FY 2016
Performance Budget
Congressional Submission

NATIONAL SECURITY DIVISION

U.S. Department of Justice

Table of Contents

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 2016 a total of 411 positions (including 270 attorneys), 359 FTE, and $96,596,000.[1]

B. Background

In recent years, 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-related programs and its intelligence oversight function;
- Continuing to bring an all-tools, integrated approach to NSD's work, while 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 2016 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 an evolving threat. NSD's assessment of the challenges it faces in fully realizing its goals in these areas are outlined more fully in section I.D.: Performance Challenges.

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:

- Office of Intelligence (OI);
- Counterterrorism Section (CTS);
- Counterespionage Section (CES);
- Office of Law and Policy (L&P); and,

[1] Within the totals outlined above, NSD has included a total of 14 positions, 14 FTE, and $14,299,000 for Information Technology (IT).

- 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

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 and homegrown violent extremism;
- 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.

Counterintelligence and Export Control

- Supporting and supervising the investigation and prosecution of cases involving treason, sedition, espionage, economic espionage, and cyber threats to the national security 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.

Intelligence Operations and Litigation

- Ensuring that IC agencies have the legal tools necessary to conduct intelligence operations while safeguarding privacy and civil liberties;
- Representing the U.S. 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.

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, 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 U.S. (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;
- Responding to Federal Communications 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 these processes.

Victims of Terrorism

- 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)

- Continued to lead the nation's counterterrorism enforcement program through collaboration with Department leadership, the FBI, the IC, and the USAOs.
- Through the National Security Cyber Specialist Network, the FBI's National Cyber Investigative Joint Task Force, and a USAO, secured the first-ever indictment of members of a nation state's military for cyber-based corporate theft.
- Continued to support the IC by seeking authority under FISA with the FISC.

- Designated 198 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.
- Successfully investigated and prosecuted national security threat actors – specific examples detailed below.
- Managed an increased workload associated with the CFIUS.

C. Full Program Costs

The NSD has a single decision unit. Its program activities include intelligence, counterterrorism, counterespionage, and cyber security, which are related to DOJ Strategic Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law, and its four 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 four 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 a significant 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 oversight, operations, and litigation; and
4. difficulties inherent in supporting the development of a Division in an ever-changing environment.

Among the most significant challenges that NSD continues to face 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 continue 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 continue to 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, including foreign fighters, have grown in national prominence, and identifying and disrupting these isolated actors and their operations pose distinct challenges for investigators and prosecutors.

Additionally, in January, 2014, the President delivered a speech announcing reforms to the nation's intelligence programs; in it, he emphasized that "threats like terrorism and proliferation and cyber-attacks are not going away any time soon,"[2] and reiterated our need to combat these growing threats. He also tasked the Department with working on at least ten different lines of effort related to intelligence reform and oversight, the vast majority of which falls to NSD to implement. NSD requires permanent resources dedicated to implementing these taskings.

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

E. Environmental Accountability

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

[2] Remarks by the President on Review of Signals Intelligence (January 17, 2014), available at http://www.whitehouse.gov/photos-and-video/video/2014/01/17/president-obama-speaks-us-intelligence-programs#transcript.

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	12	6	1,745	40
Intelligence Collection and Oversight	Requesting additional resources for NSD's work related to intelligence collection and oversight	10	5	1,486	49
Combating Terrorism including Homegrown Violent Extremism	Requesting additional resources for NSD's work related to combating terrorism	6	3	874	55
Program Decreases	Program and/or Administrative Savings	0	0	(1,200)	61
TOTAL, NSD		28	14	$2,905	

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, [$93,000,000] $96,596,000, 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

No change proposed.

IV. Program Activity Justification

National Security Division

National Security Division	Direct Pos.	Estimate FTE	Amount
2014 Enacted	383	336	$91,800,000
2015 Enacted	383	345	93,000,000
Adjustments to Base and Technical Adjustments	0	0	691,000
2016 Current Services	383	345	93,691,000
2016 Program Increases	28	14	4,105,000
2016 Program Decrease	0	0	(1,200,000)
2016 Request	411	359	96,596,000
Total Change 2015-2016	**28**	**14**	**$3,596,000**

National Security Division-Information Technology Breakout (of Decision Unit Total)	Direct Pos.	Estimate FTE	Amount
2014 Enacted	14	14	$15,419,000
2015 Enacted	14	14	14,299,000
Adjustments to Base and Technical Adjustments	0	0	0
2016 Current Services	14	14	14,299,000
2016 Program Increases	0	0	0
2016 Program Decrease	0	0	0
2016 Request	14	14	14,299,000
Total Change 2015-2016	0	0	$0

1. Program Description

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

In coordination with the FBI, the IC, and the USAOs, NSD's primary operational function is to prevent, deter, and disrupt terrorist and other acts that threaten the U.S. The NSD also serves as the Department's liaison to the Director of National Intelligence, advises the Attorney General on all matters relating to the national security activities of the U.S., and develops strategies for emerging national security threats – including cyber threats to the national security.

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 FISC, and – when evidence obtained or derived under FISA is proposed to be used in a criminal proceeding –obtains the necessary authorization for the Attorney General to take appropriate actions to safeguard national security. NSD also works closely with the Congressional Intelligence and Judiciary Committees to ensure they are apprised of Departmental views on national security and intelligence policy and are appropriately informed regarding operational intelligence and counterintelligence issues.

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 processes, 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 transactions, any foreign government ownership or control, threat assessments provided by the IC, vulnerabilities resulting from transactions, and ultimately the national security risks, if any, of allowing a 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 by integrating intelligence and law enforcement efforts to achieve a coordinated response to terrorist threats; 1.2 Prosecute those involved in terrorist acts; 1.3 Investigate and prosecute espionage activity against the U.S., strengthen partnerships with potential targets of intelligence intrusions, and proactively prevent insider threats; and 1.4 Combat cyber-based threats and attacks through the use of all available tools, strong public-private partnerships, and the investigation and prosecution of cyber threat actors												
WORKLOAD/ RESOURCES		**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)**		
		FY 2014		**FY 2014**		**FY 2015**		**Current Services Adjustments and FY 2016 Program Changes**		**FY 2016 Request**		
Workload[1]												
Cases Opened[2]		142		129		127		5		132		
Cases Closed[2]		122		162		112		0		112		
Matters Opened		72,524		85,178		72,561		0		72,561		
Matters Closed		72,411		85,111		72,458		0		72,458		
FISA Applications Filed[3]		CY 2014: 2,200		CY 2014: 2,200		CY 2015: 2,200		0		CY 2016: 2,200		
National Security Reviews of Foreign Acquisitions		CY 2014: 200		CY 2014: 233		CY 2015: 225		0		CY 2016: 225		
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**	
		336	91,800	336	91,800	345	93,000	14	2,596	359	95,596	
		FY 2014		**FY 2014**		**FY 2015**		**Current Services Adjustments and FY 2016 Program Changes**		**FY 2016 Request**		
Program Activity	**Intelligence**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	
		204	62,396	204	62,936	202	60,087	-14	(12,534)	188	47,553	
Output Measure	Intelligence Community Oversight Reviews	CY 2014: 89		CY 2014: 109		CY 2015: 97		0		CY 2016: 97		

Note: The FTE and funding data provided for 2016 changed from 2014 and 2015 due to the internal reallocation of resources between the NSD Sections.

[1]Workload 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.

[2]Beginning FY 2014, the Counterterrorism Section will count each defendant as a case to more accurately reflect workload as cases often times have multiple defendants. This will also be consistent with the way the Counterespionage Section counts cases for the cases opened and closed measures.

[3]FISA 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 U.S. Courts and the Congress in April for the preceding calendar year.

PERFORMANCE AND RESOURCES TABLE												
Decision Unit: National Security Division												
DOJ Strategic Goal/Objective: 1.1 Prevent, disrupt, and defeat terrorist operations before they occur by integrating intelligence and law enforcement efforts to achieve a coordinated response to terrorist threats; 1.2 Prosecute those involved in terrorist acts; 1.3 Investigate and prosecute espionage activity against the U.S., strengthen partnerships with potential targets of intelligence intrusions, and proactively prevent insider threats; and 1.4 Combat cyber-based threats and attacks through the use of all available tools, strong public-private partnerships, and the investigation and prosecution of cyber threat actors												
WORKLOAD/ RESOURCES		**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)**		
		FY 2014		**FY 2014**		**FY 2015**		**Current Services Adjustments and FY 2016 Program Changes**		**FY 2016 Request**		
Program Activity	**Counterterrorism**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	
		86	18,934	86	18,934	85	18,235	-3	4,829	82	23,064	
Efficiency Measure	Percentage of OVT responses to victims within 3 business days of victim request for information from OVT	80%		100%		80%		0%		80%		
Outcome Measure	Percentage of services/rights OVT successfully provided to victims of new attacks	95%		99%		95%		0%		95%		
Outcome Measure	Percentage of CT defendants whose cases were favorably resolved	90%		92%		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**	
		36	7,816	36	7,816	39	11,989	25	9,591	64	21,580	
Outcome Measure	Percentage of CE defendants whose cases were favorably resolved	90%		98%		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 completed[1]	12		12		14		0		14		
Output Measure	High priority national security reviews completed	CY 2014: 30		CY 2014: 32		CY 2015: 35		0		CY 2016: 35		
Program Activity	**Cyber**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	
		10	2,654	10	2,654	19	2,689	6	1,710	25	4,399	
New FY 2015 Outcome Measure	Percentage of Cyber defendants whose cases were favorably resolved	90%		NA[1]		90%		0		90%		

Note: The FTE and funding data provided for 2016 changed from 2014 and 2015 due to the internal reallocation of resources between the NSD Sections.

[1] NSD cannot report an actual for this measure because no cyber cases were resolved during FY 2014.

PERFORMANCE MEASURE TABLE

Decision Unit: National Security Division **DOJ Strategic Goal/Objective: 1.1 Prevent, disrupt, and defeat terrorist operations before they occur by integrating intelligence and law enforcement efforts to achieve a coordinated response to terrorist threats; 1.2 Prosecute those involved in terrorist acts; 1.3 Investigate and prosecute espionage activity against the U.S., strengthen partnerships with potential targets of intelligence intrusions, and proactively prevent insider threats; and 1.4 Combat cyber-based threats and attacks through the use of all available tools, strong public-private partnerships, and the investigation and prosecution of cyber threat actors**

Performance Report and Performance Plan Targets		FY 2010	FY 2011	FY 2012	FY 2013	FY 2014	FY 2014	FY 2015	FY 2016
		Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Performance Measure	Intelligence Community Oversight Reviews	NA	CY 2011: 92	CY 2012: 99	CY 2013: 112	CY 2014: 89	CY 2014: 109	CY 2016: 97	CY 2016: 97
Efficiency Measure	Percentage of OVT responses to victims within 3 business days of victim request for information from OVT	95%	90%	89%	100%	80%	100%	80%	80%
Outcome Measure	Percentage of services/rights OVT successfully provided to victims of new attacks	N/A	N/A	N/A	94%	95%	99%	95%	95%
Outcome Measure	Percentage of CT defendants whose cases were favorably resolved	100%	98%	98%	94%	90%	92%	90%	90%
Outcome Measure	Percentage of CT cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	100%	100%	100%	99%	99%	100%	99%	99%
Outcome Measure	Percentage of CE defendants whose cases were favorably resolved	94%	98%	100%	100%	90%	98%	90%	90%
Performance Measure	FARA inspections completed	15	15	15	15	12	12	12	14
Performance Measure	High priority national security reviews completed	FY 2010: 28	FY 2011: 29	CY 2012: 37[1]	CY 2013: 30	CY 2014: 30	CY 2014: 32	CY 2015: 35	CY 2016: 35
Outcome Measure	Percentage of CE cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	100%	100%	100%	100%	99%	100%	99%	99%
New FY 2014 Outcome Measure	Percentage of Cyber defendants whose cases were favorably resolved	N/A	N/A	N/A	NA	90%	NA[2]	90%	90%

[1] 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.

[2] NSD cannot report an actual for this measure because no cyber cases were resolved during FY 2014.

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 four Objectives:

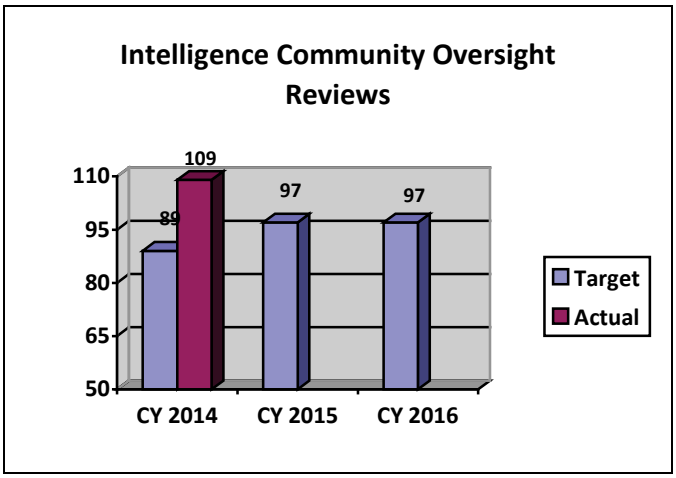
1.1 Prevent, disrupt, and defeat terrorist operations before they occur by integrating intelligence and law enforcement efforts to achieve a coordinated response to terrorist threats
1.2 Prosecute those involved in terrorist acts
1.3 Investigate and prosecute espionage activity against the U.S., strengthen partnerships with potential targets of intelligence intrusions, and proactively prevent insider threats
1.4 Combat cyber-based threats and attacks through the use of all available tools, strong public-private partnerships, and the investigation and prosecution of cyber threat actors

Based on these four objectives, performance resources are allocated to four program activities: Intelligence, Counterterrorism, Counterespionage, and Cyber Security

A. Performance Plan and Report for Outcomes

Intelligence Performance Report

Measure: Intelligence Community Oversight Reviews
CY 2014 Target: 89
CY 2014 Actual: 109
CY 2015 Target: 97
CY 2016 Target: 97
Discussion: The CY 2016 target is an increase over previous targets. The work in this area is expected increase in future years due to the expansion of current oversight programs and the development and implementation of new oversight programs, and anticipated new oversight and reporting requirements.



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.

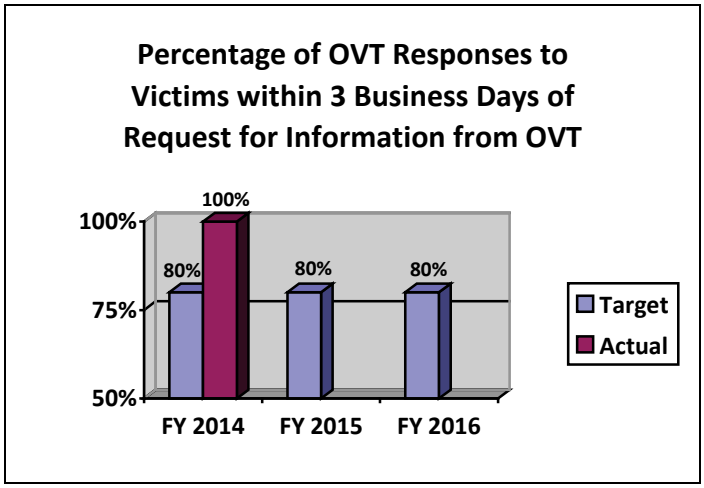
Data Collection and Storage: The information collected during each review is compiled into a report, which is then provided to the reviewed Agency. Generally, the information collected during each review, as well as the review reports, are stored on a classified database. However, some of the data collected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

Counterterrorism Performance Report

Measure: Percentage of OVT Responses to Victims within 3 Business Days of Victim Request for Information from OVT
FY 2014 Target: 80%
FY 2014 Actual: 100%
FY 2015 Target: 80%
FY 2016 Target: 80%
Discussion: The FY 2016 target is consistent with previous years. Additional personnel resources could allow OVT to improve efficiency regarding responses to victims.



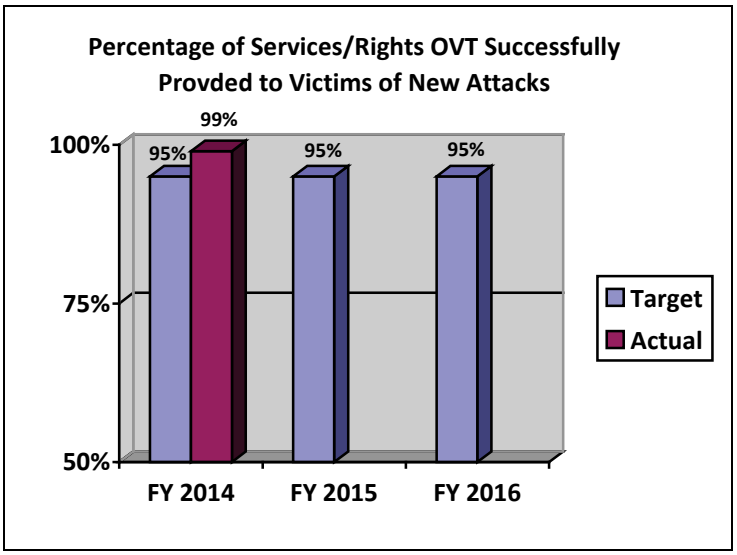
Data Definition: Victims: American citizens who are the victims of terrorism outside the borders of the U.S. This measure reflects OVT's efficiency in providing information to victims after they have contacted OVT.

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

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

Data Limitations: None.

Measure: Percentage of Services/Rights OVT Successfully Provided to Victims of New Attacks
FY 2014 Target: 95%
FY 2014 Actual: 99%
FY 2015 Target: 95%
FY 2016 Target: 95%
Discussion: The FY 2016 target is consistent with previous fiscal years. Additional personnel resources could allow OVT to improve upon its ability to successfully provide victims of new attacks with services/rights.



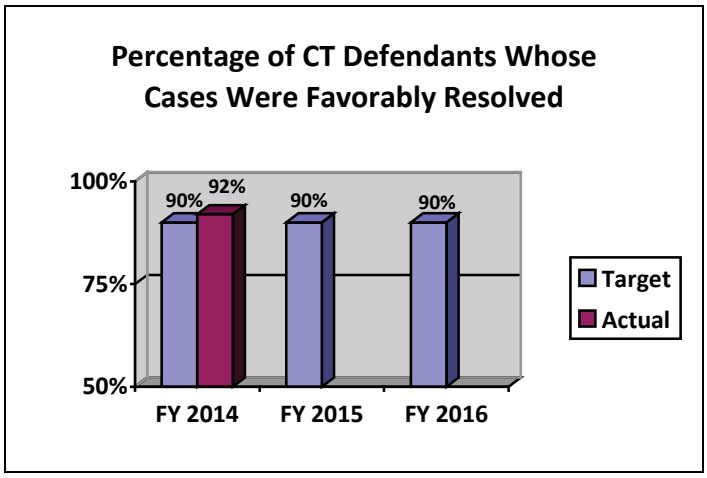
Data Definition: This measure counts the percentage of services/rights OVT provided during the fiscal year that are successfully resolved through the provision of a set group of services. OVT monitors only new attacks that occurred during the fiscal year. Most referrals come from the FBI's Office for Victim Assistance, which will inform OVT when a foreign attack has U.S. victims and the FBI is opening an investigation. Another source for information is CTS, which will inform OVT about foreign and domestic terrorism trials with U.S. victims. In some situations, referrals may come from the State Department, media, or other victims.

Data Collection and Storage: For each new attack identified to OVT, OVT creates a paper file to document OVT efforts. The file contains a checklist of services that OVT can either provide or refer to another agency to provide, or which cannot be provided for a legitimate reason (e.g., it would involve divulging National Security information or information pertaining to a criminal justice proceeding that is ongoing at the time). On a quarterly basis, OVT analyzes and reviews the paper files to determine whether the checklist services have been successfully addressed as indicated in the previous sentence. The performance measure is the percentage of services OVT successfully provided during the fiscal year.

Data Validation and Verification: OVT reviews the paper files on a quarterly basis. The information in the paper files is then loaded into OVT's automated Victim/Attack Tracking Tool so the information can be easily accessed.

Data Limitations: Some criminal justice proceedings and OVT support efforts will take place over several years, but OVT's efforts will only be reported in the year in which the attack occurred to avoid duplication.

Measure: Percentage of CT Defendants Whose Cases Were Favorably Resolved
FY 2014 Target: 90%
FY 2014 Actual: 92%
FY 2015 Target: 90%
FY 2016 Target: 90%
Discussion: The FY 2016 target is consistent with previous fiscal years. Among the strategies that NSD will pursue in this area are consulting, advising, and collaborating with prosecutors nationwide on international and domestic terrorism prosecutions.



Data Definition: Defendants whose cases were favorably resolved include those defendants whose cases were 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 PROSECUTIONS:

Boston Marathon Bombings – On April 15, 2013, two near-simultaneous explosions occurred on Boylston Street, near hundreds of spectators along the Boston Marathon's final stretch. Dzhokhar Tsarnaev was apprehended following an extensive manhunt the next day. The investigation into the bombings continues. On July 10, 2013, Dzhokhar Tsarnaev was arraigned on a 30-count indictment filed on June 27, 2013, charging him with use of a weapon of mass destruction conspiracy, bombing a place of public use and conspiracy, malicious destruction of property and conspiracy, use of a firearm during and in relation to a crime of violence, use of a firearm during and in relation to a crime of violence causing death, carjacking resulting in

serious bodily injury, and interference with commerce by threats or violence. On January 30, 2014, the Attorney General announced that prosecutors would pursue the death penalty against Tsarnaev. Jury selection commenced January 5, 2015.

In connection with the investigation of the Boston Marathon bombing, on August 8, 2013, in the District of Massachusetts, an indictment was returned charging Dias Kadyrbayev and Azamat Tazhayakov with conspiracy to obstruct justice and obstruction of justice. Kadyrbayev, Tazhayakov, and a third friend, Robel Phillipos, are accused of going into Dzhokhar's dorm room at his suggestion and removing his black backpack, some fireworks, and his computer in an attempt to protect Dzhokhar, whom they then believed to be one of the bombers. To conceal evidence of the crime, Kadyrbayev and Tazhayakov are alleged to have thrown the backpack and its contents into a dumpster outside of the apartment that Kadyrbayev and Tazhayakov shared. The backpack was found in a landfill on April 26, 2013. On two occasions, during the investigation, Phillipos lied to the FBI about his involvement saying he never went to the dorm room.

On September 13, 2013, Tazhayakov, Kadyrbayev, and Phillipos were arraigned on the superseding indictment which was filed against them on August 29, 2013. The superseding indictment charged Kadyrbayev and Tazhayakov with conspiracy to obstruct justice, in violation of 18 U.S.C. § 371, and obstruction of justice, in violation of 18 U.S.C. § 1519. The grand jury charged Phillipos with two counts of making false statements, in violation of 18 U.S.C. § 1001.

On July 21, 2014, a jury found Tazhayakov guilty of conspiracy to obstruct justice, in violation of 18 U.S.C. § 371, and obstruction of justice, in violation of 18 U.S.C. § 1519. On August 21, 2014, Kadyrbayev pled guilty to conspiracy to obstruct justice, in violation of 18 U.S.C. § 371, and obstruction of justice, in violation of 18 U.S.C. § 1519. Pursuant to Fed. R. Crim. P. 11(c)(1)(C), the parties agreed that his period of incarceration would not exceed seven years. The sentencing dates for Tazhayakov and Kadyrbayev have been suspended pending the United States Supreme Court decision in *U.S. v. Yates*. On October 28, 2014, in the District of Massachusetts, the jury found Robel Phillipos guilty of both counts of making false statements, in violation of 18 U.S.C. § 1001. Sentencing is scheduled for January 29, 2015.

<u>*U.S. v. Fazliddin Kurbanov*</u> – On May 16, 2013, Fazliddin Kurbanov, an Uzbekistan national residing in the U.S., was indicted by a grand jury in Boise, Idaho, on three charges, including conspiracy to provide material support to a designated Foreign Terrorist Organization; conspiracy to provide material support to terrorists; and possession of an unregistered firearm. On the same day, Kurbanov was also indicted by a grand jury in the District of Utah charging him with one count of distribution of information relating to explosives, destructive devices, and weapons of mass destruction. The Idaho indictment alleges that between August 2012 and May 2013, Kurbanov knowingly conspired with unnamed co-conspirators to provide material support and resources to the Islamic Movement of Uzbekistan, a designated foreign terrorist organization. The indictment also alleges that the material support and resources included himself, computer software, and money. In count two, the indictment further alleges that the defendant conspired to provide material support and resources, including himself, to terrorists

knowing that the material support was to be used in preparation for and in carrying out an offense involving the use of a weapon of mass destruction. On December 2, 2014, in the District of Idaho, Fazliddin Kurbanov was arraigned on a superseding indictment. On November 14, 2014, a superseding indictment was returned charging him with two additional counts: one count of attempting to provide material support to a designated foreign terrorist Organization (the Islamic Movement of Uzbekistan), in violation of 18 U.S.C. § 2339B; and one count of attempting to provide material support to terrorists, in violation of 18 U.S.C. § 2339A. Trial in Idaho is scheduled for May 4, 2015.

U.S. v. Sulaiman Abu Ghayth – From at least May 2001 until approximately 2002, Sulaiman Abu Ghayth served alongside Usama Bin Laden, appearing with Bin Laden and his then-deputy Ayman al-Zawahiri, speaking on behalf of the terrorist organization and in support of its mission. Among many other things, after the September 11 terrorist attacks, Abu Ghayth delivered a speech in which he addressed the then-U.S. Secretary of State and warned that "the storms shall not stop, especially the Airplanes Storm," and advised Muslims, children, and opponents of the United States "not to board any aircraft and not to live in high rises." On February 28, 2013, at an overseas location, Abu Ghayth was arrested on a complaint filed in the Southern District of New York charging him with conspiring to kill United States nationals. A superseding indictment was filed on December 20, 2013, charging Abu Ghayth with the additional crimes of conspiring to provide, and providing, material support to terrorists. On March 27, 2014, Abu Ghayth was found guilty of all charges after a three-week trial. On September 23, 2014, Abu Ghayth was sentenced to life in prison.

U.S. v. Hage, et al. – On October 15, 2013, in the Southern District of New York, Anas al Liby (a/k/a Nazih al Raghie) was arraigned after his capture by U.S. military personnel in Libya on October 5, 2013. Al Liby is charged in a tenth superseding indictment that was returned by a federal grand jury in the Southern District of New York on March 12, 2001. He is indicted for his role in al Qaeda's broad conspiracy during the 1990s to kill U.S. nationals throughout the world, which culminated in the near-simultaneous bombings of the U.S. Embassies in Tanzania and Kenya in August 1998. Over 200 people died in those bombings. The superseding indictment charges al Liby with conspiracy to kill U.S. nationals; conspiracy to murder; conspiracy to destroy U.S. property; and conspiracy to attack national defense utilities. Throughout the 1990s, al Liby is alleged to have been closely associated with several senior al Qaeda leaders and to have acted as Usama bin Laden's personal bodyguard at one point. In addition, al Liby furthered al Qaeda's goals by serving as a document forger and a computer expert for the group. Stemming from this broad conspiracy, several co-conspirators of al Liby's have been convicted over the years in federal court in the Southern District of New York. In May 2001, a jury found Wadih El Hage, Mohammed Sadeek Odeh, Mohamed Rashed Daoud Al-'Owhali, and Khalfan Khamis Mohamed guilty for their roles in the al Qaeda conspiracies that culminated in the 1998 East Africa Embassy bombings. All four were sentenced to life in prison. In November 2010, Ahmed Khalfan Ghailani similarly was convicted of conspiring to destroy buildings and property of the United States and was later sentenced to life in prison. Al Liby was set to stand trial on January 12, 2015, but passed away January 2, 2015 while in custody. Al Liby had two co-defendants: Khaled al Fawwaz and Adel Bary. Adel Bary pleaded

guilty on September 19, 2014, and is to be sentenced on January 16, 2015. The trial of Fawwaz is set to begin on January 20, 2015.

U.S. v. Abu Hamza al-Masri – On, May 19, 2014, in the Southern District of New York, Mustafa Kamel Mustafa, a/k/a Abu Hamza al-Masri, was convicted by a jury on 11 counts related to his involvement in the hostage taking of tourists in Yemen in 1998, attempting to set up a jihad training camp outside Bly, Oregon, and providing material support to al Qaeda in Afghanistan. Trial commenced on April 14, 2014. The indictment also charged two co-conspirators, Oussama Kassir and Haroon Aswat. Kassir was convicted in federal court of various terrorism offenses in 2009, including his participation in efforts to establish the Bly terrorist training camp, and was sentenced in 2009 to life in prison. Aswat is in custody in the United Kingdom, and the U.S. has sought his extradition. Mustafa was sentenced on January 9, 2015, to life in prison.

U.S. v. Babafemi – On April 27, 2014, Lawal Olaniyi Babafemi, a Nigerian national, pleaded guilty to providing and conspiring to provide material support to Al Qaeda in the Arabian Peninsula (AQAP). Between approximately January 2010 and August 2011, Babafemi traveled twice from Nigeria to Yemen to meet and train with leaders of AQAP. Babafemi assisted in AQAP's English-language media operations, which included the publication of the magazine "Inspire." At the direction of the now-deceased senior AQAP commander Anwar al-Aulaqi, Babafemi was provided with the equivalent of almost $9,000 in cash by AQAP leadership to recruit other English-speakers from Nigeria to join the group. While in Yemen, Babafemi also received weapons training from AQAP. At sentencing, scheduled for January 22, 2015, Babafemi faces a maximum of 30 years in prison.

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, was convicted of multiple federal terrorism offenses in the Eastern District of New York. Evidence at trial demonstrated that the defendant and his accomplices, Najibullah Zazi and Zarein Ahmedzay, traveled to Afghanistan and Pakistan in 2008, where they met senior al-Qaeda leaders and received al Qaeda training. Upon their return to the United States, Medunjanin, Zazi, and Ahmedzay met and agreed to carry out suicide bombings in New York City. They came within days of executing a plot to conduct coordinated suicide bombings in the New York City subway system in September 2009, as directed by senior al Qaeda leaders in Pakistan. When the plot was foiled, Medunjanin attempted to commit a terrorist attack by crashing his car on the Whitestone Expressway in New York in an effort to kill himself and others. To date, seven defendants, including Medunjanin, Zazi, Amanullah Zazi and Ahmedzay, have been convicted in connection with the New York City bombing plot and related charges. Medunjanin was sentenced to life imprisonment, and Amanullah Zazi was sentenced to 40 months' imprisonment with a judicial order of removal to Pakistan upon completion of his sentence. On May 20, 2014, the Court of Appeals for the Second Circuit affirmed the conviction of Adis Medunjanin. Najibullah Zazi and Zarein Ahmedzay, who each face a maximum sentence of life imprisonment, have not yet been sentenced. On January 3, 2013, Abid Naseer was extradited from the United Kingdom to the United States to become the eighth defendant to face charges in

Brooklyn federal court related to this plot. He faces a maximum sentence of life imprisonment if convicted of all counts. Trial is scheduled for January 26, 2015.

SYRIAN TRAVELER CASES:

There have been a number of prosecutions in the last year involving American citizens attempting to travel to Syria to join the conflict there. A sample of those cases includes:

U.S. v. Teusant – On March 26, 2014, in the Eastern District of California, a grand jury returned a one-count indictment charging Nicholas Teausant, age 20, of Acampo, California, with attempting to provide material support to a foreign terrorist organization in violation of 18 U.S.C. § 2339B. The indictment followed Teausant's arrest on a federal criminal complaint after he was intercepted by law enforcement while traveling in Blaine, Washington, near the Canadian border. The complaint alleged that Teausant intended to travel to Syria to work under the direction and control of al-Qa'ida in Iraq under its alias, the Islamic State of Iraq and Syria, knowing it to be a foreign terrorist organization, and knowing that the organization had engaged in, and was engaging in, terrorist activity and terrorism.

U.S. v. Jordan et al. – April 1, 2014, in the Eastern District of North Carolina, a grand jury returned a one-count indictment charging Avin Marsalis Brown and Akbar Jihad Jordan with conspiracy to travel overseas to provide material support for terrorists, in violation of 18 U.S.C. § 2339A. Brown and Jordan were originally arrested on March 19, 2014, and charged by complaint the next day. The complaint alleged that Jordan and Brown conspired to travel overseas to engage in violent jihad against "kuffars" or non-Muslims. Jordan and Brown, on numerous occasions, discussed traveling to Yemen, Syria, and other locations to fight, and undertook concrete steps to further this purpose. Specifically, they contacted other westerners who were fighting in Syria with Islamist groups, researched the safest modes of travel to countries to conduct violent jihad, and undertook efforts to obtain travel documents. Jordan, who possessed an AK-47 and other weapons, counseled Brown in the proper use of firearms and practiced fighting techniques and procedures with him. Brown obtained a United States Passport and purchased a ticket to fly to Turkey with the intent of crossing the border into Syria. He was arrested on March 19, 2014, at the Raleigh-Durham International Airport prior to the scheduled departure of his flight. Jordan had a passport application appointment for March 21, 2014, but was arrested prior to the appointment. October 16, 2014, Jordan entered a plea of guilty. Sentencing will be scheduled for March 2015.

U.S. v. Wolfe - Beginning in early 2013, Michael Todd Wolfe began expressing a committed interest in traveling overseas with the intent to participate in a violent form of jihad. Specifically, Wolfe contemplated traveling to Syria to join ISIS to engage in terrorist acts. Wolfe took a variety of steps to reach his violent jihadi goal. He discussed, researched, and ultimately made plans to travel from the United States to Turkey by way of Copenhagen, Denmark. Wolfe, along with an FBI employee operating in an undercover capacity, selected Turkey as his destination because he knew that: (1) Turkey shares a border with Syria; and (2) the barriers to entering Syria from Turkey to join the conflict there are minimal. Wolfe was

arrested at the Houston International Airport attempting to board an international flight to Copenhagen. On June 27, 2014, in the Western District of Texas, Wolfe waived indictment and pleaded guilty to a one count information charging him with an attempt to provide material support to a designated foreign terrorist organization, the Islamic State of Iraq and Sham/Syria ("ISIS"), in violation of 18 U.S.C. § 2339B. Previously, on June 18, 2014, Michael Wolfe was indicted with one count of attempting to provide material support and resources to terrorists, in violation of 18 U.S.C. § 2339A. The predicate offense for that violation was conspiracy to murder, kidnap, or maim persons outside the United States, in violation of 18 U.S.C. § 956. Wolfe is scheduled to be sentenced on January 30, 2015.

WMD/BIOLOGICAL TOXIN/DOMESTIC TERRORISM CASES:

There has also been an increase in domestic terrorism cases and those involving biological toxins, such as ricin, and weapons of mass destruction in the past year. Below is a sampling of these cases:

U.S. v. James Everett Dutschke – On May 19, 2014, James Everett Dutschke was sentenced in federal district court in Oxford, Mississippi to 300 months' imprisonment for his role in developing and possessing the biological agent ricin and subsequently mailing ricin-laced threatening letters to public figures, including the President of the United States. Dutschke, of Tupelo, Mississippi, developed a scheme to retaliate and frame another individual by mailing threatening letters. As part of the scheme, he used the internet to research how to produce and use ricin, a biological agent and toxin. Dutschke purchased castor beans or seeds, a key ingredient for the manufacture and production of ricin, from vendors via eBay and PayPal. Additionally, he purchased other tools and implements such as latex gloves, grinders, and masks from area vendors to develop the toxin. Dutschke then produced ricin for use as a weapon, drafted the letters and mailed them using the U.S. Mail system. Three of the letters were mailed to the President of the United States, a U.S. Senator, and a Mississippi Justice Court Judge. He pleaded guilty in January 2014 to knowingly developing, producing, stockpiling, transferring, acquiring, retaining and possessing a biological agent, toxin, and delivery system as a weapon.

U.S. v. Shannon Richardson – On December 10, 2013, in the Eastern District of Texas, Shannon Richardson pleaded guilty to an Information charging her with possession of a toxin for use as a weapon, in violation of 18 U.S.C. § 175(a). On May 20, 2013, Richardson is alleged to have mailed three letters containing the toxin ricin. The letters were sent to President Barack Obama and Mark Glaze in Washington, D.C. and to Mayor Michael Bloomberg in New York City. On July 16, 2014, Richardson was sentenced to 18 years' imprisonment.

U.S. v. Buquet – On June 19, 2013, in the Eastern District of Washington, a federal grand jury returned a three-count superseding indictment charging Matthew Ryan Buquet with Weapons of Mass Destruction (WMD) and threat offenses related to ricin-tainted letters sent in May 2013 to President Obama, a federal judge, and others. Buquet was previously charged in May 2013 with a single violation of 18 U.S.C. § 876(c) for a ricin-tainted letter sent to a senior district judge in

Spokane. The superseding indictment adds charges that Buquet possessed ricin, a biological agent, for use as a weapon, in violation of 18 U.S.C. § 175(a), and that Buquet mailed a threatening communication to the President of the United States, in violation of 18 U.S.C. § 871.

U.S. v. Korff – On August 12, 2014, Korff pleaded guilty to an information charging him with five counts of developing and transferring a biological toxin (abrin), in violation of 18 U.S.C. § 175(a); five counts of exporting a biological toxin, in violation of 18 U.S.C. § 554(a); and one count of conspiring to kill a person in a foreign country, in violation of 18 U.S.C. § 956. Korff was arrested on January 18, 2014, outside Ft. Myers, Florida, after a joint FBI and DHS (Homeland Security Investigations (HSI)) investigation revealed that Korff was making biological toxins for use as weapons and selling them over the internet. Korff allegedly produced and then sold biological toxins, knowing that the buyers were intending to use them to kill other people. Korff is scheduled to be sentenced on January 12, 2015.

U.S. v. Levenderis - On June 4, 2014, in the Northern District of Ohio, Jeff Boyd Levenderis was convicted by a federal jury on all four-counts of a superseding indictment relating to his possession of ricin for use as a weapon. On November 22, 2011, a federal grand jury returned the superseding indictment alleging that Levenderis: (1) knowingly developed, produced, stockpiled, retained and possessed a biological toxin and delivery system (ricin), for use as a weapon, in violation of 18 U.S.C. § 175(a); (2) knowingly possessed a biological toxin (ricin) of a type or quantity not reasonably justified by peaceful purposes, in violation of 18 U.S.C. § 175(b); and (3) made two material, false statements to the FBI (that the substance was not ricin), both in violation of 18 U.S.C. § 1001. In January of 2011, Robert Coffman, an associate of Levenderis, contacted civilian and military authorities to ask how to safely dispose of ricin. Those authorities contacted the FBI. Coffman told the FBI that he was cleaning a friend's house and the friend, Levenderis, had alerted him that ricin was present in the freezer. Laboratory testing confirmed that the substance in the freezer was a finely powdered form of ricin, capable of killing hundreds of adult humans if even minuscule amounts of the toxin were inhaled or injected. When confronted, Levenderis claimed the substance was ant poison not ricin, before admitting the substance was "weaponized" ricin which he had produced and claimed would use to deter first responders from coming to his rescue in a planned suicide. Since that confession in January 2011, the government has discovered significant evidence that Levenderis, who has been unemployed since the late 90s and relied on his family for financial support, planned to murder his stepfather with the ricin in order to inherit from him. On June 4, 2014, Levenderis was convicted on all four counts of a superseding indictment charging him with possession of hundreds of lethal doses of ricin. On September 29, 2014, Jeff Boyd Levenderis was sentenced to 72 months' imprisonment.

U.S. v. Crump, et al. - On November 14, 2014, in the Northern District of Georgia, Raymond Adams and Samuel Crump were both sentenced to 120 months' imprisonment to be followed by 5 years' supervised release. On January 17, 2014, in the Northern District of Georgia, Samuel Crump and Raymond Adams were found guilty of conspiracy to possess and produce a biological toxin (ricin) and possession of a biological toxin (castor beans) for use as a weapon, both in violation of 18 U.S.C. § 175(a). The Government presented evidence, including

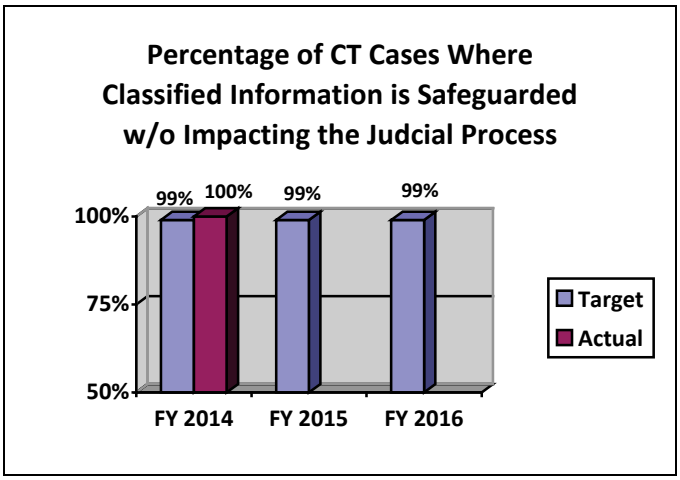
numerous recorded statements of the defendants describing plans to use ricin to "make [federal] buildings toxic" and attack city centers, including Washington, D.C., as well as internet recipes for extracting ricin from the castor beans and the tools necessary to complete the recipe recovered during the search of their properties. In 2010, the FBI identified Crump and Adams during the course of an FBI investigation into members of a covert, anti-government association known as the Militia of Georgia ("MoG"). A confidential human source recorded meetings of MoG members, including Crump and Adams, at which participants discussed means of attacking urban population centers with biological weapons, including ricin. During a search, the FBI recovered more than 500 castor beans from Crump's and Adams's properties, as well as recipes for extracting ricin from castor beans. In addition, the FBI seized 33 mason jars from Adams's residence which contained a brown, liquid substance that has since tested positive for the presence of ricin. In November 2011, Crump and Adams were indicted, along with two other MoG members, Frederick Thomas and Emory Dan Roberts. Thomas and Roberts were charged with Conspiring to Possess an Unregistered Explosive Device and Possession of an Unregistered Silencer, in violation of 18 U.S.C. § 371 and 26 U.S.C. §§ 5861(d), 5871, 5841 and 5845(a)(7). On April 10, 2012, Thomas and Roberts pled guilty and on August 22, 2012, they were sentenced to 60 months' incarceration. Crump and Adams were charged with Conspiracy to Possess and Produce a Biological Toxin, as well as Attempted Production of a Biological Toxin, in violation of 18 U.S.C. §§ 175(a) and 2. A superseding indictment filed on December 10, 2013 charged Crump and Adams with Attempted Possession and Conspiracy to Possess and Produce a Biological Toxin for Use as a Weapon, in violation of 18 U.S.C. § 175(a), as well as Possession of a Biological Toxin for Use as a Weapon, in violation of 18 U.S.C. §§ 175(a) and 2.

U.S. v. Loewen - On December 13, 2013, Terry Lee Loewen was arrested while attempting to access the tarmac of the Wichita Mid-Continent Airport with what he believed to be a functional vehicle-borne improvised explosive device (VBIED). Until that time, Loewen was an avionics technician at the Wichita Mid-Continent Airport. Over previous months, he had unknowingly been speaking with FBI undercover agents as he expressed a desire and developed a plan to utilize his airport access to conduct a terrorist plot. He surveilled the Wichita airport's access points and security, and helped build and wire the VBIED. Loewen planned, with the help of an FBI employee he believed to be a member of Al Qaeda in the Arabian Peninsula (AQAP), to detonate the bomb by the airport terminal in the early morning in order to maximize casualties. In a letter left for a family member, he said people would rightfully call him a "terrorist" and that it was true the attack had been planned for "maximum carnage + death." On December 18, 2013, Loewen was indicted with one count of attempted use of a weapon of mass destruction, in violation of 18 U.S.C. § 2332a, one count of attempted destruction of property by an explosive device, in violation of 18 U.S.C. § 844(i), and one count of attempted material support of a designated foreign terrorist organization, AQAP, in violation of 18 U.S.C. § 2339B. The case is currently in pretrial litigation with trial to be scheduled in 2015.

U.S. v. Osmakac - On June 10, 2014, in the Middle District of Florida, a jury found Sami Osmakac guilty on both counts of a February 2012 indictment which charged him with attempting to use a weapon of mass destruction, in violation of 18 U.S.C. § 2332a, and possessing an unregistered machine gun, in violation of 26 U.S.C. § 5861. The jury returned the

guilty verdict after approximately four and-a-half hours of deliberation. At trial, the defense argued that the government entrapped Osmakac, a Yugoslavian native and naturalized United States citizen, and that he was highly susceptible to inducement due to mental illness. The government adduced evidence that Osmakac intended to remotely explode a bomb concealed in a vehicle in front of a Tampa-area bar, move to a second location and take hostages with the intent of demanding the release of Muslim prisoners, and then explode a suicide vest when law enforcement attempted to arrest him. The government introduced evidence that beginning in September 2011, the defendant communicated with an FBI confidential source (CS) about his intention to commit a violent attack in the United States. Specifically, Osmakac told the CS that he intended to use explosive devices and firearms to conduct an attack in the Tampa, Florida. An FBI undercover agent (UC) testified that he meet with Osmakac three times to discuss the purchase of a fully automatic AK-47, grenades, a suicide belt or vest, and a bomb that could be placed in the trunk of a car. Osmakac identified a number of potential targets to the UC in Tampa, Florida. On January 7, 2012, FBI agents arrested Osmakac after he took possession of purported explosive devices and firearms. Shortly prior to his arrest, Osmakac also made a video of himself explaining his motives for carrying out the attack that he had planned. The government argued that based on Osmakac's extensive preparations and his own statements, it was clear that Osmakac's goal was to kill United States citizens and to create a major disruption in the Tampa Bay area. On November 5, 2014, Sami Osmakac was sentenced to 40 years' imprisonment and a lifetime of supervised release.

Measure: **Percentage of CT Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2014 Target: 99%
FY 2014 Actual: 100%
FY 2015 Target: 99%
FY 2016 Target: 99%
Discussion: The FY 2016 target is consistent with previous fiscal years. NSD will support successful prosecutions by providing advice and assistance on the use of classified evidence through the application of the Classified Information Procedures Act (CIPA).



Data Definition: Classified information - information that has been determined by the U.S. 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.

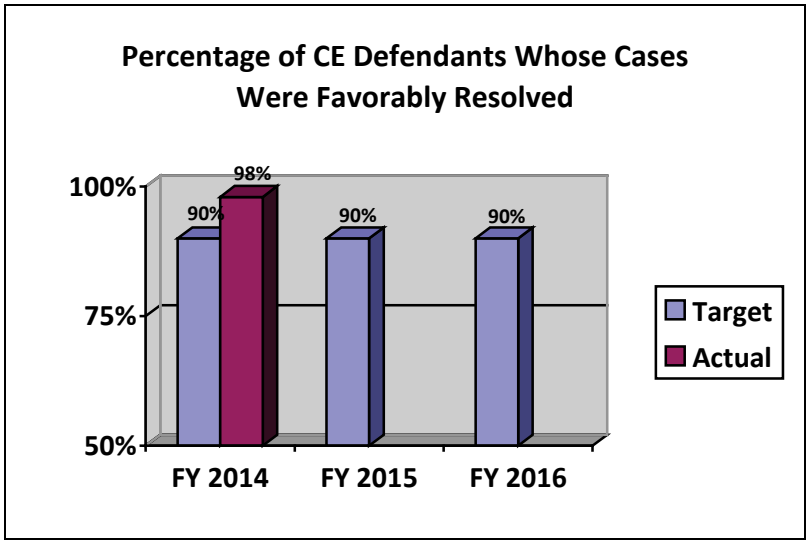
Data Collection and Storage: Data collection and storage is manual.

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 2014 Target: 90%
FY 2014 Actual: 98%
FY 2015 Target: 90%
FY 2016 Target: 90%
Discussion: The FY 2016 target is consistent with previous fiscal years. Among the strategies that NSD will pursue in this area are: supporting and supervising the prosecution of espionage and related cases through coordinated efforts and close collaboration with Department leadership, the FBI, the IC, and the 94 USAOs; assisting in and overseeing the expansion of investigations and prosecutions into the unlawful export of military and strategic commodities and technology; and coordinating and providing advice in connection with cases involving the unauthorized disclosure of classified information.



Data Definition: Defendants whose cases were favorably resolved include those defendants whose cases were 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 ensure that records are current and accurate.

Data Limitations: Reporting lags.

Select Recent Counterespionage and Counterproliferation

State Advisor Sentenced for Disclosing National Defense Information / U.S. v. Kim – On April 2, 2014, Stephen Jin-Woo Kim, a former federal contract employee, was sentenced to 13 months in prison for the unauthorized disclosure of national defense information. Kim pleaded guilty on February 7, 2014, in the District of Columbia to one count of making an unauthorized disclosure of national defense information. Kim was a Lawrence Livermore National Laboratory employee on detail to the State Department's Bureau of Verification, Compliance, and Implementation (VCI) at the time of the disclosure. At the time, Kim worked as a senior advisor to the assistant secretary of state for VCI. According to court documents, on June 11, 2009, Kim knowingly and willfully disclosed to a reporter top secret/sensitive compartmented information (TS/SCI) relating to the national defense. The information concerned the military capabilities and preparedness of North Korea and was contained in an intelligence report classified at the TS/SCI level that Kim accessed on a classified computer database. Within hours of the disclosure, a news organization published an article on the Internet that included the TS/SCI national defense information that Kim had disclosed.

Defense Contractor Sentenced for Disclosing National Defense Information / U.S. v. Bishop – On March 13, 2014, in the District of Hawaii, Benjamin Pierce Bishop, a defense contractor and former Lt. Colonel in the U.S. Army, pleaded guilty to willfully communicating classified national defense information to a person not authorized to receive it and willfully retaining classified national defense information. Bishop was arrested on March 15, 2013, on charges that he communicated classified information to a Chinese woman with whom he had a romantic relationship. According to the criminal complaint, during Bishop's relationship with the woman (further identified as a graduate student in the United States on a J1 Visa), Bishop communicated classified information concerning U.S. national defense systems and removed classified information from his work space at U.S. Pacific Command which he then kept at his Honolulu area residence. In his plea agreement filed with the court, Bishop admitted that he willfully communicated secret U.S. national defense information related to joint training and planning sessions between the United States and the Republic of Korea. Bishop also admitted to willfully retaining multiple classified documents at his residence related to U.S. national defense. On September 17, 2014, Bishop was sentenced to 87 months in prison.

DuPont Trade Secrets to China / U.S. v. Liew et al. – This case is one of the largest economic espionage cases in history. According to a March 2013 second superseding indictment, several former employees with more than 70 combined years of service to DuPont were engaged in the sale of trade secrets to Pangang Group, a state-owned enterprise in the People's Republic of China (PRC). Pangang and its subsidiaries sought information on the production of titanium dioxide, a white pigment used to color paper, plastics, and paint. The PRC government had long sought to encourage entry into titanium dioxide industry, a $12-15 billion annual market of which DuPont has the largest share. Five individuals and five companies were charged in a scheme designed to take DuPont's technology to the PRC and build competing titanium dioxide plants, which would undercut DuPont revenues and business. Three co-conspirators were arrested and one additional co-conspirator pled guilty in the Northern District of California. In

March of 2014, a jury convicted three defendants on all 20 counts, including 18 U.S.C. § 1831 (economic espionage) and 18 U.S.C. § 1832 (theft of trade secrets), which marks the first jury conviction for economic espionage. Defendant Walter Liew was sentenced to 180 months in prison and ordered to pay $500,000 restitution. Defendant Robert Maegerle was sentenced to 30 months in prison and $367,000 restitution. Corporate defendant USAPTI was sentenced to 5 years of probation and fined $18.9 million.

Industrial Cutting Machines to Iran / U.S. v. Alexander – On January 6, 2014, Mark Mason Alexander, a/k/a Musa Mahmood Ahmed, was sentenced in the Northern District of Georgia to 18 months in prison, followed by three years of supervised release. Alexander was found guilty by a jury on September 26, 2013, of conspiracy to violate the International Emergency Economic Powers Act. According to the charges and other information presented in court, between October 2006 and June 2008, Alexander conspired with two Iranian businessmen to sell Hydrajet water-jet cutting systems to customers in Iran. Hydrajet Technology, located in Dalton, Georgia, manufactured the water-jet cutting systems, which are used for the precision cutting of materials such as steel, aluminum, granite, and glass. In 2007, as part of the conspiracy, Alexander negotiated the sale of two water-jet cutting systems to companies located in the Islamic Republic of Iran. He concealed the true destination of these machines by causing them to be trans-shipped to Iran via Alexander's company in the United Arab Emirates (UAE). Alexander additionally instructed his employees in the UAE to travel to Iran to install the machines and to conduct software training for the Iranians who would operate them.

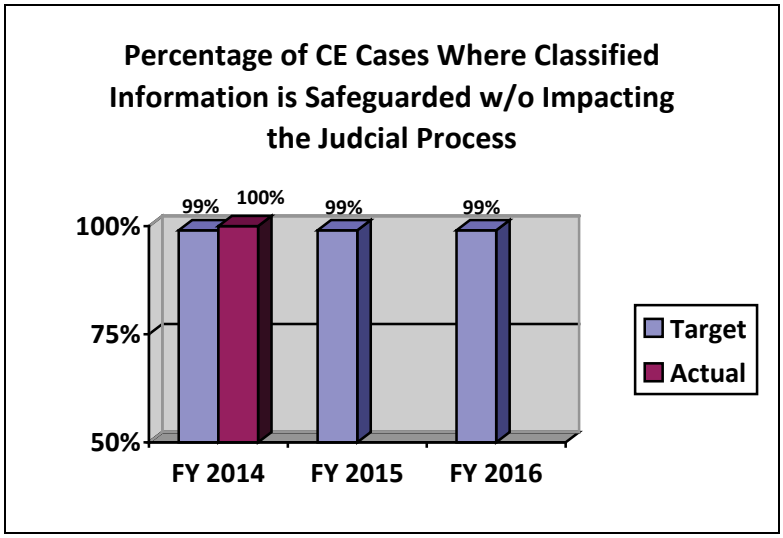
Embargo Violations by Arms Dealer / U.S. v. Chichakli – On December 13, 2013, Richard Ammar Chichakli, an associate of international arms dealer Viktor Bout, was found guilty by a jury in the Southern District of New York of conspiring with Bout and others to violate the International Emergency Economic Powers Act (IEEPA) by attempting to purchase commercial airplanes from American companies, in violation of U.S. sanctions. Chichakli, a citizen of Syria and the United States, was also found guilty of money laundering conspiracy, wire fraud conspiracy, and six counts of wire fraud, in connection with the attempted aircraft purchases. According to evidence at trial and documents previously filed in Manhattan federal court, Chichakli conspired with Bout and others to violate IEEPA by engaging in prohibited business transactions with companies based in the United States. The focus of these transactions was the purchase of commercial airplanes for a company that Bout and Chichakli controlled, and the ferrying of those aircraft to Tajikistan. On December 4, 2014, Chichakli was sentenced to 60 months in prison and ordered to pay $70,000 restitution.

Aerospace-Grade Carbon Fiber to China / U.S. v. Zhang – On December 10, 2013, Ming Suan Zhang, a citizen of the People's Republic of China, was sentenced in the Eastern District of New York to 57 months in prison. Previously, on August 19, 2013, Zhang pleaded guilty to violating the International Emergency Economic Powers Act by attempting to export thousands of pounds of aerospace-grade carbon fiber from the United States to China. Zhang was arrested in the United States after trying to negotiate a deal to acquire the specialized carbon fiber, a high-tech material used frequently in the military, defense, and aerospace industries, and which is therefore

closely regulated by the U.S. Department of Commerce to combat nuclear proliferation and terrorism.

Controlled Microelectronics to Russia / U.S. v. Fishenko et al. – On January 10, 2013, defendants Lyudmila Bagdikian and Viktoria Klebanova pleaded guilty in the Eastern District of New York (EDNY) to their roles in illegally exporting goods from the United States to Russian end users. On October 3, 2012, an indictment was unsealed in EDNY charging 11 members of a Russian procurement network operating in the United States and Russia, as well as a Houston-based export company, Arc Electronics Inc., and a Moscow-based procurement firm, Apex System LLC, with illegally exporting high-tech microelectronics from the United States to Russian military and intelligence agencies. Alexander Fishenko, an owner and executive of both the American and Russian companies, is also charged with operating as an unregistered agent of the Russian government inside the United States by illegally procuring the microelectronics on behalf of the Russian government. As alleged in the indictment, beginning in October 2008, Fishenko and the other defendants engaged in a conspiracy to obtain advanced microelectronics from manufacturers and suppliers located in the United States and to export those high-tech goods to Russia, while evading the U.S. export licensing system. The microelectronics allegedly exported to Russia are subject to U.S. controls due to their potential use in a wide range of military systems, including radar and surveillance systems, weapons guidance systems, and detonation triggers.

Measure: **Percentage of CE Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2014 Target: 99%
FY 2014 Actual: 100%
FY 2015 Target: 99%
FY 2016 Target: 99%
Discussion: The FY 2016 target is consistent with previous fiscal years. NSD will support successful prosecutions by providing advice and assistance on the use of classified evidence through the application of the Classified Information Procedures Act (CIPA).



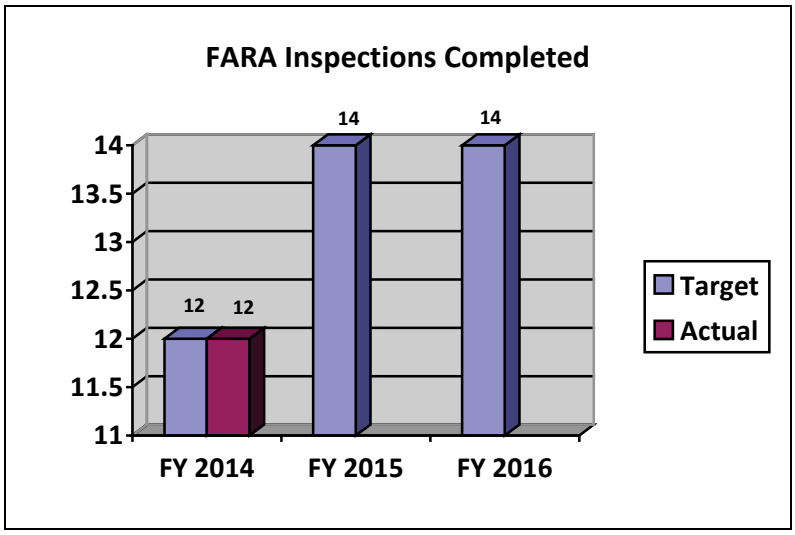
Data Definition: Classified information - information that has been determined by the United State Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data as defined by the 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 ensure that records are current and accurate.

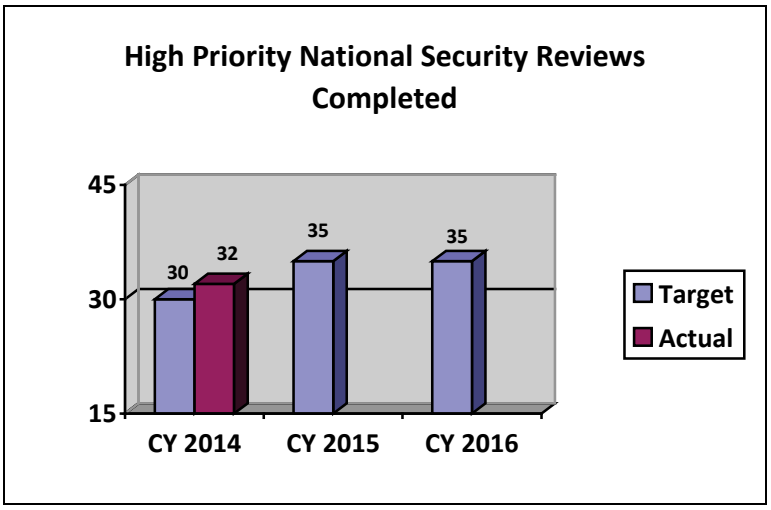
Data Limitations: Reporting lags.

Measure: FARA Inspections Completed
FY 2014 Target: 12
FY 2014 Actual: 12
FY 2015 Target: 14
FY 2016 Target: 14
Discussion: The FY 2016 target is consistent with previous fiscal years. Performing targeted inspections allows the FARA Unit to more effectively enforce compliance among registrants under the Foreign Agents Registration Act of 1938 (FARA).



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 2014 Target: 30
CY 2014 Actual: 32
CY 2015 Target: 35
CY 2016 Target: 35
Discussion: The FY 2016 target is consistent with previous fiscal years. To address potential national security concerns with foreign investment, NSD will continue to work with its partners to perform these high priority reviews.



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.

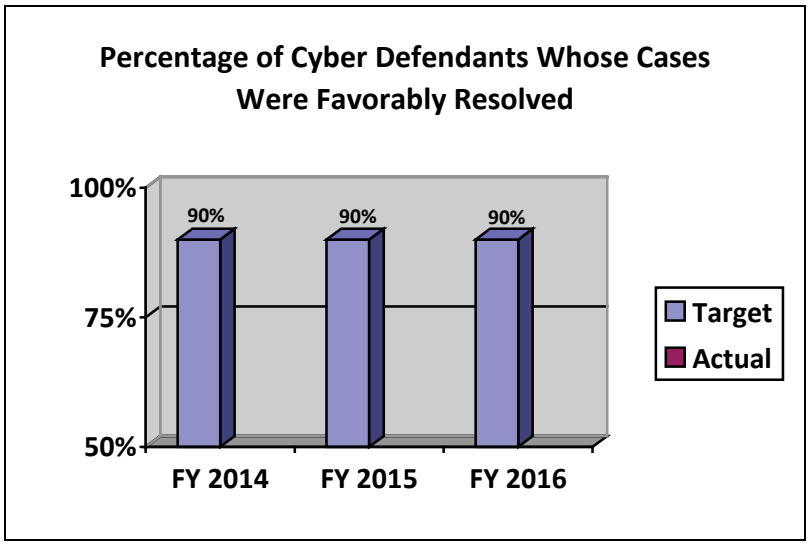
Data Collection and Storage: Data is collected manually and stored in generic files; however management is reviewing the possibility of utilizing a modified automated tracking system.

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.

Cyber Performance Report

Measure: Percentage of Cyber Defendants Whose Cases Were Favorably Resolved
FY 2014 Target: 90%
FY 2014 Actual: NA – No cyber cases were resolved in FY 2014
FY 2015 Target: 90%
FY 2016 Target: 90%
Discussion: The FY 2016 target is consistent with previous fiscal years. Among the strategies that NSD will pursue in this area are: recruit, hire, and train additional cyber-skilled professionals.



Data Definition: Defendants whose cases were favorably resolved include those defendants whose cases resulted in court judgments favorable to the government.

Data Collection and Storage: Data will be collected manually and stored in internal files.

Data Validation and Verification: Data validation and verification is accomplished via quarterly reviews done by CTS and CES.

Data Limitations: There are no identified data limitations at this time.

Select Recent National Security Cyber Prosecutions

People's Liberation Army Officers Indicted for Computer Intrusions, Theft of Trade Secrets, and Economic Espionage / U.S. v. Wang Dong, et al. – On May 1, 2014, five members of China's People's Liberation Army (PLA) were indicted by a federal grand jury in the Western District of Pennsylvania on 31 counts related to computer fraud and abuse, aggravated identity theft, economic espionage, and trade secret theft affecting five victims in the nuclear and solar power and metals industries. This case marks the first charges against state-sponsored military actors for economic espionage. The Indictment alleges that the five PLA members conspired to hack into the U.S. victims "for the purpose of commercial advantage and private financial gain," and that the stolen information would have been particularly beneficial to the victims' Chinese competitors at the time such information was stolen, including Chinese companies adverse to the victims in then-ongoing international trade disputes.

U.S. Charges Chinese National for Participating in Hacking Scheme to Steal U.S. Military Technology / U.S. v. Su Bin - On June 28, 2014, Su Bin was arrested in Canada based on a complaint filed in the Central District of California (CDCA) alleging that he worked with two unnamed co-conspirators to steal U.S. military technology. The complaint described how Su worked with one of the co-conspirators to seek files that had value and in one instance

information that could be sold to a state-owned Chinese aviation company, and it alleged that Su and the other co-conspirators sought and obtained data related to the C-17, F-35, F-22 and at least thirty other military technologies or projects. Subsequently, Su was indicted in the CDCA for unauthorized access to computers, violating the Arms Export Control Act, and conspiring to steal trade secrets. CDCA has formally requested Su's extradition from Canada, and those proceedings are ongoing.

B. Strategies to Accomplish Outcomes

NSD's performance goals support the Department's Strategic Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law. Strategies for accomplishing outcomes within each of the 4 Strategic Objectives are detailed below:

Strategic Objective 1.1 - Prevent, disrupt, and defeat terrorist operations before they occur by integrating intelligence and law enforcement efforts to achieve a coordinated response to terrorist threats

NSD will continue to ensure that the IC is able to make efficient use of foreign intelligence information collection authorities, particularly FISA by representing the U.S. before the FISC. This tool has been critical in protecting against terrorism, espionage, and other national security threats. NSD will also continue to expand its oversight operations within the IC and develop and implement new oversight programs, promote ongoing communication and cooperation with the IC, and advise partners on the use of legal authorities.

Strategic Objective 1.2 - Prosecute those involved in terrorist acts

NSD will promote and oversee a coordinated national counterterrorism enforcement program, through close collaboration with Department leadership, the National Security Branch of the FBI, the IC, and the 94 U.S. Attorneys' Offices (USAOs); develop national strategies for combating emerging and evolving terrorism threats, including the threat of cyber-based terrorism; consult, advise, and collaborate 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); share information with and provide advice to international prosecutors, agents, and investigating magistrates to assist in addressing international threat information and litigation initiatives; and manage 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.

Strategic Objective 1.3 - Investigate and prosecute espionage activity against the U.S., strengthen partnerships with potential targets of intelligence intrusions, and proactively prevent insider threats

Among the strategies that the National Security Division will pursue in this area are: supporting and supervising the investigation and prosecution of espionage and related cases through coordinated efforts and close collaboration with Department leadership, the FBI, the Intelligence Community (IC), and the 94 U.S. Attorney Offices (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, and violations of U.S. economic sanctions; 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 Classified Information Procedures Act; and enforcing the Foreign Agents Registration Act of 1938 and related disclosure statutes.

Strategic Objective 1.4 - Combat cyber-based threats and attacks through the use of all available tools, strong public-private partnerships, and the investigation and prosecution of cyber threat actors

NSD will recruit, hire, and train additional cyber-skilled professionals; prioritize disruption of cyber threats to the national security through the use of the U.S. Government's full range of tools, both law enforcement and intelligence; promote legislative priorities that adequately safeguard national security interests; and invest in information technology that will address cyber vulnerabilities while also keeping the Department at the cutting edge of technology.

C. Priority Goals (Not Applicable)

V. Program Increases

A. Item Name:	**Combating Cyber Threats to National Security**
AG Targeted Priority Options:	Cybersecurity
Strategic Goal:	Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law
Strategic Objective:	Objective 1.4: Combat cyber-based threats and attacks through the use of all available tools, strong public-private partnerships, and the investigation and prosecution of cyber threat actors
Budget Decision Unit(s):	National Security Division
Organizational Program:	Counterespionage Section, Office of Intelligence

Program Increase: Positions 12 Atty 9 FTE 6 Dollars $1,745,231

Description of Item

The NSD requests a total of 12 positions, including 9 attorneys and 3 non-attorneys, to support the growing area of combating cyber threats to national security.

Justification

As predicted in prior year program budget requests, the national security threat to the U.S. is evolving rapidly. As FBI Director Comey noted in a recent speech, "the threat is so dire that cyber security has topped Director of National Intelligence Jim Clapper's list of global threats for the second consecutive year, surpassing both terrorism and espionage—even the threat posed by weapons of mass destruction."[3] Director Clapper has previously assessed that "[t]hreats are more diverse, interconnected, and viral than at any time in history. Attacks, which might involve cyber and financial weapons, can be deniable and unattributable. Destruction can be invisible, latent, and progressive… State and nonstate actors increasingly exploit the Internet to achieve strategic objectives."[4]

[3] James B. Comey, Director of the Federal Bureau of Investigation, remarks delivered to RSA Cyber Security Conference (February 26, 2014), available at http://www.fbi.gov/news/speeches/the-fbi-and-the-private-sector-closing-the-gap-in-cyber-security.

[4] James R. Clapper, Director of National Intelligence, Unclassified Statements on the Worldwide Threat Assessment to the House Permanent Select Committee on Intelligence (April 11, 2013), available at http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20WWTA%20US%20IC%20SFR%20%20HPSCI%2011%20Apr%202013.pdf.

Indeed, a wide range of actors – terrorists, nation states, transnational organized crime groups, and others, may seek to sabotage our critical infrastructure, while foreign intelligence collectors also try to steal our defense secrets or intellectual property. Despite significant investments and concerted efforts by the private sector and government to build more secure and defendable computer networks, the asymmetric threats in cyberspace leave Americans extremely vulnerable both physically and economically. As we have seen, al Qaeda has instructed 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 11th,"[5] and General Keith Alexander, former Director of the National Security Agency, has called cybercrime "the greatest transfer of wealth in history."[6] Indeed, President Obama wrote in July 2012 "[T]he cyber threat to our nation is one of the most serious economic and national security challenges we face,"[7] and it remains that way today.

NSD continues to be 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.

Support of the Department's Strategic Goals

Combating Cyber Threats to National Security is a cross-cutting effort that impacts each objective under DOJ Strategic Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law. Because cyber resources can be used by threat actors as a means of accomplishing terrorism or espionage, NSD's Division-level strategic priorities include a significant focus on combating cyber threats to the national security,[8] and each of its organizational programs are involved in these efforts:

---

[5] "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.

[6] Remarks by General Keith Alexander at the American Enterprise Institute, July 9, 2012, as reported in Foreign Policy online by Josh Rogin, accessible at: http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history. [hereinafter Alexander remarks]

[7] President Barack Obama, *Taking the Cyberattack Threat Seriously*, Wall Street Journal (July 19, 2012), available at http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html. [hereinafter "WSJ statement"]

[8] Cyber threats to the national security include: 1) cyber-based terrorism; 2) cyber-based espionage and other intelligence activities conducted by, for, or on behalf of foreign powers, organizations, or persons; and 3) the use of cyber activity or other means, by, for, or on behalf of a foreign power to scan, probe, or gain unauthorized access into U.S.- based computers.

- Prosecutors in NSD's CTS and CES, in close coordination with the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) and USAOs across the nation, assist investigators and intelligence professionals in preventing and disrupting cyber threats, and prosecute those who use cyber technologies and platforms to commit crimes falling within NSD's jurisdiction;

- NSD's OI provides technical, legal, and policy analysis to IC elements working on cyber issues to ensure that operators have the authorities necessary to carry out their intelligence missions, specifically with regard to operations involving the FISA, and provides oversight to ensure that those missions are carried out lawfully;

- Attorneys in NSD's L&P assess gaps in existing statutory frameworks, participate in several interagency and White House-led cyber security working groups, and advise operators on novel legal questions confronting the government's counter-cyber efforts; and

- NSD's FIRS reviews foreign investments in U.S. industry that may impact the national security, and works to harden corporate cyber defenses and security policies through mitigation agreements and ongoing efforts to monitor those agreements for compliance.

Because of its statutory role as the Department's liaison to the Director of National Intelligence and the IC—as well as its operational responsibilities for carrying out the Department's top priority national security mission—NSD has a duty to provide leadership in the effort to combat national security cyber threats, and is committed to using an intelligence-driven, threat-based, all-tools approach to the problem that draws on both law enforcement and intelligence capabilities and expertise, and includes close partnership with departments and agencies from across the government and the private sector.

The U.S. government needs to leverage criminal law enforcement tools in the fight against national security cyber threats, and that will require significant support from NSD. This approach has already yielded historic success – with the announcement in May of the first-ever criminal charges against members of the Chinese military for cyber-based corporate theft.

Looking ahead, to build upon this momentum and continue success, additional growth is needed. The FBI plans continued growth of its cyber resources, both to expand their technical capabilities and enhance partnerships via the National Cyber Investigative Joint Task Force (NCIJTF). NSD seeks additional resources, in part, to align NSD's growth with the FBI's and to capitalize on the FBI's shift in policy toward investigation and, ultimately, criminal prosecution, where appropriate.

In planning for the growth required in FY 2016 and beyond, NSD notes that notwithstanding the limited resources it has available to devote to cybersecurity, NSD has already made great strides in its efforts to combat cyber threats to the national security, as further detailed below.

National Security Cyber Specialist (NSCS) Network

In FY 2012, NSD established the nationwide NSCS Network—a cadre of cyber specialists from across all of NSD's sections and offices, CCIPS, each USAO, and representatives from other components of Justice. This network is designed to serve as a single point of entry – and a valuable and experienced resource – within the Department for national security cyber matters and issues.

Members of the national NSCS Network work closely with law enforcement and the IC to identify tools available for the disruption of cyber threats to the national security. This includes reviewing threat streams to determine where criminal prosecution may offer an effective and appropriate tool for disrupting or deterring national security cyber actors. With a keen understanding of the tradeoffs involved and the tools available, NSD is assisting investigators, prosecutors, and analysts in collaboratively identifying the best approach to particular cyber incidents. In addition, where prosecution is a viable option, NSCS Network members, along with other prosecutors in CTS and CES collaborate with their counterparts in the field to ensure they are equipped to handle the legal and evidentiary challenges that may arise.

In addition, within NSD, several NSCS Network prosecutors from the CTS and CES have been asked to focus *exclusively* on cyber matters. These prosecutors are relied upon both to drive investigations and prosecutions and to build capacity within the USAOs. It is this model that resulted in the recent historic national security cyber charges announced in May.

Building Expertise and Cultivating Cyber Specialists

To ensure that all NSD personnel are equipped to help address the national security cyber threat, NSD has also focused on training its existing counterterrorism, counterespionage, and intelligence experts on cyber-related issues including electronic evidence, the cyber threat landscape, and prosecuting cyber crimes. NSD has set an internal target of having a specially trained NSCS representative in 95% of the U.S. Attorneys' Offices. Every U.S. Attorney's Office has named at least one NSCS representative, and as of the end of June FY2014, 91 out of the 93 USAOs (one of which covers both Guam and the Northern Mariana Islands) have sent representatives to at least one of the two NSCS trainings held in 2012 or 2013 (for a total of 98%), up from 82% at the end of FY 2013. There are additional trainings scheduled in FY 2015, including a National Security Cyber Specialists course scheduled for November 2015 at the National Geospatial Intelligence Center as well as an Electronic Evidence and Cybercrime Seminar scheduled for NSD attorneys in October 2015.

National Cyber Investigative Joint Task Force Staffing

During the past two years, NSD has also increased its role on the NCIJTF, an FBI-led interagency body that coordinates domestic cyber threat investigations across nearly twenty government agencies, providing strategic direction to cyber investigators and intelligence

analysts alike. For over a year, NSD has had a dedicated liaison to NCIJTF, who provides legal guidance on intelligence-related issues arising in context of cyber national security investigations, helps preserve the option to prosecute in appropriate cases, serves as an information conduit to DOJ, and promotes NSD's ongoing efforts to bring all tools to bear against cyber threats to the national security.

Outreach Efforts

Cyber threats are often directed at private company networks and individuals. And as the front line in many cyber confrontations, private entities often have a great deal to lose from cyber attacks. In recognition of the private sector's mounting losses and consistent with President Obama's Cybersecurity Executive Order, NSD, working through the NSCS, continues to conduct outreach to the private sector in the interests of forging relationships built on trust and mutual interest. Through the NSCS Network, NSD has engaged in significant outreach, meeting with dozens of companies over the past two years. These meetings have greatly strengthened partnerships between NSD and the business community, and they promote cooperation in the event of a cyber incident. In addition, the NSCS has created a national outreach program for USAOs with talking points and presentations that can be used to develop relationships with the business community nation-wide. Using this information, NSCS field resources have begun reaching out to local business associations, promoting awareness of national security cyber threats, and encouraging reporting to law enforcement. Additional personnel-related resources will be needed to continue and enhance NSD's involvement in these important and productive initiatives.

Counterespionage Section

Program Change: Positions 5 Atty 2 FTE 2 Dollars $610,636

NSD requests 2 attorneys, 1 Intelligence Research Specialist (IRS), 1 paralegal, and 1 administrative assistant to assist in export control, counterintelligence, and national security cyber investigations and prosecutions. The full range of CES's work is increasingly moving toward cyber-based offenses.

CES Attorneys

The 2 CES attorneys will:

- **Support the FBI Counterintelligence Division (FBI CD) and FBI Cyber Division (FBI CYD)** in conducting investigations, developing potential criminal charges, and otherwise disrupting the increasing threats of economic espionage, cyber intrusions that impact national security, and the illegal export of military and strategic commodities. Additional attorneys are necessary to address the prevalence, sophistication, and growing complexity of these threats to our nation in a coordinated and effective manner.

- **Support an increase in strategic prosecutions arising out of interagency counterproliferation task forces.** These task forces will continue to adapt to the changing landscape of export control reform efforts. CES must devote the necessary resources to ensure USAOs and the export control community stay abreast of the changes while continuing to address and disrupt the threats using all available tools.

- **Support an increased focus on document intensive white-collar investigations into possible sanctions/export violations for which there is little investigative agency personnel support.** CES attorneys' expertise in these cases has expanded over the past few years, and, as the number of cases increase, the demand for resources within CES to focus on them will also increase.

- **Support the DOJ's role in leading the ongoing insider threat initiative**, a proactive and prophylactic effort to prevent and deter insider threats to not only classified information but also to critical sensitive but unclassified information. Cybersecurity is of particular concern in Insider Threat cases, in light of the high level of access to government computer networks and classified information that is now available to hundreds of thousands of government employees, defense contractors, and third party vendors and consultants. This widespread access to sensitive information via the government's varied computer networks presents a tremendous challenge for monitoring and national security reviews, and requiring investment of dedicated resources.

The following CES support staff is also requested:

Intelligence Research Specialist. NSD requests 1 CES IRS to assist with intelligence research in support of CES's work, including national security cyber cases. As the number of these cases increases and NSD continues to build subject matter expertise, the need for dedicated intelligence support is evident. The NSD IRS would be an important resource for developing threat-based intelligence about nation-state actors, cyber attack methodologies, and export controlled items that would enhance CES's ability to use prosecutions or other tools in strategic ways to disrupt the threats.

Paralegal Specialist. NSD requests 1 CES paralegal specialist position. There is a current gap in CES's ability to support attorneys on the increasing number of national security cyber, counterintelligence, and export control matters. An additional support position would allow attorneys to dedicate more time to attorney responsibilities and leverage support staff to support ongoing criminal investigations and other matters.

Administrative Specialist. NSD requests CES 1 administrative specialist position to assist with maintaining files, answering phones, and providing additional data entry and other support as needed.

Office of Intelligence

Program Change: Positions 7 Atty 7 FTE 4 Dollars $1,134,595

NSD requests 7 attorney positions to support combating cyber threats to national security in the areas of Intelligence Operations and Litigation.

Operations Attorneys

NSD requests 5 attorneys for OI's Operations Section. NSD expects to see continuation of a trend towards increasingly complex investigations, particularly with regard to cyber matters, which will require more attorney hours to process. 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, which are often technically complex and time consuming, and to become cyber experts. OI also will play a larger role in the Division's efforts to coordinate cyber-related efforts within the Department and across the Government, and that cannot be accomplished using existing resources.

Litigation Attorneys

NSD requests 2 litigation attorneys to support NSD's cyber efforts and use of FAA[9] information. OI expects to see continued considerable growth in the cyber area consistent with

[9] FISA Amendments Act of 2008

the Department and NSD's strategic goals. In accordance with the growing threat and increased prioritization, the Litigation Section anticipates dedicating an increasing number of resources to work on cyber-related litigation. In addition, OI anticipates a continued increase in resources dedicated to complex 702-related litigation.

OI's responsibilities in overseeing the use of FISA obtained or derived information in criminal, civil, and administrative proceedings have increased dramatically since 2001. 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 FISC and to suppress information obtained or derived from FISC-authorized electronic surveillance and physical search. In just one year 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.

Impact on Performance

As described above, these requests for resources are critical so that NSD can 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. Performance goals that track the Percentage of Defendants whose Cases are Favorably Resolved (for both CE and Cyber cases) would be the best indicator of success in the current endeavors.

Funding

Base Funding

FY 2014 Enacted				FY 2015 Enacted				FY 2016 Current Services			
Pos	Atty	FTE	$(000)	Pos	Atty	FTE	$(000)	Pos	Atty	FTE	$(000)
19	13	10	$2,654	19	13	19	$2,689	19	13	19	$2,689

Personnel Increase Cost Summary

Type of Position/Series	Modular Cost per Position ($000)	Number of Positions Requested	FY 2016 Request ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Intelligence Series (0132)	$122	1	$122	$66	$0
Clerical and Office Services (0300-0399)	60	1	$60	23	0
Attorneys (0905)	162	9	1,459	768	0
Paralegals / Other Law (0900-0999)	104	1	$104	43	0
Total Personnel		12	$1,745	$900	$0

Total Request for this Item

	Pos	Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Current Services	19	13	19	$2,689	$0	$2,689		
Increases	12	9	6	1,745	0	1,745	$900	$0
Grand Total	31	22	25	$4,434	$0	$4,434	$900	$0

B. Item Name: Intelligence Collection and Oversight

AG Targeted Priority Options:	Targeting and disrupting terrorist threats and groups
Strategic Goal:	Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law
Strategic Objective:	Objective 1.1: Prevent, disrupt, and defeat terrorist operations before they occur by integrating intelligence and law enforcement efforts to achieve a coordinated response to terrorist threats
Budget Decision Unit(s):	National Security Division
Organizational Program:	Office of Intelligence

Program Increase: Positions 10 Atty 8 FTE 5 Dollars $1,486,162

Description of Item

The NSD requests a total of 10 positions, including 8 attorneys and 2 non-attorneys, to support the growing area of intelligence collection and oversight.

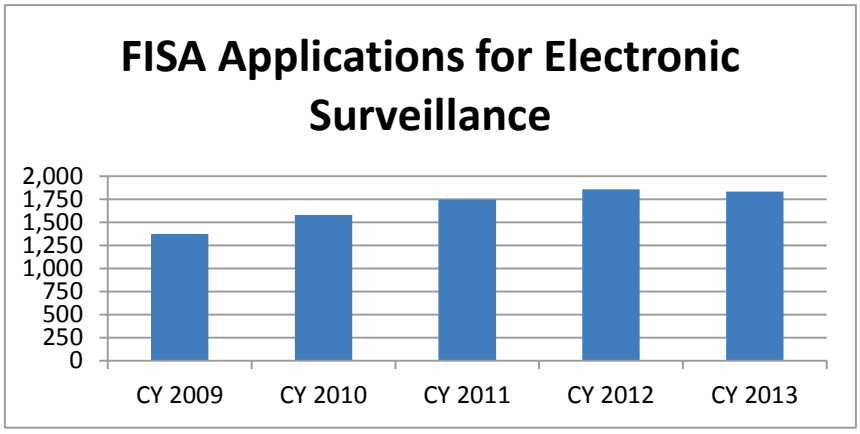
OI's work supports the U.S. Government's national security mission fully, including combating the threats posed by terrorists, threats to our nation's cybersecurity, and other threats. As President Obama stated in a speech early this year, our nation's intelligence agencies are asked to "identify and target plotters in some of the most remote parts of the world, and to anticipate the actions of networks that, by their very nature, cannot be easily penetrated with spies or informants." OI's work directly contributes to these efforts, and is increasingly important as the nation faces a growing and evolving threat landscape, including the threats of foreign terrorist fighters and homegrown violent extremism, cyber attacks, and other counterintelligence threats. The President has also tasked the Department with working on at least ten different lines of effort related to intelligence reform and oversight, the vast majority of which will fall to NSD to implement. NSD will require permanent resources to implement these taskings on an ongoing basis.

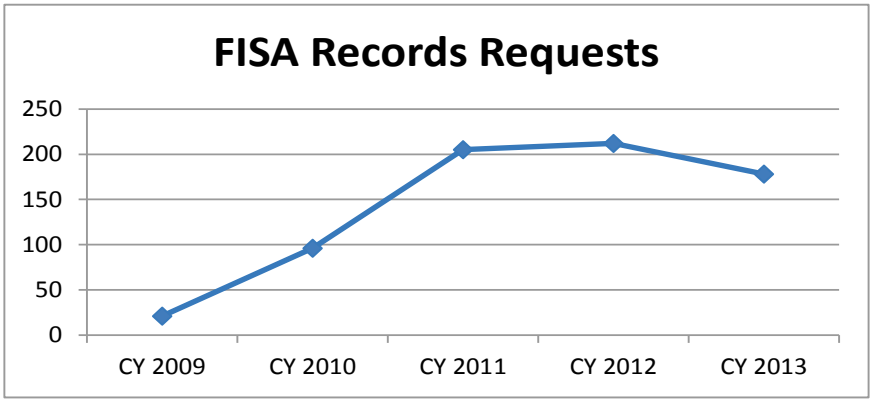
Justification

Operations Attorneys

NSD requests 4 attorneys for the Operations Section of OI. The complexity of intelligence investigations is ever increasing and requires increased attorney hours to process. OI's Operations Section, including its Counterterrorism Unit, has contributed to broader U.S. government disruptions of terrorist threats, and the identification of new threat actors and threat streams. These attorneys will be responsible for, among other things, preparing applications for electronic surveillance and physical search to the FISC in national security investigations, including counterterrorism investigations, pursuant to FISA, as well as for providing legal advice to Division and Department leadership and the Intelligence Community (IC) on a variety of intelligence-related matters. NSD has assessed that the Operations Section needs these resources to ensure it can fully meet its mission requirements. In addition, NSD anticipates it will continue to deal with increased workload generated from recent unauthorized disclosures, which have put significant strains on the staffing of a wide variety of projects, such as declassification reviews, reviews of legislative proposals, and responding to FOIA and other types of litigation.

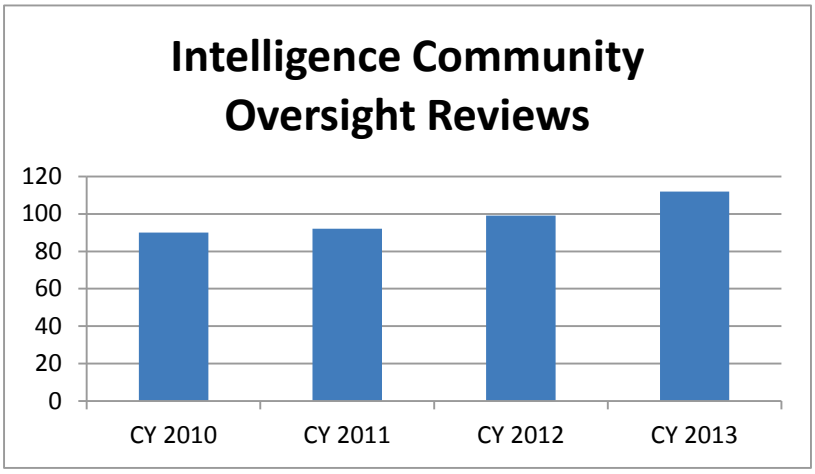
The trends over the last several years have shown an unmistakable increase in the number of requests for FISA authorities handled by the Operations Section. For example, between 2009 and 2013, the number of FISA applications for electronic surveillance and/or physical search increased by approximately 33 percent (from 1,376 in 2009 to 1,833 in 2013). 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 and 178 were approved in 2013 (an increase of approximately 748 percent between 2009 and 2013). OI expects the number of business records requests to remain near or above this level for the foreseeable future. Additional attorney resources are needed in order to address the increased workload.





Oversight Attorneys

NSD requests 4 attorneys for the Oversight Section of OI. OI continues to develop its oversight capabilities and programs to support Intelligence Community operations and to increase assurance that operational activities are executed in compliance with governing rules. Efforts related to intelligence oversight and reform have been of the highest priority to the Department and to the President. OI anticipates that additional Oversight resources will enable OI to better help agencies avoid mistakes that could lead to compliance problems, and ensure that intelligence collection is conducted consistent with the laws and policies by which it is governed. 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, and its enhanced oversight role is expected to continue to grow in the future. As just one example, OI's Oversight Section has expanded, and will continue to expand, the number of IC oversight reviews it conducts. These rigorous 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 focus shared by the Department, the FISC, the Executive Branch more broadly, and Congress in how FISA-derived information is being marked, used, retained and disseminated by the government.



Additionally, NSD anticipates new oversight and reporting requirements to arise from the current FISA amendment proposals currently under consideration in Congress. Furthermore, in light of recent public disclosures, Executive Branch review panels and inspectors general have been actively engaged in reviewing and evaluating oversight mechanisms. These reviews have required significant Oversight Section resources to help ensure that such review panels are fully briefed on Department oversight activities and are given access to documents and information needed for their consideration. Finally, the Oversight Section has experienced significant impacts on resources from staffing a wide variety of projects, such as declassification reviews, reviews of legislative proposals, and responding to FOIA and other types of litigation.

Support Staff

Finally, NSD requests 2 support staff positions to support the work of these additional OI attorneys.

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. All of these OI positions are critical to our Department's efforts to fully support the nation's security, including its counterterrorism mission. OI plays a critical role supporting IC partners as well. As those partners continue to grow, OI will need commensurate resources to support their operations. Without them, NSD anticipates it will not have sufficient staff to fully execute the intelligence-related work needed to

support national security investigations, including those targeting terrorist threats. All of the requested resources are critical to ensure that NSD can keep pace with the changing and growing threat landscape, and to fully support disruption of these threats.

Funding

Base Funding

FY 2014 Enacted				FY 2015 Enacted				FY 2016 Current Services			
Pos	Atty	FTE	$(000)	Pos	Atty	FTE	$(000)	Pos	Atty	FTE	$(000)
165	134	149	$48,331	165	134	149	$47,068	153	110	140	$28,864

Personnel Increase Cost Summary

Type of Position/Series	Modular Cost per Position ($000)	Number of Positions Requested	FY 2016 Request ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Clerical and Office Services (0300-0399)	$95	2	$190	71	0
Attorneys (0905)	$162	8	$1,296	682	0
Total Personnel		10	$1,486	$753	$0

Total Request for this Item

	Pos	Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Current Services	153	110	140	$28,864	$0	$28,864		
Increases	10	8	5	1,486	0	1,486	$753	$0
Grand Total	163	118	145	$30,350	$0	$30,350	$753	$0

C. Item Name:	**Combating Terrorism, including Homegrown Violent Extremism**
AG Targeted Priority Options:	Targeting and disrupting terrorist threats and groups
Strategic Goal:	Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law
Strategic Objective:	Objective 1.1: Prevent, disrupt, and defeat terrorist operations before they occur by integrating intelligence and law enforcement efforts to achieve a coordinated response to terrorist threats Objective 1.2: Prosecute those involved in terrorist acts
Budget Decision Unit(s):	National Security Division
Organizational Program:	Counterterrorism Section, Office of Justice for Victims of Overseas Terrorism

Program Increase: Positions 6 Atty 4 FTE 3 Dollars $874,383

Description of Item

NSD requests a total of 6 positions, including 4 attorneys and 2 non-attorneys, to support combating homegrown violent extremist (HVE) threats.

Justification

Counterterrorism Section

Program Change: Positions 5 Atty 3 FTE 2 Dollars $712,298

NSD requests 3 attorneys, 1 paralegal, and 1 Intelligence Research Specialist (IRS), to address the on-going HVE threat. CTS continues to see a rise in homegrown violent extremism, which has resulted in terrorist attacks on U.S. soil inflicting civilian casualties, such as in the Boston Marathon bombings in April 2013. The threat is only heightened by the increasing number of U.S. persons traveling to Syria to join the on-going conflict there. These individuals may return to the U.S. trained in the use of improvised explosive devices and other weapons. Islamic extremists on-line are continuing to seek to recruit individuals, including U.S. persons, to join the conflict in Syria, as well as to join al-Shabaab and other terrorist organizations

Over the past decade, terrorism has become increasingly diverse and decentralized – as CTS has made progress against core al Qaeda, and as the cadre of al Qaeda affiliates around the globe continues to grow, terrorists have turned to a more diverse set of tactics. As a result, CTS is focused on a trend toward smaller, faster-developing plots, rather than larger, longer-term plots like 9/11. One of the biggest issues that continues to present itself is the threat of HVEs. These

HVEs reside or operate in the U.S. and become inspired by al Qaeda or similar groups through English-language propaganda, but do not have any ties to al Qaeda or any other foreign terrorist organization. In testimony to the Senate Committee on Homeland Security and Government Affairs, the head of the National Counterterrorism Center (NCTC) said, "Lone actors or insular groups pose the most serious HVE threat to the homeland. HVEs could view lone offender attacks as a model for future plots in the U.S. and overseas. The perceived success of previous lone offender attacks combined with al Qaeda and AQAP's propaganda promoting individual acts of terrorism is raising the profile of this tactic."[10]

The distributed nature of these types of threats makes investigation of them incredibly complex – as terrorist groups have turned to inspiring individuals across the globe to commit independent and more easily executed acts of terror, identifying and disrupting the threat has become increasingly resource-intensive. Unlike the small, organized cells that CTS has traditionally dealt with, the new face of terrorism is everywhere, and the potential population of would-be attackers is not easily knowable. In recognition of this new reality, FBI has evolved and reorganized to devote additional resources to this problem. CTS and the IC predict a continued trend of self-radicalized individuals engaging in these types of attacks on government and civilian targets. CTS provides full spectrum support to the FBI, IC, and USAOs for every HVE case in the country, and thus, NSD must devote additional resources to this critical threat.

CTS Attorneys

Terrorism investigations involving HVEs are complex and involve difficult legal issues requiring extensive attorney support throughout the investigations, advising on both the investigative strategy and ultimate prosecution. CTS attorneys are specially trained to handle these types of investigations with expertise in prosecuting cases involving weapons of mass destruction and classified information. The attorneys also routinely serve as members of the trial team on these cases in districts around the country, sometimes for extended periods of time. It is imperative to national security that CTS is able to meet the increasing HVE threat by providing critical resources to these investigations and prosecutions.

CTS Paralegal and Intelligence Research Specialist

Additional support staff resources are also necessary to support CTS's efforts on these investigations and prosecutions. Paralegals provide critical assistance to CTS and USAOs on these investigations. Discovery is extensive in these types of cases and it is frequently requested that CTS provide paralegal support as well as attorney support to the USAOs during both the investigative phases and trial preparation and presentation. It is also critical to have intelligence specialist support to assist CTS attorneys in wading through the extensive intelligence reporting on these investigations. Intelligence Research Specialists highlight those reports that are relevant

[10] Matthew G. Olson, Director of NCTC, Hearing before the Senate Committee on Homeland Security and Government Affairs, *The Homeland Threat Landscape and U.S. Response*, September 19, 2012.

to on-going investigations and help identify new matters in need of investigation involving HVEs.

Office for Justice for Victims of Overseas Terrorism

Program Change: Positions 1 Atty 1 FTE 1 Dollars $162,085

NSD requests 1 OVT attorney advisor. This request relates most directly to DOJ Objective 1.2's strategy to build strong cases for prosecution both in the U.S. and overseas. The OVT's unique support to U.S. victims of overseas terrorism builds stronger cases against terrorists in foreign prosecutions. Stronger cases lead to more convictions of dangerous terrorists, putting them in prison and limiting their ability to engage in future attacks against U.S. citizens and interests. Moreover, increased victim participation in foreign trials encourages longer prison sentences for convicted terrorists and is a key element in the global strategy to fight and overcome violent extremism around the world.

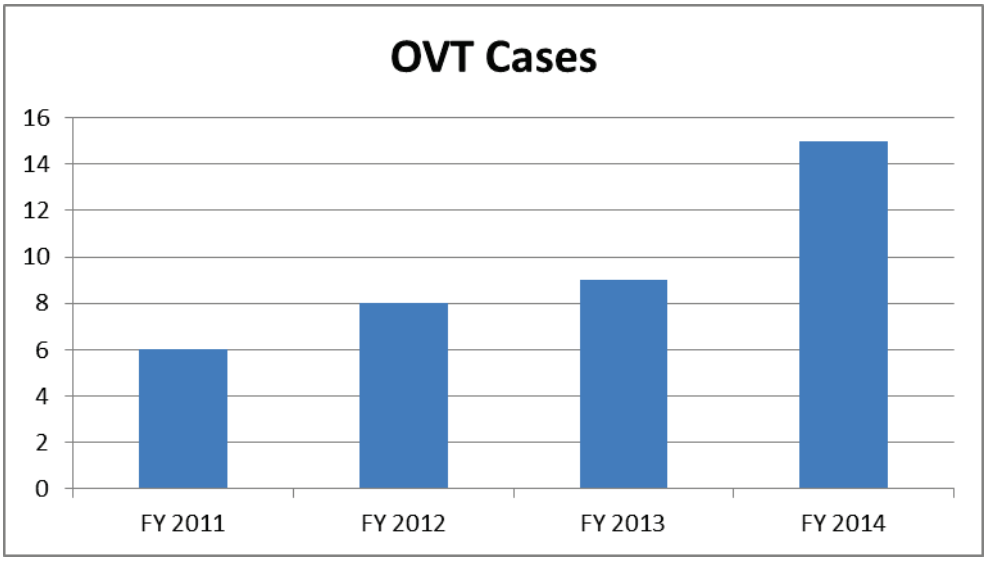
OVT's recent success in supporting U.S. victims during the Indonesian trial of convicted Bali bomber Umar Patek shows the terrorism fighting potential of OVT's programs. In that case, OVT educated Indonesian prosecutors on victims' rights and victim participation in criminal trials. As a result, the Indonesian prosecutors requested that U.S. victims testify in the Indonesian prosecution. OVT identified one U.S. victim willing to travel to Indonesia to testify. OVT funded the victim's travel and also arranged to collect victim impact statements from 10 other U.S. victims to provide to the Indonesian court. The U.S. victim provided strong testimony in the case, and his presence encouraged our ally, Australia, who lost many more victims in the Bali attack, to send three Australian victims to testify. According to those observing the trial, the presence of the foreign witnesses significantly strengthened the prosecution and led to a lengthier prison sentence once Patek was convicted. Patek is now serving a 20 year sentence in prison. Experts tell us that they expected him to receive 7 years. That is 13 additional years during which Patek will be unable to make bombs.

In addition, the U.S. government is currently in a position to provide significant international leadership concerning terrorism victim rights. The U.S. State Department is actively promoting the Global Counterterrorism Forum (GCTF), a collection of 30 countries that have joined together to fight international terrorism in a coordinated way. One of the GCTF's most important initiatives is its effort to fight violent extremism, particularly in countries where the terrorists' claims and propaganda are prominent. A key part of the strategy to fight violent extremism propaganda is to support and encourage the terrorism victim narrative. Ensuring that victims' voices are publicly heard, and that victims play a role in criminal prosecutions, will erode support for terrorists and limit terrorist organizations' ability to recruit new adherents. The momentum for these efforts is building and now is the time to advance this agenda with the support of our international allies.

The additional OVT attorney advisor would support the efforts of the GCTF and where appropriate, other international counterterrorism forums. The attorney would assist the GCTF in

the implementation of its *Plan of Action on Victims of Terrorism* and the promotion of best practices outlined in the *Madrid Memorandum,* which the GCTF formally adopted in September, 2013. OVT offered technical assistance in the creation of these documents and the GCTF has requested OVT's continued assistance. Wider implementation of the *Madrid* principles would result in greater international cooperation in terrorist investigations and prosecutions as well as increase investigatory and prosecutorial capacity, and thereby fortify U.S. counterterrorism efforts. The added attorney would explore collaborative relationships with other global efforts, including relevant initiatives of the United Nations Office on Drugs and Crime, which has also promulgated basic international standards in regard to a terrorist victim's access to justice. Participation in global forums would also strengthen DOJ's relationship with its international counterparts also working to dismantle terrorist organizations.

The number of active cases OVT monitors overseas has almost doubled in the past 3 fiscal years. At this time OVT is monitoring and providing limited services in 15 foreign prosecutions. In contrast, during FY 2013, OVT monitored nine cases, and in FY 2012, OVT monitored eight cases.



Impact on Performance

This request is directly tied to DOJ's Strategic Objectives 1.1 and 1.2, as CTS is the driving force behind NSD's efforts to prevent, detect, deter, and prosecute terrorist activities. These objectives have been supported with existing resources, some of which have now been shifted to focus on the cyber threat, another high priority of the Division. As CTS attorneys are increasingly called upon to handle cyber cases, which typically require an extensive amount of NSD involvement, CTS resources will continue to be strained. NSD predicts a slowing in timeliness of responses to USAOs if additional resources are not provided to support CTS cases, in particular HVE-

focused cases.
This increase is tracked in large measure by percentage of CT defendants whose cases were favorably resolved. Without these personnel increases, it is anticipated that as attorney resources continue to be redirected to cyber cases, HVE cases may suffer declining success rates. If NSD is able to remain on target with a high percentage of CT cases favorably adjudicated, NSD will be able to meet DOJ's Strategic Goals 1.1 and 1.2, thereby preventing terrorist operations before they occur and successfully disrupt terrorist attacks.

Funding

Base Funding

FY 2014 Enacted				FY 2015 Enacted				FY 2016 Current Services			
Pos	Atty	FTE	$(000)	Pos	Atty	FTE	$(000)	Pos	Atty	FTE	$(000)
71	53	64	$14,167	71	53	64	$13,797	57	47	55	$13,103

Personnel Increase Cost Summary

Type of Position/Series	Modular Cost per Position ($000)	Number of Positions Requested	FY 2016 Request ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Intelligence Series (0132)	$122	1	$122	$66	$0
Attorneys (0905)	$162	4	648	341	0
Paralegals / Other Law (0900-0999)	$104	1	104	43	0
Total Personnel		6	$874	$450	$0

Total Request for this Item

	Pos	Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Current Services	57	47	55	$13,103		$13,103		
Increases	6	4	3	874	$0	874	450	0
Grand Total	63	51	58	$13,977		$13,977	$450	$0

VI. Program Decrease by Item

A. Item Name: Program and/or Administrative Savings

Program Decrease: Positions _0__ Agt/Atty __0___ FTE _0___ Dollars ($1,200,000)

Description of Item
Program and/or administrative savings.

Justification
Examples of savings to be realized in 2016 include, but are not limited to reducing the physical footprint, leveraging and extending the useful life of existing technology, bulk purchases and bundling technology procurements.

Funding

Non-Personnel Program Decrease

Type of Position/Series	Unit Cost	Quantity	FY 2016 Request ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Program Decrease	($1,200)	1	($1,200)	0	0
Total Non-Personnel		1	($1,200)	0	0

Total Request for this Item

	Pos	Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Current Services	0	0	0	0	0	0		
Offset	0	0	0	0	(1,200)	(1200)	0	0
Grand Total	0	0	0	0	($1,200)	($1,200)	$0	$0

VII. Exhibits