 percent increase in the number of FISA litigation briefs filed in district courts throughout the country. Aside from their role in overseeing the use of FISA-obtained or FISA-derived information in court proceedings, the attorneys in OI's Litigation Section review requests from the FBI relating to undercover operations and for approval for its agents and sources to engage in otherwise illegal activities. The Litigation Section anticipates a continued increase in workload in all areas of responsibility, as well as an additional complexity of work due in part to the Division's cyber initiatives.

Case Management Specialists

Two case management specialists are requested to support OI's attorneys. The Classified Information Management Unit (CIMU) supports OI's Operations, Oversight, and Litigation Section attorneys in a time-sensitive litigation support environment. Among other things, CIMU provides information management and operations information processing support for specific ongoing programs, and serves as a liaison to the court. Functionally CIMU maintains OI's case tracking system, including processing, scanning, indexing, and filing of all incoming and outgoing matters, to include data integrity function.

Administrative Support

Two administrative support positions are requested to support OI's attorneys. These individuals will assist with the office administrative and personnel support functions for the section. In addition, due to the unique security needs of the OI SCIF environment, it is critical to have adequate support staff to cover the entrances and exits to OI, as well as to provide escorts for visitors to the OI SCIFs.

Law and Policy

Program Increase: Positions 4 Atty 1 FTE 2 Dollars \$383,000

The Law and Policy Office (L&P) requests the following four positions to support combating cyber threats to national security: one attorney, one paralegal, one records management specialist, and one administrative support specialist.

Attorney

One attorney is requested to focus on cyber issues relating to national security. NSD is working to expand its work on cyber matters to align it with the magnitude of the threat posed to our national security by malicious cyber actors, whether they are sponsored by states, terrorist organizations, or others. NSD's leadership recently endorsed the report of its Cyber Review Team that calls for a number of substantial cyber policy initiatives, including development and coordination of an NSD Cyber Strategy and an action plan for accomplishing its goals. It also directs preparation of a bluebook on legal issues pertaining to combating cyber threats, for use by USAOs and others involved in the investigation and prosecution of these threats; an evaluation of AG Guidelines pertaining to cyber investigations and prosecutions; issuance of detailed standard operating procedures to assist victims of intrusions and investigative agencies; and steady distribution of legal development updates in the cyber area for the field. More generally, it calls for NSD to take a more active policy role in cyber policy matters across the government. This work is expressly assigned to L&P. It is anticipated that work in the cyber area will continue to grow in the years ahead. L&P currently has only two attorneys working principally on cyber issues, and neither of them does so exclusively. A third attorney is on a one-year detail from the Southern District of New York. The new attorney position would enable L&P to fill that third position on a permanent basis.

Paralegal Specialist

One paralegal Specialist is requested to support L&P attorneys. L&P has more than twenty-five attorneys supported by one paralegal. This individual principally supports the appellate unit, which continues to grow as the appellate work expands. Moreover, there are a number of functions frequently performed by others in the office for which paralegal support would be extremely helpful and would save scarce attorney time, such as preparation for Congressional hearings, briefing books for senior officials, and basic research assistance. In addition, the legislative referral memorandum process for which the office is responsible is labor intensive and is currently managed by several attorneys in the office on a rotating basis. Much of this work would be more appropriately performed by a paralegal under the supervision of an attorney, which would free up scarce attorney time to focus on more substantive work.

Records Management Specialist

One records management specialist is requested to assist with records management issues throughout the Division, with a particular emphasis on electronic records management and case file management in the Counterespionage and Counterterrorism Sections both of which are expected to see an increase in cyber related investigations and prosecutions. Each component of

the Department is responsible for managing its own records throughout the records management lifecycle (creation, maintenance and use, disposition). Currently this function is performed on an ad hoc basis by the Division's Records and FOIA Chief and one contractor, along with the assistance of case managers in each component. Adding a professional records manager with a career ladder built into the position will allow us to manage the Division's records more effectively in the short term and lay the foundation for an effective program in years to come.

Administrative Support

One administrative support position is requested to support L&P attorneys. L&P has more than twenty-five attorneys supported by one administrative liaison/office manager. There is no administrative assistant to perform routine office support functions such as assisting in preparation of documents, helping with scheduling meetings, taking phone messages, escorting visitors, and the like. The office manager assists with these functions but cannot accomplish this work for the number of attorneys in the office and do all the other work for which she is responsible, including managing time and attendance and travel, supporting the Deputy Assistant Attorney General for L&P, handling financial/budget and procurement issues, ensuring compliance of the office with administrative policies. As a result, the attorneys in the office spend a lot of valuable time performing functions that are more properly done by administrative support staff. Adding an administrative support position would make the ratio of attorneys to support staff for L&P closer to the ratio that exists in other parts of the Division and the Department and will significantly improve the overall efficiency of the office.

Impact on Performance

As described above, these requests for resources will allow NSD to keep pace with the growth of cyber threats to the national security, and can ensure that the government is taking a proactive, all-tools approach to deterrence and disruption of these threat actors.

Funding

Summary

FY 2012 Enacted (w/cancellations)				FY 2013 Continuing Resolution				FY 2014 Current Services			
Pos	Atty	FTE	\$(000)	Pos	Atty	FTE	\$(000)	Pos	Atty	FTE	\$(000)
117	113	117	\$22,963	138	132	138	\$27,021	138	132	138	\$27,021

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)
Attorney (GS 15)	\$160	16	\$2,560	\$1,280
Intelligence Research Specialist (GS 13)	120	2	240	124
Cyber Auditor (14)	137	1	137	57
Case Management Specialist (GS 9)	94	2	188	66
Administrative Support (GS 7)	60	3	180	85
Paralegal Specialist (GS 11)	103	1	103	40
Records Management Specialist (GS 7)	60	1	60	28
Total Personnel		26	\$3,468	\$1,680

Total Request for this Item

	Pos	Atty	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)	FY 2015 Net Annualization (Change from 2014) (\$000)
Current Services	138	132	138	\$27,021	\$0	\$27,021	\$0
Increases	26	16	13	3,468	0	3,468	1,680
Grand Total	164	148	151	\$30,489	\$0	\$30,489	\$1,680

B. Item Name: **Combating Homegrown Violent Extremist Threats**

Budget Decision Unit: National Security Division

Strategic Goal: Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law
Objective 1.2 Prosecute those involved in terrorist acts

Organizational Program: Counterterrorism, Information Technology

Component Ranking of Item: 2 of 3

Program Increase: Positions 2 Atty 2 FTE 1 Dollars \$320,000

Description of Item

NSD requests two attorneys to support combating homegrown violent extremist (HVE) threats.

Justification

Two attorneys are requested to address the increasing demand for attorney resources in HVE investigations and prosecutions. While cyber-related terrorism is poised to pose the overall fastest-growing threat to the homeland, HVEs represent the most significant threat for violent attacks in the homeland. CTS provides full spectrum support to the FBI, IC, and the United States Attorneys' Offices for every HVE case in the country, and the numbers are increasing. These investigations are complex and involve a number of difficult legal issues requiring extensive attorney support throughout the investigations advising on both the investigative strategy and conduct. As a general rule CTS attorneys are also on the trial team prosecuting the cases in districts around the country, sometimes for extended periods of time.

Impact on Performance

As described above, the request for resources for CTS relates directly to the Department's highest priority: Preventing Terrorism and Promoting the Nation's Security Consistent with the Rule of Law. It is imperative to national security that CTS be able to meet increasing demands to combating homegrown violent extremist threats.

Funding

Summary

FY 2012 Enacted (w/cancellations.)				FY 2013 Continuing Resolution				FY 2014 Current Services			
Pos	Atty	FTE	\$(000)	Pos	Atty	FTE	\$(000)	Pos	Atty	FTE	\$(000)
71	53	71	\$14,201	71	53	71	\$14,534	71	53	71	\$14,871

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)
Attorney (GS 15)	\$160	2	\$320	\$160
Total Personnel	\$160	2	\$320	\$160

Total Request for this Item

	Pos	Atty	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)	FY 2015 Net Annualization (Change from 2014) (\$000)
Current Services	71	53	71	\$14,871	\$0	\$14,871	\$0
Increases	2	2	1	320	0	320	160
Grand Total	73	55	72	\$15,191	\$0	\$15,191	\$160

C. Item Name: Intelligence Collection and Oversight

Budget Decision Unit: National Security Division

Strategic Goal: Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law
Objective 1.1 Prevent, disrupt, and defeat terrorist operations before they occur

Organizational Program: Intelligence, Information Technology

Component Ranking of Item: 3 of 3

Program Increase: Positions 2 Atty 2 FTE 1 Dollars \$320,000

Description of Item

NSD requests two attorneys to support other intelligence collection and oversight. As noted above, OI is comprised of three sections: Litigation, Operations, and Oversight. While each section has a distinct mission, the three sections work collaboratively in support of the national security priorities of the Division, the Department, and the IC. To this end, office resources, are frequently shifted within OI to allow flexibility as operational needs dictate.

Although much of OI's increase in workload is expected to come in combating cyber threats to the national security, NSD expects additional increases in other intelligence-related areas as well.

Justification

Operations Attorney

One operations attorney is requested to support other intelligence collection and oversight. OI's Operations Section is responsible, among other things, for preparing applications for electronic surveillance and physical search to the FISC in national security investigations pursuant to FISA, as well as for providing legal advice to Division and Department leadership and the IC on a variety of intelligence-related matters. The trends over the last several years have shown an unmistakable increase in the number of requests for FISA authorities handled by the Operations Section. For example, between 2009 and 2010, the number of FISA applications for electronic surveillance and/or physical search increased by approximately 15 percent (from 1,376 in 2009 to 1,579 in 2010); that number increased a further approximately 11 percent in the following year (from 1,574 in 2010 to 1745 in 2011). OI anticipates a continuation of this trend over the coming years. Also particularly noteworthy has been the increase in the demand for business records requests pursuant to Section 1861 of FISA: 21 such requests were approved in 2009; 96 in 2010; and 205 in 2011 (an increase of approximately 876 percent between 2009 and 2011). OI expects the number of business records requests to remain near or above 2011 levels for the

foreseeable future. Additional attorney resources are needed in order to address the increased workload.

Litigation Attorney

One litigation attorney is requested to support other intelligence collection and oversight. OI's responsibilities in overseeing the use of FISA obtained or derived information in criminal, civil, and administrative proceedings has increased dramatically since 2001. There was a 144 percent increase in the number of FISA use requests processed by the Litigation Section compared to the previous calendar year. The Litigation Section attorneys not only process use requests and make recommendations to the Attorney General, but, once authorization has been granted, the attorneys have a significant role in drafting responses to defense motions to disclose FISA applications, orders, and other materials filed with the Foreign Intelligence Surveillance Court and to suppress information obtained or derived from FISC-authorized electronic surveillance and physical search. In calendar year 2011, there was a 300 percent increase in the number of FISA litigation briefs filed in district courts throughout the country. Aside from their role in overseeing the use of FISA-obtained or FISA-derived information in court proceedings, the attorneys in OI's Litigation Section review requests from the FBI relating to undercover operations and for approval for its agents and sources to engage in otherwise illegal activities. Recently, there has been a growing complexity of many of these operations and additional resources are required.

Impact on Performance

OI's daily activities in support of the IC include the preparation and filing of pen register/trap and trace applications, requests for the production of tangible things, and requests for statutory exemptions related to undercover operations and the conduct of otherwise illegal activities as allowed by law. They also include handling requests for Attorney General authorization to use FISA information in criminal and civil proceedings, authorizations for certain intelligence activities under Executive Order 12333, and, as described above, an extensive oversight and advisory role within the IC that continues to grow. These resources will better enable OI to meet an ever-increasing workload that directly relates to the Department's highest priority: Preventing Terrorism and Promoting the Nation's Security Consistent with the Rule of Law.

Funding

Summary

FY 2012 Enacted (w/cancellations)				FY 2013 Continuing Resolution				FY 2014 Current Services			
Pos	Atty	FTE	\$(000)	Pos	Atty	FTE	\$(000)	Pos	Atty	FTE	\$(000)
165	134	163	\$49,115	165	134	163	\$50,265	165	134	163	\$51,431

Personnel Increase Cost Summary

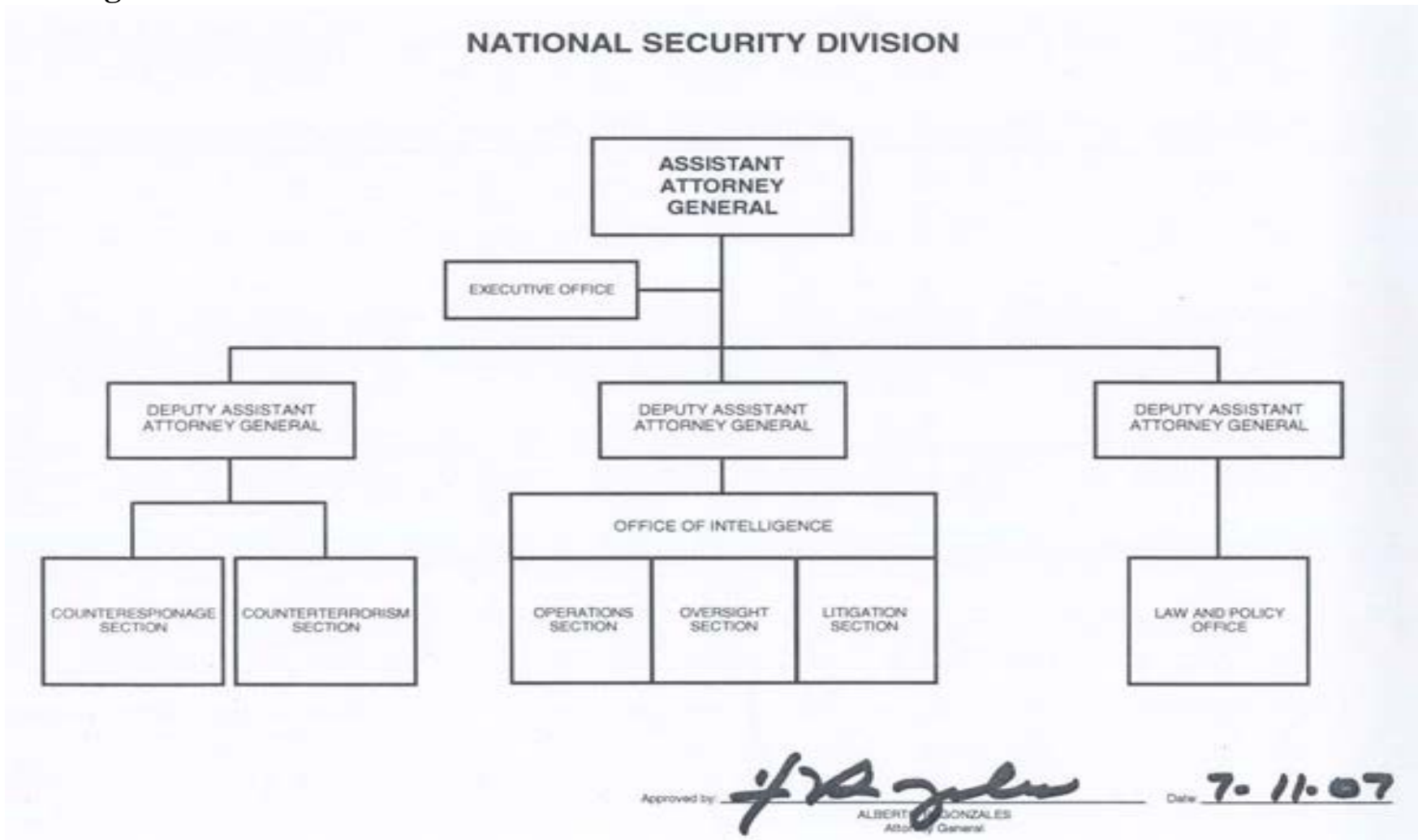
Type of Position	Modular Cost per Position (\$000)	Number of Positions Requested	FY 2014 Request (\$000)	FY 2015 Net Annualization (Change from 2014) (\$000)
Attorney (GS 15)	\$160	2	\$320	\$160
Total Personnel	\$160	2	\$320	\$160

Total Request for this Item

	Pos	Atty	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)	FY 2015 Net Annualization (Change from 2014) (\$000)
Current Services	165	134	163	\$51,431	\$0	\$51,431	\$0
Increases	2	2	1	320	0	320	160
Grand Total	167	136	164	\$51,751	\$0	\$51,751	\$160

VII. Exhibits

A. Organizational Chart



B. Summary of Requirements

Summary of Requirements

National Security Division
Salaries and Expenses
(Dollars in Thousands)

	FY 2014 Request		
	Direct Pos.	Estimate FTE	Amount
2012 Enacted	359	298	87,000
2013 Continuing Resolution*	359	304	87,000
2013 CR 0.612% Increase	0	0	532
Total 2013 Continuing Resolution	359	304	87,532
Technical Adjustments			
Adjustment - 2013 CR 0.612%	0	0	(532)
Total Technical Adjustments	0	0	(532)
Base Adjustments			
Transfers:			
JCON and JCON S/TS	0	0	1,182
Office of Information Policy (OIP)	0	0	(22)
Professional Responsibility Advisory Office (PRAO)	0	0	(69)
Pay and Benefits	0	6	624
Domestic Rent and Facilities	0	0	3,417
Total Base Adjustments	0	6	5,132
Total Technical and Base Adjustments	0	6	4,600
2014 Current Services	359	310	92,132
Program Changes			
Increases:			
Combating Cyber Threats to National Security	26	13	3,468
Combating Homegrown Violent Extremist Threats (HVE)	2	1	320
Intelligence Collection	2	1	320
Subtotal, Increases	30	15	4,108
Total Program Changes	30	15	4,108
2014 Total Request	389	325	96,240
2012 - 2014 Total Change	30	27	9,240

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

B. Summary of Requirements

Summary of Requirements

National Security 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
National Security Division	359	298	87,000	359	304	87,532	0	6	4,600	359	310	92,132
Total Direct	359	298	87,000	359	304	87,532	0	6	4,600	359	310	92,132
Balance Rescission			0			0			0			0
Total Direct with Rescission			87,000			87,532			4,600			92,132
Reimbursable FTE		0			0			0			0	
Total Direct and Reimb. FTE		298			304			6			310	
Other FTE: LEAP Overtime												
Grand Total, FTE		298			304			6			310	

Program Activity	2014 Increases			2014 Offsets			2014 Request		
	Direct Pos.	Actual FTE	Amount	Direct Pos.	Est. FTE	Amount	Direct Pos.	Est. FTE	Amount
National Security Division	30	15	4,108	0	0	0	389	325	96,240
Total Direct	30	15	4,108	0	0	0	389	325	96,240
Balance Rescission			0			0			0
Total Direct with Rescission			4,108			0			96,240
Reimbursable FTE		0			0			0	
Total Direct and Reimb. FTE		15			0			325	
Other FTE: LEAP Overtime									
Grand Total, FTE		15			0			325	

*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

National Security Division
Salaries and Expenses
(Dollars in Thousands)

Program Increases	Location of Description by Program Activity	National Security Division				Total Increases			
		Direct Pos.	Agt./ Atty.	Est. FTE	Amount	Direct Pos.	Agt./ Atty.	Est. FTE	Amount
Combating Cyber Threats to National Security	National Security Division	26	16	13	3,468	26	16	13	3,468
Combating Homegrown Violent Extremist Threats	National Security Division	2	2	1	320	2	2	1	320
Intelligence Collection	National Security Division	2	2	1	320	2	2	1	320
Total Program Increases		30	20	15	4,108	30	20	15	4,108

D. Resources by DOJ Strategic Goal and Strategic Objective

Resources by Department of Justice Strategic Goal/Objective

National Security 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.												
	192	61,123	195	61,497	199	64,729	8	1,994	0	0	207	66,723
1.2 Prosecute those involved in terrorist acts.	73	17,498	75	17,605	76	18,530	2	839	0	0	78	19,369
1.3 Combat espionage against the United States.	33	8,379	34	8,430	35	8,873	5	1,275	0	0	40	10,148
Subtotal, Goal 1	298	87,000	304	87,532	310	92,132	15	4,108	0	0	325	96,240
TOTAL	298	87,000	304	87,532	310	92,132	15	4,108	0	0	325	96,240

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

National Security 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.			(532)
Subtotal, Technical Adjustments	0	0	(532)
Transfers			
1 <u>JCON and JCON S/TS:</u> A transfer of \$1,182,000 is included in support of the Department's Justice Consolidated Office Network (JCON) and JCON S/TS programs which moved to the Working Capital Fund and is provided as a billable service.			1,182
2 <u>Office of Information Policy (OIP):</u> The National Security Division transfers for the Office of Information Policy (OIP) into the General Administration appropriation and 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.			(22)
3 <u>Professional Responsibility Advisory Office (PRAO):</u> The National Security Division transfers for the Professional Responsibility Advisory Office (PRAO) into the General Administration appropriation will transfer 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.			(69)
Subtotal, Transfers	0	0	1,091
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 increase only includes the general pay raise. The amount request, \$355,000, represents the pay amounts for 3/4 of the fiscal year plus appropriate benefits (\$252,050 for pay and \$102,950 for benefits.)			355
2 <u>Annualization of 2012 Approved Positions:</u>		6	
3 <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 percent included in the 2013 President's Budget. The amount requested \$70,000 represents the pay amounts for 1/4 of the fiscal year plus appropriate benefits (\$49,700 for pay and \$20,300 for benefits).			70
4 <u>Employee Compensation Fund:</u> The \$1,000 decrease reflects anticipated changes in payments to the Department of Labor for injury benefits under the Federal Employee Compensation Act.			(1)
5 <u>Health Insurance:</u> Effective January 2014, the component's contribution to Federal employees' health insurance increases by 5.4 percent. Applied against the 2013 estimate of \$2,224,000, the additional amount required is \$119,000.			119
6 <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 \$81,000 is necessary to meet our increased retirement obligations as a result of this conversion.			81
Subtotal, Pay and Benefits	0	6	624
Domestic Rent and Facilities			
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 increase of \$954,000 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 increases.			954
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 increase of \$63,000 is required to meet these commitments.			63
3 <u>Non-GSA:</u> The requested increase of \$2,400,000 is required to meet our commitment for locations which are not provided by GSA.			2,400
Subtotal, Domestic Rent and Facilities	0	0	3,417
TOTAL DIRECT TECHNICAL and BASE ADJUSTMENTS	0	6	4,600

F. Crosswalk of 2012 Availability

Crosswalk of 2012 Availability

National Security Division
Salaries and Expenses
(Dollars in Thousands)

Program Activity	2012 Appropriation Enacted w/o Balance Rescission			Balance Rescission			Reprogramming/Transfers			Carryover	Recoveries/ Refunds	2012 Actual		
	Direct Pos.	Actual FTE	Amount	Direct Pos.	Actual FTE	Amount	Direct Pos.	Actual FTE	Amount	Amount	Amount	Direct Pos.	Actual FTE	Amount
National Security Division	359	298	87,000	0	0	0	0	0	2,500	7,659	26	359	298	97,185
Total Direct	359	298	87,000	0	0	0	0	0	2,500	7,659	26	359	298	97,185
Reimbursable FTE		0												0
Total Direct and Reimb. FTE		298												298
Other FTE: LEAP Overtime														
Grand Total, FTE		298			0			0					298	

Reprogramming/Transfers: NSD transferred \$2,500,000 of prior year funds for IT related projects.

Carryover: NSD carryover of \$7,659,000 will fund IT related projects.

Recoveries/Refunds: NSD has a recovery of \$26,000.

G. Crosswalk of 2013 Availability

Crosswalk of 2013 Availability
National Security Division
Salaries and Expenses
(Dollars in Thousands)

Program Activity	FY 2013 Continuing Resolution*			2013 Supplemental Appropriation Amount	2013 Reprogramming/Transfers			2013 Carryover Amount	2013 Recoveries/ Refunds Amount	2013 Availability		
	Direct Pos.	Estim. FTE	Amount		Direct Pos.	Estim. FTE	Amount			Direct Pos.	Estim. FTE	Amount
National Security Division	359	304	87,532	0	0	0	0	6,179	0	359	304	93,711
Total Direct	359	304	87,532	0	0	0	0	6,179	0	359	304	93,711
Balance Rescission			0									0
Total Direct with Rescission			87,532									93,711
Reimbursable FTE		0				0		0			0	
Total Direct and Reimb. FTE		304				0		6,179			304	
Other FTE:												
LEAP		0				0		0			0	
Overtime		0				0		0			0	
Grand Total, FTE		304				0		6,179			304	

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

Carryover: NSD carried over \$6,179,000 of prior year funds for IT related projects.

I. Detail of Permanent Positions by Category

Detail of Permanent Positions by Category

National Security 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.
Security Specialists (080)	4		4			0		4	
Intelligence Series (132)	11		11			2		13	
Clerical and Office Services (300-399)	78		78			6		84	
Accounting and Budget (500-599)	7		7			1		8	
Attorneys (905)	236		236			20		256	
Paralegals / Other Law (900-998)	13		13			1		14	
Business & Industry (1100-1199)	1		1			0		1	
Information Technology Mgmt (2210)	9		9			0		9	
Total	359	0	359	0	0	30	0	389	0
Headquarters (Washington, D.C.)	358		358			30		388	
U.S. Field	1		1			0		1	
Foreign Field									
Total	359		359			30		389	

Financial Analysis of Program Changes

National Security Division
Salaries and Expenses
(Dollars in Thousands)

Grades	National Security Division						Total Program Changes	
	Combating Cyber Threats to National Security		Countering Homegrown Violent Extremist Threats		Intelligence Collection			
	Direct Pos.	Amount	Direct Pos.	Amount	Direct Pos.	Amount	Direct Pos.	Amount
GS-15	16	2,256	2	282	2	282	20	2,820
GS-14	1	106	0	0	0	0	1	106
GS-13	2	179	0	0	0	0	2	179
GS-11	1	63	0	0	0	0	1	63
GS-9	2	104	0	0	0	0	2	104
GS-7	4	170	0	0	0	0	4	170
Total Positions and Annual Amount	26	2,878	2	282	2	282	30	3,442
Lapse (-)	(13)	(1,439)	(1)	(141)	(1)	(141)	(15)	(1,721)
11.5 Other Personnel Compensation		0		0		0		0
Total FTEs and Personnel Compensation	13	1,439	1	141	1	141	15	1,721
13.0 Benefits for former personnel		404		39		39		482
21.0 Travel and Transportation of Persons		81		7		7		95
22.0 Transportation of Things		28		2		2		32
23.3 Communications, Utilities, and Miscellaneous Charges		130		10		10		150
25.2 Other Services from Non-Federal Sources		68		8		8		84
25.3 Other Goods and Services from Federal Sources		162		13		13		188
26.0 Supplies and Materials		15		1		1		17
31.0 Equipment		1,141		99		99		1,339
Total Program Change Requests	13	3,468	1	320	1	320	15	4,108

K. Summary of Requirements by Grade

Summary of Requirements by Grade

National Security 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
SES/SL \$ 119,554 - 179,700	18		18		18		0	
GS-15 \$ 123,758 - 155,500	221		221		241		20	
GS-14 \$ 105,211 - 136,771	24		24		25		1	
GS-13 \$ 89,033 - 115,742	34		34		36		2	
GS-12 \$ 74,872 - 97,333	13		13		13		0	
GS-11 \$ 62,467 - 81,204	21		21		22		1	
GS-9 \$ 51,630 - 67,114	16		16		18		2	
GS-8 \$ 46,745 - 60,765	10		10		10		0	
GS-7 \$ 42,209 - 54,875	1		1		5		4	
GS-6 \$ 37,983 - 49,375	1		1		1		0	
Total, Appropriated Positions	359		359		389		30	
Average SES Salary		174,273		175,144		176,895		
Average GS Salary		121,514		122,122		123,343		
Average GS Grade		14		14		14		

L. Summary of Requirements by Object Class

Summary of Requirements by Object Class

National Security 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	298	36,818	304	42,497	325	45,443	21	2,946
11.3 Other than Full-Time Permanent	0	618	0	625	0	625	0	0
11.5 Other Personnel Compensation	0	583	0	595	0	595	0	0
<i>Overtime</i>	0	0	0	0	0	0	0	0
<i>Other Compensation</i>	0	0	0	0	0	0	0	0
11.8 Special Personal Services Payments	0	498	0	0	0	0	0	0
Total	298	38,517	304	43,717	325	46,663	21	2,946
Other Object Classes								
12.0 Personnel Benefits		11,027		12,753		13,054		301
21.0 Travel and Transportation of Persons		1,275		2,141		2,141		0
22.0 Transportation of Things		762		760		760		0
23.1 Rental Payments to GSA		9,448		9,903		10,857		954
23.2 Rental Payments to Others		203		213		213		0
23.3 Communications, Utilities, and Miscellaneous Charges		3,971		4,176		7,703		3,527
24.0 Printing and Reproduction		2		1		1		0
25.1 Advisory and Assistance Services		1,124		1,150		1,150		0
25.2 Other Services from Non-Federal Sources		8,886		9,825		8,245		(1,580)
25.3 Other Goods and Services from Federal Sources		2,502		3,950		2,498		(1,452)
25.4 Operation and maintenance of facilities		0		5		5		0
25.6 Medical Care		26		23		23		0
25.7 Operation and Maintenance of Equipment		213		195		195		0
26.0 Supplies and Materials		327		253		253		0
31.0 Equipment		6,983		4,646		2,479		(2,167)
Total Obligations		85,266		93,711		96,240		2,529
Subtract - Unobligated Balance, Start-of-Year		(7,659)		(6,179)		0		6,179
Subtract - Transfers/Reprogramming		(2,500)		0		0		0
Subtract - Recoveries/Refunds		(26)		0		0		0
Add - Unobligated End-of-Year, Available		6,179		0		0		0
Add - Unobligated End-of-Year, Expiring		5,740		0		0		0
Total Direct Requirements	0	87,000	0	87,532	0	96,240	0	8,708
Reimbursable FTE								
Full-Time Permanent								
23.1 Rental Payments to GSA (Reimbursable)								
25.3 Other Goods and Services from Federal Sources - DHS Security (Reimbursable)								

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