FY 2017
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 2017 a total of 393 positions (including 254 attorneys), 364 FTE, and $97,337,000.[1]

B. Background

In recent years, NSD engaged in a comprehensive strategic assessment of the Division's current operations and future requirements. The outcome of the assessment resulted in NDS outlining three areas of new or renewed focus that will guide its operations in the coming years:

- Continuing to bring an all-tools, integrated approach to NSD's counterterrorism work, while adapting to address the changing terrorism threats that include cyber-based terrorism and homegrown violent extremism;
- Continuing to protect national assets from both cyber-based and non-cyber-based threats through a strong counterintelligence and export control program designed to combat traditional espionage, economic espionage and proliferation of weapons of mass destruction; and
- Enhancing NSD's intelligence-related programs and its intelligence oversight function.

All of the program increases reflected in NSD's FY 2017 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 evolving and growing threats. NSD's assessment of the challenges it faces in fully realizing its goals in these areas are further outlined 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);
- Counterintelligence and Export Control Section (CES);
- Office of Law and Policy (L&P);

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

- Foreign Investment Review Staff (FIRS); and
- Office of Justice for Victims of Overseas Terrorism (OVT).

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

NSD Major Responsibilities

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 National Security Coordinator/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;
- 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 United States (U.S.) Government efforts on the Financial Action Task Force; and
- Through OVT, prioritizing within the Department the investigation and prosecution of terrorist attacks that have resulted in the deaths and/or injuries of American citizens overseas, and ensuring support for, and the protection of rights of, victims and families.

Protection of National Assets through 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;
- Enforcing the Foreign Agents Registration Act of 1938 (FARA) and related disclosure statutes;
- Through FIRS, 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.

Intelligence Operations, Litigation, *Oversight and Reporting*

- 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;
- Serving as the Department's primary liaison to the Director of National Intelligence and the IC.
- 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.

Cross-Cutting National Security Policy, Litigation, and Legal Support

- 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.

NSD Recent Accomplishments (unclassified selections only)

- Brought scores of charges against foreign terrorist fighters and homegrown violent extremists to disrupt these emerging and growing threats.
- 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 number of USAOs across the country, successfully brought charges in a number of complex national security cyber cases.
- Continued to support the IC by seeking authority under FISA with the FISC.
- Designated 245 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.
- Helped lead the President's efforts to review hostage procedures and staffed a hostage review group.

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 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 changing terrorism threat, including the risks posed by homegrown violent extremists and the potential for cyber-based terrorism;
2. The recent recognition of increasing and changing threats to our national assets, including significant growth of cyber threats to the national security; and
3. An increasing workload in intelligence oversight, operations, and litigation; and
4. Difficulties inherent in supporting the continued development of a relatively new Division in an ever-changing environment.

The terrorism threat continues to become increasingly diverse and decentralized – as the world has made progress against core al Qaeda, the Islamic State of Iraq and the Levant ("ISIL") has emerged and turned to a more diverse set of tactics, calling on operatives to engage in terrorism attacks wherever the opportunity arises. Thus, NSD and its partners are increasingly focused on this new trend and disrupting smaller, faster-developing plots, rather than larger, longer-term plots like 9/11.

As part of this changing threat environment, there continues to be 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. In addition, there continues to be an increasing number of U.S. persons traveling to Syria to join the ongoing conflict there. These individuals may return to the U.S. trained in the use of improvised explosive devices and other weapons, prepared to conduct attacks.

The threat of these types of attacks is heightened by Islamic extremists aligned with ISIL and other terrorist organizations, such as al-Shabaab, that continue to leverage social media and online engagement to further their recruitment efforts and call for attacks against the homeland. This environment gives rise to the potential for increasing number of HVEs, who – although they do not necessarily have any direct ties to ISIL, al Qaeda or any other foreign terrorist organization – reside or operate in the U.S. and become inspired by ISIL, al Qaeda or similar groups through social media and English-language propaganda.

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 NSD has traditionally seen, the new face of terrorism is everywhere, and the potential population of would-be attackers is not easily knowable.

Also 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.

NSD expects to see continued considerable growth in the area of use and litigation relating to Section 702 information. There have been several high-profile litigation matters during the past year involving individuals indicted for terrorism-related charges. A sample of those cases includes the following:

U.S. v. Fazliddin Kurbanov – On January 7, 2016, Fazliddin Kurbanov was sentenced in the District of Idaho to 25 years in prison. Kurbanov was charged in a 5 count superseding indictment with conspiring and attempting to provide material support to terrorists, conspiring and attempting to provide material support to a designated foreign terrorist organization, and possession of an unregistered firearm (destructive device). After a five week jury trial in Idaho, Kurbanov was convicted of 3 of the 5 counts on August 12, 2015. He was convicted of conspiring and attempting to provide material support to a designated foreign terrorist organization, and possession of an unregistered firearm (destructive device). The evidence at trial demonstrated that Kurbanov sought to provide himself as personnel to the Islamic Movement of Uzbekistan, a designated foreign terrorist organization, for the purpose of conducting a bomb attack within the United States. Kurbanov had purchased various bomb-making components, conducted research on how to make explosives and asked the IMU for assistance in making a remote detonator for an attack. Kurbanov also conspired with the IMU to provide money and computer software. While meeting with an FBI Confidential Human Source (CHS) in Utah, Kurbanov spent hours showing the CHS videos about bomb-making, and instructing the CHS on how to build and utilize explosives for an attack. Kurbanov is separately charged in a pending indictment in the District of Utah with one count of distribution of

information relating to explosives, destructive devices and weapons of mass destruction. Kurbanov has not yet made an appearance in Utah on that charge.

U.S. v. Mohamed Osman Mohamud - In the district of Oregon, Mohamud was found guilty of attempting to use a weapon of mass destruction for his attempt to detonate a bomb at the annual Christmas tree lighting ceremony at Pioneer Square in Portland, Oregon. The government successfully litigated before the District Court the legality of the use of certain information acquired pursuant to Section 702 of the FISA Amendments Act. This case is currently being appealed.

U.S. v. Agron Hasbajrami – In the Eastern District of New York, Hasbajrami pleaded guilty to attempting to provide material support to terrorists. Hasbajrami's case arose out of his activities in support of Islamic fundamentalist terrorist organizations and his attempt to travel to Pakistan to join a foreign fighter group. Following imposition of his sentence, the District Court granted the defendant's motion to vacate and set aside his sentence. Thereafter, the government successfully litigated before the District Court the legality of the use of certain information acquired pursuant to Section 702 of the FISA Amendments Act. This case is currently being appealed.

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.

II. Summary of Program Changes (Not Applicable)

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, [$95,000,000] *$97,337,000*, 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
2015 Enacted	383	354	$93,000,000
2016 Enacted	393	359	95,000,000
Adjustments to Base and Technical Adjustments	0	5	2,337,000
2017 Current Services	393	364	97,337,000
2017 Program Increases	0	0	0
2017 Program Offsets	0	0	0
2017 Request	393	364	97,337,000
Total Change 2016-2017	**0**	**5**	**$2,337,000**

***National Security Division*-Information Technology Breakout (of Decision Unit Total)**	Direct Pos.	Estimate FTE	Amount
2015 Enacted	14	14	14,299,000
2016 President's Budget	14	14	14,299,000
Adjustments to Base and Technical Adjustments	0	0	0
2017 Current Services	14	14	14,299,000
2017 Program Increases	0	0	0
2017 Program Offsets	0	0	0
2017 Request	14	14	14,299,000
Total Change 2016-2017	0	0	$0

1. Program Description

The National Security Division (NSD) is responsible for:

- overseeing terrorism investigations and prosecutions;
- protecting critical national assets from national security threats, including through handling counterespionage, counterproliferation, and national security cyber cases and matters;
- serving as the Department's liaison to the Director of National Intelligence;
- administering 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;

- conducting 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; 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., including counterintelligence threats and cyber threats to the national security 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, 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, NSD, through its 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 2015		**FY 2015**		**FY 2016**		**Current Services Adjustments and FY 2017 Program Changes**		**FY 2017 Request**		
Workload[1]												
Defendants Charged[2]		127		143		137		0		137		
Defendants Closed[3]		112		136		117		5		122		
Matters Opened		72,561		96,652		72,596		13,015		85,611		
Matters Closed		72,458		96,395		72,473		13,010		85,483		
FISA Applications Filed[4]		CY 2015: 2,200		CY 2015: 2,200		CY 2016: 2,200		0		CY 2017: 2,200		
National Security Reviews of Foreign Acquisitions		CY 2015: 225		CY 2015: 222		CY 2016: 225		0		CY 2017: 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**	
		345	93,000	354	93,000	359	95,000	5	2,337	364	97,337	
		FY 2015		**FY 2015**		**FY 2016**		**Current Services Adjustments and FY 2017 Program Changes**		**FY 2017 Request**		
Program Activity	**Intelligence**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	
		202	60,087	207	60,087	197	47,178	2	1,206	199	48,384	
Output Measure	Intelligence Community Oversight Reviews	CY 2015: 97		CY 2015: 124		CY 2016: 100		0		CY 2017: 105		

[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]Title has been modified to more accurately reflect the data being collected.

[3]Title has been modified to more accurately reflect the data being collected.

[4]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

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 2015		FY 2015		FY 2016		Current Services Adjustments and FY 2017 Program Changes		FY 2017 Request	
Program Activity	**Counterterrorism**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		85	18,235	87	18,235	90	22,225	0	310	90	22,535
Efficiency Measure	Percentage of OVT responses to victims within 3 business days of victim request for information from OVT	80%		90%		80%		0%		80%	
Outcome Measure	Percentage of services/rights OVT successfully provided to victims of new attacks	95%		95%		95%		0%		95%	
Outcome Measure	Percentage of CT defendants whose cases were favorably resolved	90%		98%		90%		0		90%	
Outcome Measure	Percentage of CT cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	99%		100%		99%		0		99%	
Program Activity	**Counterespionage**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		39	11,989	41	11,989	49	22,125	0	309	49	22,434
Outcome Measure	Percentage of CE defendants whose cases were favorably resolved	90%		100%		90%		0		90%	
Outcome Measure	Percentage of CE cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	99%		100%		99%		0		99%	
Output Measure	FARA inspections completed	14		14		14		0		14	
Output Measure	High priority national security reviews completed	CY 2015: 35		CY 2015: 35		CY 2016: 35		0		CY 2017: 35	
Program Activity	**Cyber**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		19	2,689	19	2,689	22	3,472	3	512	25	3,984
New FY 2015 Outcome Measure	Percentage of Cyber defendants whose cases were favorably resolved	90%		100%		90%		0		90%	

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 2011	FY 2012	FY 2013	FY 2014	FY 2015	FY 2015	FY 2016	FY 2017
		Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Performance Measure	Intelligence Community Oversight Reviews	CY 2011: 92	CY 2012: 99	CY 2013: 112	CY 2014: 109	CY 2015: 97	CY 2015: 124	CY 2016: 100	CY 2017: 105
Efficiency Measure	Percentage of OVT responses to victims within 3 business days of victim request for information from OVT	90%	89%	100%	100%	80%	90%	80%	80%
Outcome Measure	Percentage of services/rights OVT successfully provided to victims of new attacks	N/A	N/A	94%	99%	95%	95%	95%	95%
Outcome Measure	Percentage of CT defendants whose cases were favorably resolved	98%	98%	94%	92%	90%	98%	90%	90%
Outcome Measure	Percentage of CT cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	100%	100%	99%	100%	99%	100%	99%	99%
Outcome Measure	Percentage of CE defendants whose cases were favorably resolved	98%	100%	100%	98%	90%	100%	90%	90%
Performance Measure	FARA inspections completed	15	15	15	12	14	14	14	14
Performance Measure	High priority national security reviews completed	FY 2011: 29	CY 2012: 37[1]	CY 2013: 30	CY 2014: 32	CY 2015: 35	CY 2015: 38	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	NA	NA[2]	90%	100%	90%	90%

[1] Beginning CY 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 did report an actual for this measure because no cyber cases were resolved during the fiscal year.

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:

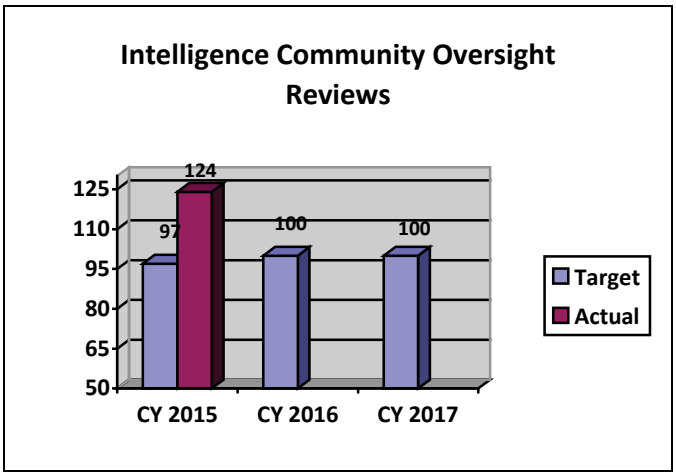
1.1 Prevent, disrupt, and defeat terrorist operations before they occur by integrating intelligence and law enforcement efforts to achieve a coordinated response to terrorist threats
1.2 Prosecute those involved in terrorist acts
1.3 Investigate and prosecute espionage activity against the U.S., strengthen 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 2015 Target: 97
CY 2015 Actual: 124
CY 2016 Target: 100
CY 2017 Target: 105
Discussion: The CY 2017 target is consistent with the previous targets. The work in this area is expected to continue to 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 IC Oversight Reviews.

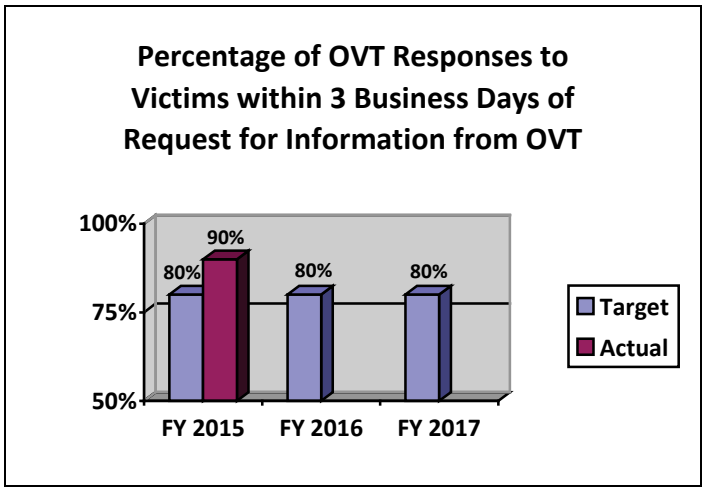
Data Collection and Storage: The information collected during each review is compiled into a report, which is then provided to the reviewed Agency. Generally, the information collected during each review, as well as the review reports, are stored on a classified database. However, some of the data collected 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 2015 Target: 80%
FY 2015 Actual: 90%
FY 2016 Target: 80%
FY 2017 Target: 80%
Discussion: The FY 2017 target is consistent with previous years. Additional personnel resources could allow OVT to improve efficiency regarding responses to victims.



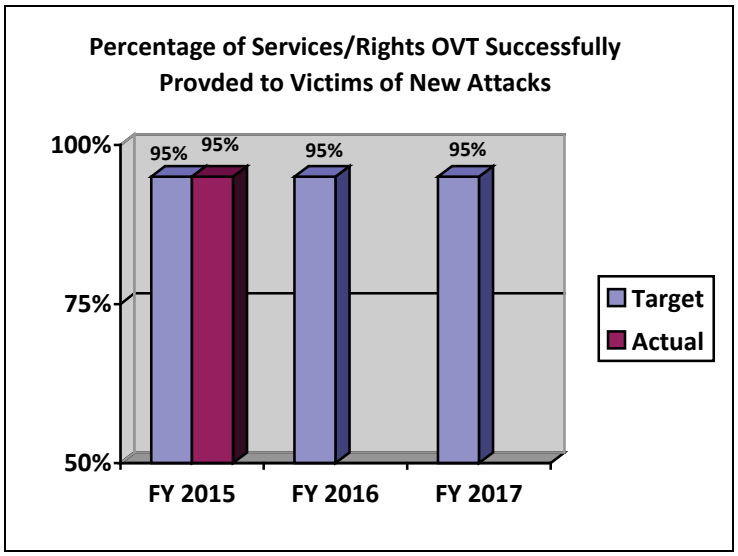
Data Definition: Victims: American citizens who are the victims of terrorism outside the borders of the U.S. This measure reflects OVT's efficiency in providing information to victims after they have contacted OVT.

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 2015 Target: 95%
FY 2015 Actual: 95%
FY 2016 Target: 95%
FY 2017 Target: 95%
Discussion: The FY 2017 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.



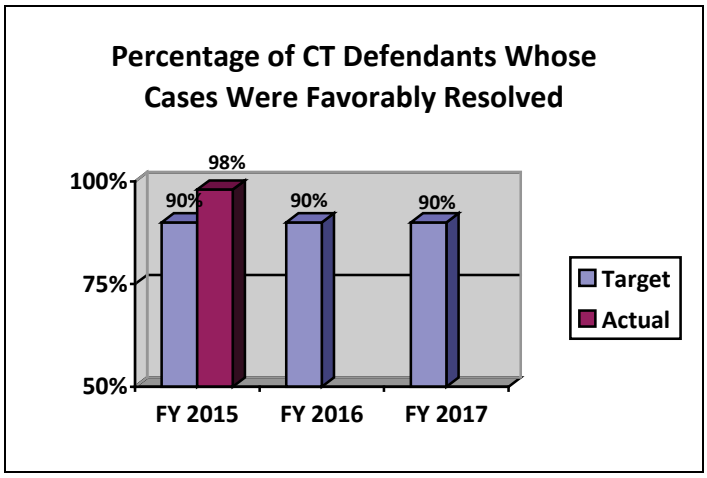
Data Definition: This measure counts the percentage of services/rights OVT provided during the fiscal year that are successfully resolved through the provision of a set group of services. OVT monitors only new attacks that occurred during the fiscal year. Most referrals come from the FBI's Office for 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 2015 Target: 90%
FY 2015 Actual: 98%
FY 2016 Target: 90%
FY 2017 Target: 90%
Discussion: The FY 2017 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 June 24, 2015, Dzhokhar Tsarnaev was sentenced to death in the District of Massachusetts for his role in the Boston Marathon bombings that occurred on April 15, 2013. As a result of the explosions at the Boston Marathon that day, three people were killed and over two hundred were injured. In addition, an MIT police offer was subsequently killed. Tsarnaev and his brother Tamerlan were identified as the individuals who had left the explosive-laden backpacks at the scene. Tamerlan Tsarnaev died after a gun fight with law enforcement on April 18, 2013. Dzhokhar Tsarnaev was apprehended following an extensive manhunt the next day and charged with numerous offenses including conspiracy to use weapons

of mass destruction, conspiracy to bomb a place of public use, malicious destruction of property, 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 April 8, 2015, Tsarnaev was convicted on all 30 counts of the charging document.

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 was 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 was 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 charged 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 was 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. 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.

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 on February 6, 2015, was sentenced to twenty-five years' imprisonment. On February 26, 2015, in the Southern District of New York, a jury convicted al Fawwaz of all counts. He was sentenced on May 15, 2015 to life imprisonment.

U.S. v. Abu Hamza al-Masri, et al. – 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 eleven 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. Mustafa was sentenced on January 9, 2015, to life in prison. The indictment also charged two co-conspirators, Oussama Abdullah Kassir and Haroon Rashid Aswat. Kassir was convicted in federal court of various terrorism offenses on in May 2009, including his participation in efforts to establish the Bly terrorist training camp, and was sentenced in September 2009 to life in prison. On March 30, 2015, nearly 10 years after an arrest in Zambia and a long extradition process, Aswat pleaded guilty to providing and conspiring to provide material support to a designated terrorist group, al Qaeda, in connection with his efforts to establish the Bly camp. On October 16, 2015, Aswat was sentenced to 20 years in prison.

New York Subway Bomb Plot / U.S. v. Medunjanin, et al. – On March 4, 2015, an eighth defendant in this case, Abid Naseer, was convicted of multiple terrorism offenses in the Eastern District of New York. On November 24, 2015, in the Eastern District of New York, he was sentenced to a term of 40 years' imprisonment for his role in the international terrorism conspiracy.

Evidence at trial demonstrated that in 2008 and 2009, al-Qaeda external operations leaders and facilitators located in the Waziristan region of Pakistan tasked Naseer, along with Adis Medunjanin, Najibullah Zazi, Zarein Ahmedzay, and a Norwegian operative to return to their home countries and conduct terrorist attacks. The evidence revealed that these Western operatives all traveled to Pakistan and met with al-Qaeda members who provided them with training. They subsequently returned to their respective target locations to begin preparing for attacks.

Medunjanin, Zazi, and Ahmedzay (cooperating with authorities) 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. 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.

As to Naseer specifically, evidence collected by law enforcement from the United Kingdom demonstrated that between November 2008 and April 2009, he, another Pakistani named Tariq ul-Rahman, and several associates from Liverpool, United Kingdom, prepared to conduct a terrorist attack in Manchester in mid-April 2009. Naseer and the others purchased ingredients and components for explosives, conducted reconnaissance at potential target locations, transported reconnaissance photographs back and forth to Pakistan, and maintained frequent contact with al-Qaeda leadership. Law enforcement disrupted the plot and arrested the subjects in April 2009.

U.S. v. Muhanad Mahmoud Al Farekh - On May 28, 2015, a grand jury returned a three-count indictment charging Al Farekh with conspiring to provide material support to terrorists, attempting to provide material support to terrorists, and providing material support to terrorists, all in violation of 18 U.S.C. § 2339A.

Al Farekh is alleged, along with two co-conspirators, to have entered into an agreement to travel from Winnepeg, Canada, where the three men were enrolled as students, to the Federally Administered Tribal Areas ("FATA") of Pakistan with the intention of training for violent jihad against U.S. personnel operating in Afghanistan. The men discussed jihad and viewed videos encouraging violence, including lectures by the now-deceased al-Qaeda leader Anwar al-Awlaki. The witnesses also observed the men making preparations for travel that included liquidating assets and purchasing gear such as mountain boots. In March 2007, the three men traveled to Karachi, Pakistan using round trip tickets with tourist visas. The return tickets were never used, and to date, there is no record that either Al Farekh or his co-conspirators lawfully re-entered the United States or Canada. Additionally, two cooperating witnesses who traveled to the FATA to fight violent jihad and join al-Qaeda in Spring of 2008 indicate that they received weapons training at an al-Qaeda training camp in the FATA from one of Al Farekh's co-conspirators.

*U.S. v. Khatallah ("*Benghazi*")* – Ahmed Abu Khatallah faces charges in the District of Columbia for the terrorist attack on the United States Special Mission in Benghazi, Libya, on September 11, 2012, and a second attack the following day at a nearby U.S. facility known as the Annex. The attacks resulted in the deaths of four American citizens: U.S. Ambassador to Libya J. Christopher Stevens and Information Management Officer Sean Patrick Smith at the Special Mission, and Security Officers Tyrone Snowden Woods and Glen Anthony Doherty at the Annex. Khatallah was arrested on June 28, 2014, on a sealed indictment.

On October 14, 2014, a nineteen-count superseding indictment was returned against Khatallah, charging him for various offenses stemming from the attacks, to include: murder of an international protected person, in violation of 18 U.S.C. §§ 1116 and 1111; murder of an officer and employee of the United States, in violation of 18 U.S.C. §§ 1114 and 1111, 2; attempted murder of an officer and employee of the United States, in violation of 18 U.S.C. §§ 1114 and 1113; killing a person in the course of an attack on a federal facility involving the use of a firearm and dangerous weapon, in violation of 18 U.S.C. §§ 939(c) and 1111; maliciously damaging and destroying U.S. property by means of fire and an explosive causing death, in violation of 18 U.S.C. §§ 844(f)(1) & (3); and various other weapons, terrorism, and destruction of property charges, in violation of 18 U.S.C. §§ 924(c); 2339A; and 1363. On August 3, 2015, Khatallah filed various motions to dismiss the superseding indictment alleging lack of extraterritorial jurisdiction and that the charges are unconstitutionally vague and overbroad, among other things. A trial date has not yet been scheduled.

U.S. v. Hamidullin – On December 3, 2015, Irek Ilgiz Hamidullin, a Russian national, was sentenced in the Eastern District of Virginia to life imprisonment for his role in a November 29, 2009, attack against Camp Leyza, an Afghan Border Police camp in Khowst province. He received an additional thirty years for a related weapons charge. On November 29, 2009, Hamidullin planned and carried out the attack with a group of insurgents. He had previously communicated with Sirajuddin Haqqani, a leader of Taliban insurgents in and around Khowst Province in Afghanistan, and a commander of the Haqqani Network, to select a target to attack in Afghanistan. He conducted reconnaissance of Camp Leyza and developed a plan of attack. He obtained weapons (including heavy machine guns and a rocket propelled grenade launcher) and ammunition for use in the attack and was the commander of the insurgent group that carried out the attack. Hamidullin was charged in a 12 count indictment in the Eastern District of Virginia with conspiracy to provide material support to terrorists, providing material support to terrorists, conspiracy and attempt to destroy an aircraft of the armed forces of the United States, conspiracy and attempt to kill an officer or employee of the United States or a person assisting such officer or employee, conspiracy and attempt to murder a national of the United States, engaging in physical violence with intent to cause bodily injury to a national of the United States, conspiracy to use a weapon of mass destruction, and possession of and conspiracy to possess a firearm in connection with a crime of violence. On August 7, 2015, in the Eastern District of Virginia, Richmond Division, Hamidullin was convicted by a federal jury of all fifteen counts charged against him.

U.S. v. Fazliddin Kurbanov – On August 12, 2015, in the District of Idaho, Kurbanov was convicted by a federal jury of counts one, three, and four charged against him in the superseding indictment. Count one charged Kurbanov with conspiracy to provide material support to a designated foreign terrorist organization, in violation of 18 U.S.C. § 2339B; count three charged him with possession of an unregistered firearm (a destructive device), in violation of 26 U.S.C. § 5861(d); and count four charged him with attempting to provide material support to a designated foreign terrorist organization, in violation of 18 U.S.C. § 2339B. On January 7, 2016, Kurbanov was sentenced to 25 years' imprisonment and 3 years of supervised release.

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.

US v. Ferizi - On October 6, 2015, in the Eastern District of Virginia, a sealed complaint was filed against Ardit Ferizi, also known by the online moniker "Th3Dir3ctorY," charging him with one count of providing material support to ISIL, in violation of 18 U.S.C. § 2339B, one count of accessing a protected computer without authorization, in violation of 18 U.S.C. § 1030, and one count of aggravated identity theft, in violation of 18 U.S.C. § 1028A.

Ferizi led a Kosovo-based hacking group and used his hacking skills to intrude into a United States company's server to steal more than 1,000 United States government employees' personally identifiable information (PII). Ferizi provided the PII to a known ISIL member, knowing that it would be used to attempt to harm government employees.

On August 11, 2015, the Islamic State Hacking Division, using the PII, published a "kill list" online and identified the names and home addresses of more than 1,000 United States government employees, including military and law enforcement personnel. The FBI investigation also revealed that Ferizi provided additional PII of Western individuals to another

ISIL member. On October 15, 2015 the criminal complaint was unsealed and extradition proceedings are ongoing.

US v. Marquez, Jr. - On Wednesday, December 30, 2015, in the Central District of California, a federal grand jury returned a five-count indictment against Enrique Marquez, Jr. ("Marquez") charging Marquez with the following: count one, conspiring to provide material support and resources to terrorists, in violation of 18 U.S.C. § 2339A(a); counts two and three, making a false statement in connection with acquisition of firearms from a licensed firearms dealer, in violation of 18 U.S.C. § 922(a)(6); count four, marriage fraud, in violation of 8 U.S.C. § 1325(c); and count five, participating in fraud and misuse of visas, permits, and other documents, in violation of 18 U.S.C. § 1546.

The conduct charged in the indictment relates to Marquez's involvement with Syed Rizwan Farook ("Farook"), the deceased male shooter from the December 2, 2015, shooting in San Bernardino, California. Marquez admitted to law enforcement that beginning in approximately 2011, Marquez and Farook began planning to commit terrorist acts by using firearms and explosives to attack Riverside Community College ("RCC") and State Route 91 ("SR-91"). Marquez and Farook took steps to carry out their plans by purchasing firearms, ammunition, and other tactical gear, as well as going to local firing ranges.

In late 2011 and early 2012, Marquez purchased firearms on two occasions from local sporting goods stores. Marquez admitted buying the rifles for Farook as a part of their plans to attack RCC and SR-91. Moreover, in 2012, Marquez purchased a bottle of smokeless powder for the purpose of making explosives with Farook for a future attack. In 2013, Marquez's and Farook's contact began to decline and according to Marquez they ceased planning any attacks together. Nevertheless, law enforcement has identified the two rifles Marquez purchased for Farook in 2011-2012 as being used in the December 2nd shooting. The black powder Marquez purchased for Farook was traced to the improvised explosive device found at the scene of the December 2nd shooting.

Additionally, the indictment alleges Marquez entered into a fraudulent marriage for the purpose of obtaining immigration benefits for a woman who was the sister of the wife of Farook's brother. Specifically, in July 2014, Marquez submitted documents to the Department of Homeland Security, United States Citizenship and Immigrations Services in which he submitted false statements to the effect that he lived with his sham wife, when, in truth, the sham wife was living with her boyfriend and young child that she had with the boyfriend. Marquez admitted, and financial records confirmed, that Marquez was paid $200.00 a month for this illegal activity.

FOREIGN TERRORIST FIGHTER 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. Juraboev, et al. – On February 25, 2015, three individuals – Abdurasul Juraboev, Akhror Saidakhmetov, and Abror Habibov – were arrested on a complaint out of the Eastern District of New York for attempting and conspiring to provide material support to a foreign terrorist organization, Islamic State in Iraq and the Levant ("ISIL"), in violation of 18 U.S.C. § 2339B. Saidakhmetov was arrested attempting to board a flight to Turkey at John F. Kennedy International Airport. From Turkey, Saidakhmetov had planned to travel onward to Syria to join ISIL. Juraboev, who was arrested at his residence that same night, had purchased an airline ticket to follow Saidakhmetov to Syria a few weeks later. Also arrested was Habibov, Saidakhmetov's employer, who had purchased Saidakhmetov's airline ticket and attempted to organize funding to assist him in joining ISIL. Juraboev and his co-conspirators initially came to the attention of the FBI after Juraboev made a posting on a pro-ISIL website offering his allegiance to ISIL and asking if he could commit a martyrdom action in the United States on their behalf by killing President Obama. Later, Juraboev decided that he would prefer to wage violent jihad on behalf of ISIL by fighting in Syria, and he and Saidakhmetov planned to travel there together.

On March 9, 2015, Juraboev, Saidakhmetov, and Habibov were charged in a four-count indictment. Each defendant was charged with one count of attempting and one count of conspiring to provide material support to a designated foreign terrorist organization, ISIL, in violation of 18 U.S.C. § 2339B. Saidakhmetov and Habibov were additionally charged with one count each of conspiring to use a firearm during and in relation to a crime of violence, in violation of 18 U.S.C. § 924(o), based on statements they made about purchasing a weapon for Saidakhmetov to use to fight in Syria. Finally, Saidakhmetov was charged with one count of travel document fraud, in violation of 18 U.S.C. § 1546, for making false statements in his application for a travel document to leave the United States for Turkey.

On April 6, 2015, the grand jury returned a superseding indictment charging an additional defendant, Dilkhayot Kasimov, with one count of attempting and one count of conspiring to provide material support to a designated foreign terrorist organization, ISIL, in violation of 18 U.S.C. § 2339B. The charges were based on Kasimov's activities on the night of Saidakhmetov's attempted travel, during which Kasimov met Saidakhmetov at the airport and delivered approximately $1,600 to Saidakhmetov before Saidakhmetov went through security. The money had been collected from numerous individuals by Habibov and Kasimov, and was intended for Saidakhmetov's use in Syria.

On June 8, 2015, the grand jury returned a third superseding indictment charging Akmal Zakirov with one count of attempting and one count of conspiring to provide material support to ISIL in violation of 18 U.S.C. § 2339B. These charges stemmed from Zakirov's attempts to raise funds to assist Saidakhmetov in his travel to Syria.

On August 14, 2015, Juraboev pled guilty to one count of 18 U.S.C. § 2339B, pursuant to a plea agreement. Juraboev faces a sentence of up to 15 years' incarceration.

U.S. v. Jordan, et al. – On 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. 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. Brown and Jordan both pled guilty pursuant to cooperation plea agreements, and sentencing has been rescheduled for both Jordan and Brown on March 8, 2016.

U.S. v. Hodzic, et al. – Abdullah Ramo Pazara left St. Louis in May 2013, and allegedly traveled to Syria to become a mujahideen and assist foreign fighters. While in Syria, Pazara communicated with six individuals through Facebook seeking financial support: Siki Ramiz Hodzic, Sedina Hodzic, Mediha Salkicevic, Jasminka Ramic, Armin Harcevic, and Nihad Rosic. Each of these individuals contributed financially by sending funds to Hodzic in St. Louis. The funds were then sent to a third-party intermediary overseas before reaching Pazara in Syria. Pazara also requested that Hodzic provide military supplies to him such as optics, firearms accessories, camouflage clothing, military boots and gloves. These supplies were sent to and received by Pazara in September 2013. Pazara died in September 2014. On February 6, 2015, a grand jury returned an indictment charging all six individuals with conspiracy and attempt to provide material support to terrorists, in violation of 18 U.S.C. § 2339A, based on their financial support to Pazara.

In addition to providing financial support, Siki Ramiz Hodzic also allegedly provided military tactical advice to Pazara and other foreign fighters, while Rosic made two attempts to travel to Syria to join Pazara and the foreign fighters. As such, Hodzic and Rosic are also charged with conspiracy to kill and maim persons in a foreign country, in violation of 18 U.S.C. § 956. Prior to his death in September 2014, Pazara bragged on various social networks about his success on the battlefield to include killing numerous individuals and being present at the beheadings of the two American journalists. The case remains ongoing.

U.S. v. Hamza Naj Ahmed - On May 18, 2015, in the District of Minnesota, a federal grand jury returned a superseding indictment in the case of *United States v. Hamza Naj Ahmed,* adding six new defendants. Based on Ahmed's attempt to leave the United States in early November 2014, along with others from Minneapolis, with a goal of traveling to Syria to fight for ISIL, Ahmed was originally charged in a February 19, 2015, indictment with conspiracy to provide material support to ISIL in violation of 18 U.S.C. § 2339B; attempt to provide material support to ISIL in

violation of 18 U.S.C. § 2339B; and providing a false statement to FBI agents in violation of 18 U.S.C. § 1001.

The nine-count, superseding indictment adds six new defendants to the conspiracy charge: Mohamed Farah, Adnan Farah, Abdirahman Daud, Zacharia Abdurahman, Hanad Musse, and Guled Omar**.** The superseding indictment also adds new charges of attempt to provide material support to ISIL against Mohamed Farah, Daud, Omar, Musse, and Abdurahman related to attempts the defendants made to travel to Syria to fight for ISIL; an additional false statement charge against Mohamed Farah concerning his failed attempt to leave the United States in November 2014; and individual counts of federal financial aid fraud against Mohamed Farah and Musse, who partially financed their abortive trips with student loan funds, in violation of 20 U.S.C. § 1097(a).

The six newly-added defendants were arrested on April 19, 2015, outside San Diego, California (Mohamed Farah and Daud), and in Minneapolis (Adnan Farah, Omar, Musse, and Abdurahman) on a federal criminal complaint which alleged conspiracy and attempt to provide material support to ISIL, and false statements to FBI agents. At the time of their April arrest, Mohamed Farah and Daud had driven from Minneapolis to San Diego to obtain bogus United States passports which they intended to use to facilitate travel to Syria.

Two defendants, Hanad Musse and Zacharia Abdurahman, have entered guilty pleas in September 2015 to charges of conspiracy to provide material support to ISIL, in violation of 18 U.S.C. § 2339B. Trial is set for March 2016.

U.S. v. Elhuzayel, and Badawi – On June 3, 2015, in the Central District of California, an indictment was returned charging Muhanad Badawi and Nader Elhuzayel with one count of conspiring to provide material support and resources to the Islamic State of Iraq (ISIL), a designated Foreign Terrorist Organization (FTO), in violation of 18 U.S.C. § 2339B. Additional counts to the indictment charge Elhuzayel with one count of attempting to provide material support, namely himself, to ISIL, in violation of 18 U.S.C. § 2339B; and charge Badawi with one count of aiding, counseling, commanding, inducing, and procuring Elhuzayel to attempt to provide material support to ISIL, in violation of 18 U.S.C. §§ 2339B and 2. Badawi and Elhuzayel used social media to discuss ISIL and terrorist attacks, expressed a desire to die as martyrs and made arrangements for Elhuzayel to leave the United States to join ISIL. In recorded conversations, Badawi and Elhuzayel "discussed how it would be a blessing to fight for the cause of Allah, and to die in the battlefield," and they referred to ISIL as "we." The defendants discussed where in the Middle East they would rather be, and Elhuzayel said he wanted to fight and did not want to be in the United States. On May 7, Badawi purchased a one-way airline ticket for Elhuzayel to travel from Los Angeles to Tel Aviv, Israel, via Istanbul, Turkey, on a Turkish Airlines flight scheduled to depart on May 21. Badawi indicated that he would be traveling to the Middle East in the future. Elhuzayel was arrested at Los Angeles International Airport while waiting for his flight. Elhuzayel admitted, after being read his

Miranda rights, that, he planned to disembark in Istanbul to join ISIL and did not intend to travel on to Israel. Trial is set for June 2016.

CASES INVOLVING THE THREAT OF DOMESTIC TERRORISM AND/OR HOMEGROWN VIOLENT EXTREMISM

There have also been a number of as cases involving the threat of domestic terrorism, lone wolves, and homegrown violent extremism.

U.S. v. Cornell - On January 21, 2015, in Cincinnati, Ohio, Christopher Lee Cornell, a/k/a, Raheel Mahrus Ubaydah, was charged by a federal grand jury in a three count Indictment with attempting to kill employees and officers of the United States, in violation of 18 U.S.C. § 1114, solicitation of a crime of violence, in violation of 18 U.S.C. § 373, and possessing firearms in furtherance of an attempted crime of violence, in violation of 18 U.S.C. § 924(c). Cornell devised a plan to assault the United States Capitol during the State of the Union Address in an effort to murder United States Congressional Representatives and other officers and employees of the United States. He planned to detonate pipe bombs in front of the Capitol, both as a diversionary tactic and to kill guards, followed by an assault on the Capitol itself with rifles. On January 14, 2015, in furtherance of the aforementioned plan, Cornell purchased two Armalite Inc., Model M-15, 5.56mm, semi-automatic rifles and approximately 600 rounds of ammunition from a firearms store located in Cincinnati, Ohio. Cornell planned to transport these weapons to Washington, D.C. and use them to attack the Capitol in a manner similar to a recent attack on the Canadian Parliament. Cornell was arrested by the FBI in Ohio immediately after he purchased the weapons and ammunition.

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. On June 8, 2015, Loewen pled guilty to attempted use of a weapon of mass destruction, in violation of 18 U.S.C. § 2332a. On August 31, 2015, he was sentenced to 20 years' imprisonment and a lifetime of supervised release pursuant to his plea agreement.

BIOLOGICAL TOXIN/DOMESTIC TERRORISM CASES:

There has also been an increase in cases involving biological toxins, such as ricin. Below is a sampling of these cases:

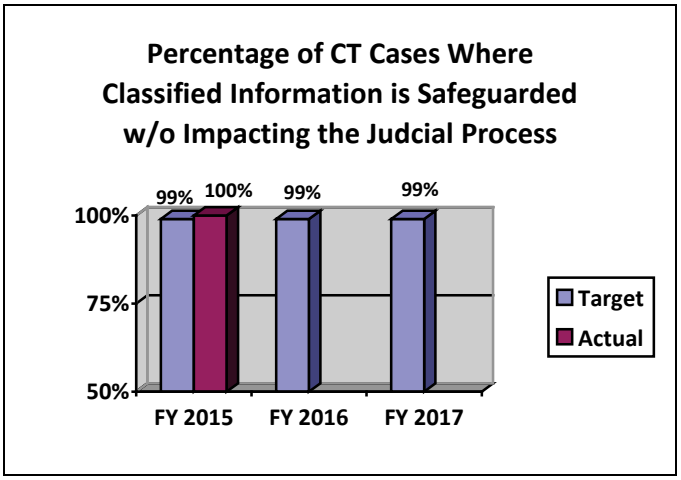
U.S. v. Korff – On February 18, 2015, in the District of New Jersey, Jesse Korff was sentenced to 110 months' imprisonment. On August 12, 2014, Korff pleaded guilty to an information charging him with five counts of developing and transferring a biological toxin (abrin), in violation of 18 U.S.C. § 175(a); 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. After Korffe's conviction on January 12, 2015, the defendant filed a notice of appeal on January 23, 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 ricin for use as a weapon – namely, that he: 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. After the jury verdict, the defendant moved for acquittal on the basis of *Bond v. United States*, A Supreme Court case limiting the application of the closely-related chemical weapons statute, decided on June 2, 2014. On September 19, 2014, the court rejected the *Bond* challenge. On September 29, 2014, he was sentenced to 72 months' imprisonment, and on October 9, 2014, he filed notice of appeal in Sixth Circuit of Appeals. Briefing of the appellate case was completed June 8, 2015. On November 12, 2015, the Sixth Circuit (Merritt, Daughtrey, Griffin) affirmed the conviction of Jeff Boyd Levenderis for one count of possessing a biological weapon, in violation of 18 U.S.C. § 175(a), and two counts of making false statements to federal agents, in violation of 18 U.S.C. § 1001(a)(2).

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). Adams was found not guilty of a third count, attempted production of a biological toxin (ricin) for use as a weapon, also in violation 18 U.S.C. § 175(a). 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. Two other MoG members previously pleaded guilty and were sentenced. On November 24, 2014, notice of appeal was filed on behalf of Crump. On July 6, 2015, Crump's conviction was affirmed by the Eleventh Circuit.

Measure: **Percentage of CT Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2015 Target: 99%
FY 2015 Actual: 100%
FY 2016 Target: 99%
FY 2017 Target: 99%
Discussion: The FY 2017 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).



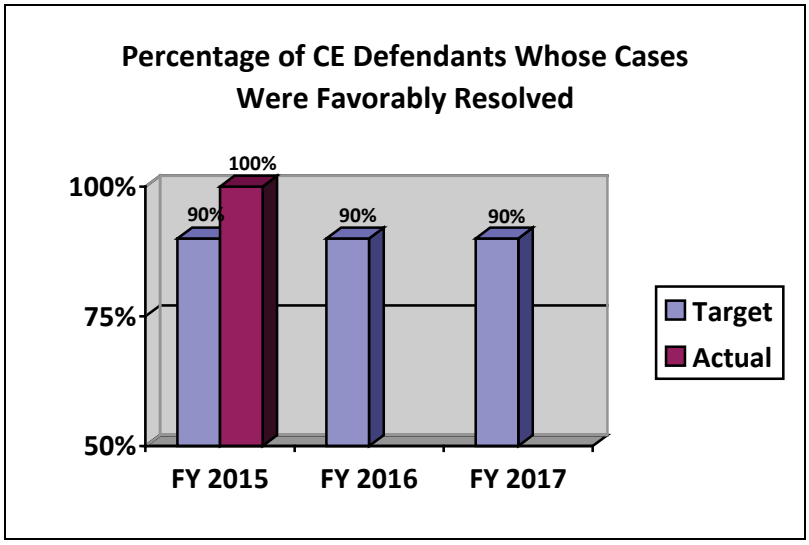
Data Definition: Classified information - information that has been determined by the U.S. Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data as defined by the Atomic Energy 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 2015 Target: 90%
FY 2015 Actual: 100%
FY 2016 Target: 90%
FY 2017 Target: 90%
Discussion: The FY 2017 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 Counterintelligence and Export Control Prosecutions

Navy Engineer Sentenced for Attempted Espionage – On October 15, 2015, in the Eastern District of Virginia, Mostafa Ahmed Awwad was sentenced to 132 months in prison. On June 15, 2015, Awwad had pleaded guilty to a criminal information charging him with attempted espionage. Awwad attempted to provide schematics of the U.S. Navy's newest nuclear aircraft carrier, the USS Gerald R. Ford, to an individual he believed to be an Egyptian intelligence officer, but who was in fact an undercover FBI agent. Awwad began working for the Navy in February 2014 as a civilian engineer at the Norfolk Naval Shipyard. Based on a joint FBI/NCIS investigation, an undercover FBI agent contacted Awwad by telephone in September 2014 and asked to meet him. The next day, Awwad met with the undercover FBI agent, who was posing as an Egyptian intelligence officer. During the meeting, Awwad claimed it was his intention to utilize his position with the U.S. Navy to obtain military technology for use by the Egyptian Government, including the designs of the new Navy "supercarrier." Several times before he was arrested, Awwad met with the undercover agent and provided schematics of the USS Gerald R. Ford in exchange for cash.

Unlawful Services in Iran and Sudan – On April 30, 2015, in the District of Columbia, Schlumberger Oilfield Holdings, Ltd. (SOHL) pleaded guilty to a conspiracy to violate the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1705, the Iranian Transactions Regulations, 31 C.F.R. Part 560, and the Sudanese Sanctions Regulations, 31 C.F.R. Part 538. Consistent with the plea agreement, SOHL was sentenced to the maximum criminal fine of $155,138,904 and a three-year period of corporate probation. In addition to the criminal fine, SOHL is required to pay a criminal forfeiture amount of $77,569,452. The criminal fine represents the largest criminal fine in connection with an IEEPA prosecution. In addition to SOHL's agreement to continue its cooperation with U.S. authorities throughout the three-year period of probation and not to engage in any felony violation of U.S. federal law, SOHL's parent company, Schlumberger Ltd., also has agreed to continue its cooperation with U.S. authorities during the three-year period of probation, withdraw its operations from Iran and Sudan, and hire an independent consultant who will review the parent company's internal sanctions policies, procedures and company-generated sanctions audit reports. Starting in or about early 2004 and continuing through June 2010, Drilling & Measurements (D&M), a U.S.-based Schlumberger business segment, provided oilfield services to Schlumberger customers in Iran and Sudan through non-U.S. subsidiaries of SOHL.

WMD Materials to North Korea – On April 24, 2015, Yueh-Hsun Tsai, a.k.a. "Gary Tsai", was sentenced in the Northern District of Illinois to 3 years of probation and a fine of $250. On March 16, 2015, Hsien Tai Tsai, a.k.a. "Alex Tsai", was sentenced to 2 years imprisonment and $100 special assessment. Previously, on October 10, 2014, Alex Tsai pleaded guilty to conspiracy to defraud the U.S. in its enforcement of regulations targeting proliferators of weapons of mass destruction. On December 16, 2014, his son, Gary Tsai, pleaded guilty to a superseding information charging him with making a false bill of lading. Each was charged with conspiring to defraud the U.S. in its enforcement of laws prohibiting the proliferation of weapons of mass destruction; conspiracy to violate the International Emergency Economic Powers Act

(IEEPA) by conspiring to evade the restrictions imposed on Alex Tsai and two of his companies by the U.S. Treasury Department, and money laundering. On January 16, 2009, the Treasury Department designated Alex Tsai, Global Interface, and Trans Merits as proliferators of weapons of mass destruction, isolating them from the U.S. financial system and prohibiting any U.S. person or company from doing business with them. The Treasury Department asserted that Alex Tsai "has been supplying goods with weapons production capabilities to KOMID and its subordinates since the late 1990s, and he has been involved in shipping items to North Korea that could be used to support North Korea's advanced weapons program."

Former Los Alamos National Laboratory Scientist Sentenced for Atomic Energy Act Violations – On January 28, 2015, in the District of New Mexico, Pedro Leonardo Mascheroni was sentenced to 60 months in prison for Atomic Energy Act and other violations relating to his communication of classified nuclear weapons data to a person he believed to be a Venezuelan government official. Mascheroni formerly was employed as a scientist at the Los Alamos National Laboratory from 1979 to 1988 and held a security clearance that allowed him access to certain classified information. In his plea agreement, Mascheroni admitted that in November 2008 and July 2009 he unlawfully communicated restricted data to another individual with reason to believe that the data would be utilized to secure an advantage to Venezuela. He also admitted to unlawfully converting Department of Energy information to his own use and selling the information, as well as failing to deliver classified information relating to U.S. national defense to appropriate authorities and instead unlawfully retaining the information in his home. Finally, Mascheroni admitted to making materially false statements when he was interviewed by the FBI.

Sanctions Violations to Aide Zimbabwean Government Officials – On January 21, 2015, C. Gregory Turner, also known as Greg Turner, was sentenced in the Northern District of Illinois to 15 months in prison, one year supervised release, $100 special assessment, and received an abstract of judgment in the amount of $90,000. Previously, on October 10, 2014, Turner was convicted by a federal jury of conspiracy to violate the International Emergency Economic Powers Act (IEEPA) from late 2008 through early 2010 by agreeing to assist Zimbabwe President Robert Mugabe and others in an effort to lift economic sanctions against Zimbabwe. Turner met multiple times in the U.S. and in Africa with Zimbabwean government officials, including President Mugabe and Gideon Gono, governor of the Reserve Bank of Zimbabwe, who were individually subject to U.S. sanctions. A November 2008 consulting agreement provided for a total payment of $3.4 million in fees for Turner and his co-defendant, Prince Asiel Ben Israel, to engage in public relations, political consulting, and lobbying efforts to have sanctions removed by meeting with and attempting to persuade federal and state government officials, including Illinois members of Congress and state legislators, to oppose the sanctions. Ben Israel was sentenced on August 21, 2014 to seven months in prison, one year supervised release, $100 special assessment and a $500 fine after pleading guilty to violating the Foreign Agents Registration Act (FARA).

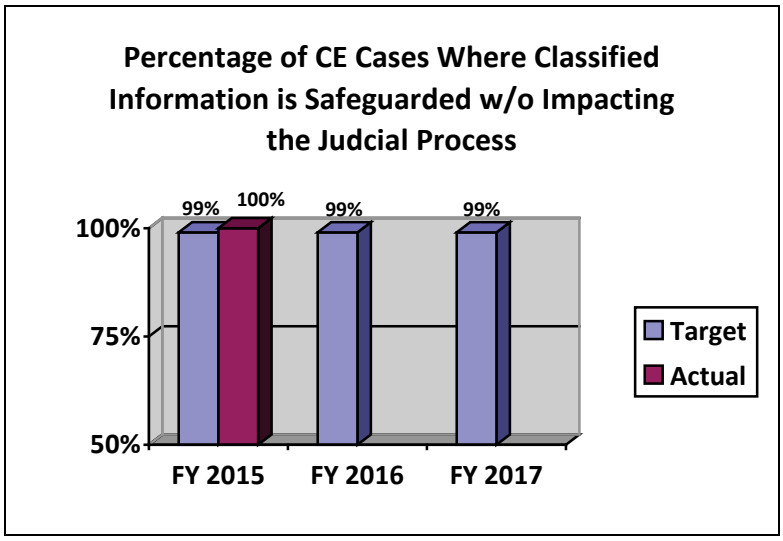
Drone, Missile and Stealth Technology to China – On January 9, 2015, Hui Sheng Shen, a.k.a. "Charlie," was sentenced in the District of New Jersey to 49 months in prison and $200 special assessment. On January 6, 2015, Huan Ling Chang, a.k.a. “Alice,” was sentenced to time served

and $200 special assessment. Previously, on September 22, 2014, Shen and Chang, both Taiwanese nationals, each pleaded guilty to one count of conspiracy to violate the Arms Export Control Act and one count of conspiracy to import illegal drugs. On April 25, 2012, Shen and Chang were charged separately by amended criminal complaints with conspiracy to violate the Arms Export Control Act. The defendants were arrested on February 25, 2012 in New York in connection with a complaint in New Jersey charging them with conspiring to import and importing crystal methamphetamine from Taiwan to the U.S. According to the amended complaint, during negotiations with undercover FBI agents over the meth deal, the defendants asked FBI undercover agents if they could obtain an E-2 Hawkeye reconnaissance aircraft for a customer in China. In subsequent conversations, Shen and Chang allegedly indicated they were also interested in stealth technology for the F-22 fighter jet, as well missile engine technology, and various Unmanned Aerial Vehicles (UAV), including the RQ-11b Raven, a small, hand-launched UAV used by the U.S. Armed Forces. Shen and Chang allegedly stated that their clients were connected to the Chinese government and its intelligence service.

DuPont Trade Secrets to China / U.S. v. Liew et al. – On October 1, 2015, in the Northern District of California, Christina Liew was sentenced to three years of probation, fined $25,000, and ordered to pay more than $6 million restitution for her role in one of the largest economic espionage cases in history. In May 2015 Christina Liew had pleaded guilty to conspiracy to tamper with evidence.

In March of 2014, a jury had 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. On July 11, 2014, defendant Walter Liew (Christina's husband) was sentenced to 180 months in prison and ordered to pay $500,000 restitution. Defendant Robert Maegerle was sentenced in August 2014 to 30 months in prison and $367,000 restitution. Corporate defendant USAPTI was sentenced to 5 years of probation and fined $18.9 million. According to a March 2013 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.

Measure: **Percentage of CE Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2015 Target: 99%
FY 2015 Actual: 100%
FY 2016 Target: 99%
FY 2017 Target: 99%
Discussion: The FY 2017 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).



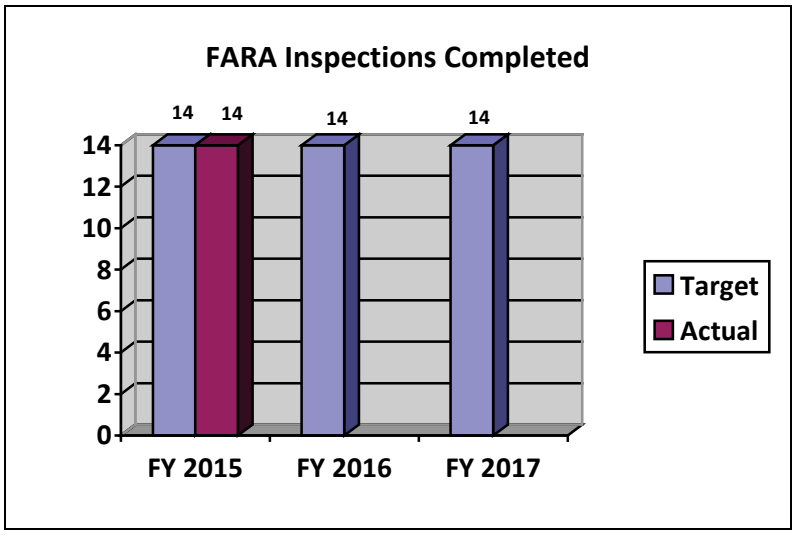
Data Definition: Classified information - information that has been determined by the United State Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data as defined by the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

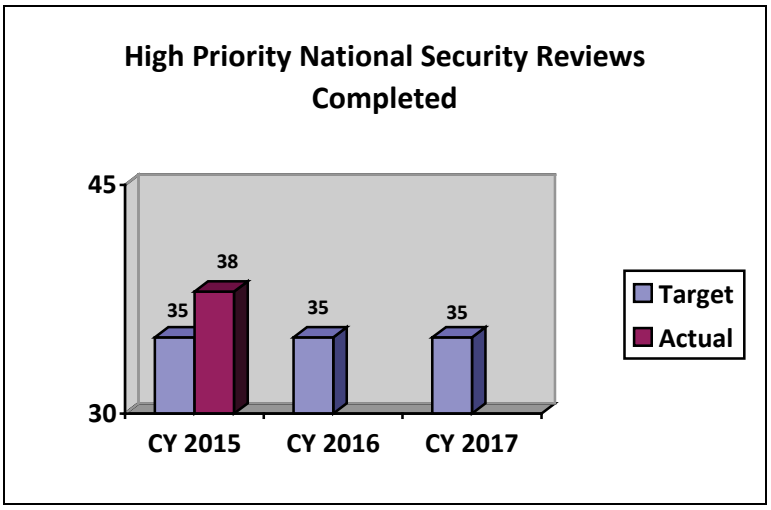
Data Limitations: Reporting lags.

Measure: FARA Inspections Completed
FY 2015 Target: 14
FY 2015 Actual: 14
FY 2016 Target: 14
FY 2017 Target: 14
Discussion: The FY 2017 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 2015 Target: 30
CY 2015 Actual: 38
CY 2016 Target: 35
CY 2017 Target: 35
Discussion: The CY 2017 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.

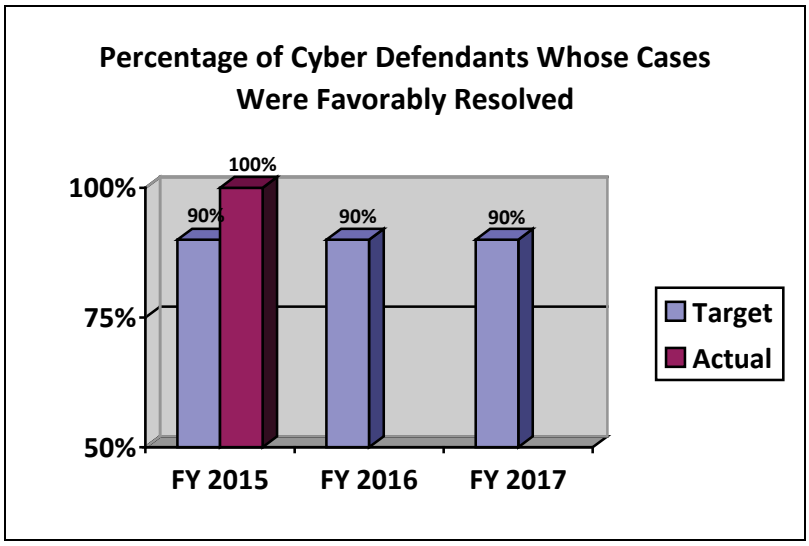
Data Collection and Storage: Data is collected manually and stored in generic files; however management is reviewing the possibility of utilizing a modified automated tracking system.

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 2015 Target: 90%
FY 2015 Actual: 100%
FY 2016 Target: 90%
FY 2017 Target: 90%
Discussion: The FY 2017 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

Iranian National Pleads Guilty to Facilitating Computer Hacking – On December 2, 2015, in the District of Vermont, Iranian national Nima Golestaneh pleaded guilty to charges of wire fraud and unauthorized access to computers related to his involvement in the hacking of a Vermont-based engineering consulting and software company. According to the plea agreement, Golestaneh conspired with others to hack network computers in order to steal valuable company software and business information. Golestaneh's role in the conspiracy was to acquire servers in other countries for his co-conspirators to use remotely in order to launch computer intrusions into victim companies, thereby masking their true location and identity. On February 13, 2015, Golestaneh was arraigned during his first appearance on a six-count indictment charging him with four counts of wire fraud, and one substantive and one conspiracy count each of unauthorized theft of information from a protected computer. In December 2013, Golestaneh was arrested on a complaint in Turkey, and indicted later that same month. He was extradited to the United States on February 12, 2015.

Former Defense Contractor Sentenced for Accessing and Removing Classified Information from Military Computers – On July 31, 2015, in the Southern District of Florida, Christopher R. Glenn, a former cleared military contractor, was sentenced to 120 months in prison. In January

2015, Glenn had pleaded guilty to a computer intrusion to obtain national defense information, willful retention of national defense information, and conspiracy to commit naturalization fraud. While employed as a computer systems administrator at a U.S. military installation in Honduras, Glenn obtained unauthorized access to a classified Department of Defense (DoD) network and removed classified national defense files from DoD and U.S. Southern Command's Joint Task Force - Bravo, including intelligence reports and military plans. Glenn proceeded to encrypt the files and place them on an Internet-accessible network storage device located in his Honduras residence. Glenn also conspired with his wife to commit naturalization fraud for her benefit by fabricating fraudulent documents and submitting false statements and documents to U.S. Citizenship and Immigration Services.

Former U.S. Nuclear Regulatory Commission Employee Charged with Attempted Spear-Phishing Cyber-Attack on Department of Energy Computers – On May 8, 2015, in the District of Columbia, Charles Harvey Eccleston, a former employee of the U.S. Department of Energy and the U.S. Nuclear Regulatory Commission (NRC), was indicted on four felony offenses in connection with an attempted e-mail "spear-phishing" attack targeting dozens of Department of Energy employee e-mail accounts. According to the indictment, the goal of the attack was to cause damage to the computer network of the Department of Energy through a computer virus that Eccleston believed was being delivered to particular department employees through e-mails; and to extract sensitive, nuclear weapons-related government information that Eccleston believed would be collected by a foreign country. The indictment includes three counts of crimes involving unauthorized access of computers and one count of wire fraud.

U.S. Charges Chinese National in Hacking Scheme to Steal U.S. Military Technology – On March 5, 2015, in the Central District of California (CDCA), Su Bin a.k.a. Stephen Su, a citizen of the People's Republic of China, was charged in a superseding indictment with unauthorized access to computers, violating the Arms Export Control Act, and conspiring to steal trade secrets from U.S. defense contractors. On June 28, 2014, Su had been arrested in Canada based on a complaint filed in the CDCA alleging that he worked with unnamed co-conspirators to steal U.S. military technology. Su subsequently was extradited from Canada. The indictment described how Su worked with two unindicted co-conspirators based in China to infiltrate computer systems and obtain confidential information about military programs, seeking files that had value and in one instance information that could be sold to a state-owned Chinese aviation company. It is alleged that Su and his co-conspirators sought and obtained data related to the C-17 transport aircraft, F-35 fighter jet, F-22 fighter jet, and at least thirty other military technologies or projects.

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. NSD takes a strategic, threat-driven, and all-tools approach to disrupting national security threats. 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 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 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, 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.

B. Priority Goals (Not Applicable)

NSD is assisting with DOJ's efforts to meet its FY 2016 – FY 2017 Cyber Priority Goals through the disruption of cyber threat actors and the dismantlement of their networks. Specifically, NSD tracks data that relates to the following one indicator and two milestones.

Indicator: Number of actions taken in support of disrupting or dismantling national security actors and/or networks.

Milestone: Support non-prosecution disruption tools with FBI investigations and DOJ legal support and information sharing, as appropriate (e.g., Treasury sanctions, Commerce designations, and diplomatic engagements, deterrence/avoidance). In FY 2016 and FY2017, NSD and the Criminal Division (CRM) will promote the use of these alternate tools to USAOs and increase cross-government communication and collaboration through interagency working groups and training efforts.

Milestone: Increase outreach efforts to FBI field offices, USAOs, victims, and targeted private and public sector entities in order to raise criminal and national security cyber threat awareness, build partnerships, and promote enhanced network defenses in order to disrupt and deter national security and criminal cyber threats. In FY2016 and FY2017, CRM and NSD will develop and disseminate investigative guidance, success stories and lessons learned to increase victim willingness to cooperate in investigations and disruptions.

VII. Exhibits