FY 2018
Performance Budget
Congressional Justification

NATIONAL SECURITY DIVISION

Protecting the United States from Threats to Our National Security by Pursuing Justice Through the Law

Table of Contents

I. Overview 1

II. Summary of Program Changes 10

III. Appropriations Language and Analysis of Appropriations Language 10

IV. Program Activity Justification 11
National Security Division
1. Program Description 11
2. Performance Tables 14
3. Performance, Resources, and Strategies 17

V. Program Increases by ..... NA

VI. Program Offset by Item ..... NA

VII. Exhibits .....

A. Organizational Chart
B. Summary of Requirements
C. FY 2018 Program Increases/Offsets by Decision Unit (Not Applicable)
D. Resources by DOJ Strategic Goal/Objective (Not Applicable)
E. Justification for Technical and Base Adjustments
F. Crosswalk of 2016 Availability
G. Crosswalk of 2017 Availability
H. Summary of Reimbursable Resources
I. Detail of Permanent Positions by Category
J. Financial Analysis of Program Changes (Not Applicable)
K. Summary of Requirements by Object Class
L. Status of Congressionally Requested Studies, Reports, and Evaluations (Not Applicable)
M. Senior Executive Service Reporting (Not Applicable)

I. Overview for National Security Division

A. Introduction

The National Security Division (NSD) works to protect this Nation's citizens against acts of terrorism, the Department of Justice's (DOJ's) top priority. To maintain current services only, as reflected more fully in the justification that follows, NSD requests for FY 2018 a total of 362 positions (including 243 attorneys), 362 FTE, and $101,031,000.[1]

B. Background

NSD has outlined five areas of continued focus that will guide its operations in the coming years. NSD will continue to:

- Prevent, disrupt, and defeat terrorist operations before they occur by integrating intelligence and law enforcement efforts to achieve a coordinated all tools response to terrorist threats;
- Prosecute those involved in terrorist acts, adapting investigations to address changing terrorism threats, including homegrown violent extremism and cyber-enabled terrorism;
- Protect national assets from nation-state and terrorist threats, including through investigating, prosecuting, and disrupting espionage activity, proliferation, and foreign investment threats; and strengthening partnerships with potential targets of intelligence intrusions;
- Combat national security cyber-based threats and attacks through the use of all available tools, strong public-private partnerships, and by investigating and prosecuting cyber threat actors; and
- Ensure that IC agencies have the legal tools necessary to conduct intelligence operations while safeguarding privacy and civil liberties.

Division Structure

NSD is designed to ensure coordination and unity of purpose between prosecutors and law enforcement agencies on the one hand, and intelligence attorneys and the Intelligence Community (IC) on the other, thus ensuring the effectiveness of the federal government's national security efforts. The NSD is comprised of the:

- Office of Intelligence (OI);
- Counterterrorism Section (CTS);
- Counterintelligence and Export Control Section (CES);
- Office of Law and Policy (L&P);
- Foreign Investment Review Staff (FIRS);
- Office of Justice for Victims of Overseas Terrorism (OVT)

[1] Within the totals outlined above, NSD has included a total of 18 positions, 18 FTE, and $16,313,000 for Information Technology (IT).

NSD Major Responsibilities

Intelligence Operations, Oversight, and Litigation

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

Counterterrorism

- Promoting and overseeing a coordinated national counterterrorism enforcement program, through close collaboration with Department leadership, the National Security Branch of the FBI, the IC, and the 94 United States Attorneys' Offices (USAOs);
- Developing national strategies for combating emerging and evolving terrorism threats, including the threat of cyber-based terrorism;
- Overseeing and supporting the National Security 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, training, and collaborating with prosecutors nationwide on international and domestic terrorism investigations, prosecutions, and appeals, including the use of classified evidence through the application of the Classified Information Procedures Act (CIPA);
- Sharing information with and providing advice to international prosecutors, agents, and investigating magistrates to assist in addressing international threat information and litigation initiatives; and
- Managing DOJ's work on counter-terrorist financing programs, including supporting the process for designating Foreign Terrorist Organizations and Specially Designated Global Terrorists, as well as staffing U.S. Government efforts on the Financial Action Task Force.

Counterintelligence and Export Control

- Developing, 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;

- Coordinating, developing, and supervising investigations and national strategies for combating the emerging and evolving threat of cyber-based espionage and state-sponsored cyber intrusions;
- Coordinating, developing, and supervising 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, developing, and supervising 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;
- Coordinating with interagency partners the use of all tools to protect our national assets, including use of law enforcement tools, economic sanctions, and diplomatic solutions; and
- Conducting corporate and community outreach relating to cyber security and other issues relating to the protection of our national assets.

Policy and Other Legal Issues

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

Foreign Investment

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

- Tracking and monitoring certain transactions that have been approved pursuant to this process; and
- In coordination with law enforcement and IC partners, conducting community outreach and corporate engagement relating to national security issues.

Victims of Terrorism

- Ensuring that the rights of victims of overseas terrorism and their families are honored and respected, and that they are supported and informed during the criminal justice process.

NSD Recent Accomplishments (unclassified selections only)

- Responding to the evolving threat posed by the Islamic State in Iraq and ash-Sham (ISIS), we have charged over 100 individuals for ISIS-related conduct and have obtained over 60 convictions as of March 2017. We have also brought dozens of charges against other foreign terrorist fighters and homegrown violent extremists.
- Between March 2013 and March 2017, we publicly charged more than 120 individuals, in over 35 districts, for foreign terrorist fighter or homegrown violent extremist (HVE)-related conduct.
- We continued to lead the nation's counterterrorism efforts through collaboration with Department leadership, the FBI, the IC, the USAOs, and other federal agencies.
- We successfully brought charges in a number of complex national security cyber cases, including the indictment of officers of the Russian Federal Security Service in connection with the 2014 hack into the network of Yahoo – one of the largest data breaches in U.S. history – as well as the indictment of Iranian hackers affiliated with the Islamic Revolutionary Guard Corps for cyber attacks against the U.S. financial sector, and charges against members of the Syrian Electronic Army for conspiracies related to computer hacking, among others.
- Continued to support the IC by seeking authority under FISA with the FISC.
- Developed comprehensive Attorney General-approved procedures for four IC components – the Department of Defense, the Central Intelligence Agency, the Department of Homeland Security Office of Intelligence and Analysis, and the Department of Energy – regarding the collection, retention, and dissemination of information concerning United States persons.
- Designated a total of 273 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 and corporate engagement relating to NSD's efforts to assess and counter national security threats by foreign investment in national assets, as well as corporate engagement relating to NSD's broader efforts to protect national assets.

C. Full Program Costs

The NSD has a single decision unit. Its program activities include intelligence, counterterrorism, counterintelligence and export control, and cyber security. 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.

The charts below represent the percentage of costs by program activity for FY 2018.

D. Performance Challenges

NSD recognizes that this is a challenging federal budget climate but continues to assert that additional resources are needed to address the threats facing this nation. Protecting the Nation's citizens against acts of terrorism is the top priority for the Department, and NSD's work is critical to that mission. As threats continue to grow and evolve, the challenges NSD must overcome also continue to increase and so does the need for additional resources. These challenges include:

1. The changing terrorism threat: The terrorism threat continues to become increasingly diverse and decentralized – as the world has made progress against core al Qaeda, the Islamic State in Iraq and ash-Sham (ISIS) 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. 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 FBI has conducted investigations of such individuals in all 50 states. The U.S. also faces numerous threats as a result of domestic terrorism, including acts of terrorism by disparate groups that pose special investigative challenges.

   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 homegrown violent extremists (HVEs), who – although they do not necessarily have any direct ties to ISIS, al Qaeda or any other foreign terrorist organization – reside or operate in the U.S. and become inspired by ISIS, al Qaeda or similar groups through social media and English-language propaganda.

The 2016 Worldwide Threat Assessment of the US Intelligence Community describes the evolving and emerging threat of terrorism, noting that "[t]he United States and its allies are facing a challenging threat environment in 2016" and that "Sunni violent extremism has been on an upward trajectory . . . and has more groups, members, and safe havens than at any other point in history." At the same time, and perhaps most alarming, we are witnessing a surge in HVEs – individuals inspired by this extremist ideology to conduct attacks inside the United States. In total, between March 2013 and March 2017, we publicly charged more than 120 individuals, in over 35 districts, for foreign terrorist fighter or HVE-related conduct.

The terrorism threat is also evolving, requiring NSD to confront novel threats while it continues to disrupt traditional ones. For example, over the past two year, we have seen first-of-their-kind cases in which terrorists are using the Internet and social media as part of conspiracies to steal personal identifying information and disseminate it online, for the purpose of soliciting the murder of or encouraging terrorist attacks against U.S. persons. We expect these kinds of blended threats—converging once-unrelated counterterrorism and cyber cases—to grow in number. Similarly, terrorists and other criminals increasingly use technology, including encryption, to conceal their crimes and hide from government detection. This poses serious challenges for public safety, and adds significant burdens on law enforcement and intelligence investigations to attempt to mitigate the loss of lawful access to information.

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.

2. <u>The recent recognition of increasing and changing threats to our national assets, including significant growth of cyber threats to the national security</u>: A top priority for NSD is the protection of national assets through counterintelligence investigations and prosecutions, enforcement of export controls and sanctions, and cyber-related investigations and prosecutions. The theft of trade secrets and other intellectual property by or for the benefit of foreign entities is an increasingly acute and costly threat to U.S. national and economic security. Foreign governments and other non-state adversaries of the United States are also engaged in an aggressive campaign to acquire superior technologies and commodities that are developed in the United States, in contravention of our export control and sanctions laws. The threat our nation confronts increasingly consists not only of unlawful shipments and deliveries of physical commodities and equipment, but also the theft of proprietary information and export-controlled technology through cyber attacks and intrusions in their computer networks, as well as through insider threats. The most sophisticated of our adversaries employ multi-faceted campaigns to acquire valuable proprietary technologies through a combination of traditional and asymmetric approaches. For example, our nation-states adversaries increasingly rely on commercial and other non-state entities

to conduct economic espionage, creating a new threat vector that is especially difficult to investigate. Adequately addressing these threats requires a comprehensive, "all-tools" approach that leverages the full array of our options under existing legal authorities. NSD plays a central role in leading these efforts.

Likewise, NSD's foreign investment review work—including its review of filings before the Committee on Foreign Investment in the United States (CFIUS) and its review of foreign entities' license applications for provision of communications services before the Federal Communications Commission (through the so-called Team Telecom working group)—has also expanded to address the asymmetric threat. With respect to Team Telecom in particular, complex transactions and differences in evaluative priorities among agencies have prompted the Administration's desire to formalize this process with stricter timelines, an administrative chair, and other indicia of a structured interagency process. NSD's responsibilities will increase greatly in effectuating this formalization.

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.

3. An increasing workload in intelligence oversight, operations, and litigation, especially as relates to the 2015 USA Freedom Act and the upcoming consideration of reauthorization of Section 702 of the Foreign Intelligence Surveillance Act: NSD's intelligence-related work supports the U.S. Government's national security mission fully, including combating the threats posed by terrorists, threats to our nation's cybersecurity, and other threats. NSD's Intelligence Operations attorneys work closely with the intelligence community to ensure that they have the legal authorities required to conduct electronic surveillance and physical search of agents of foreign powers, including agents of international terrorist groups, in fast-paced national security investigations. Due to ISIS's prolific use of social media to spread propaganda and recruit followers on-line, NSD has seen an increase in the domestic HVE threat over the last few years, with more U.S. persons being recruited and radicalized on-line. This threat is likely to continue for some time. NSD's Oversight work is a critical (and often required) component of NSD's implementation of national security initiatives and authorities, including combating cyber-attacks, terrorism, espionage and the proliferation and use of weapons of mass destruction. Historical trends in NSD's Oversight work related to the IC's implementation of Section 702, as well as new DOJ obligations under the USA FREEDOM Act, indicate that the work in this area will grow in the coming years.

   As a part of Section 702 oversight, NSD has reviewed an increasing number of (1) National Security Agency (NSA) and FBI targeting decisions and (2) queries concerning a known U.S.

person (USP) of unminimized noncontents information obtained under Section 702. While the number of targeting decisions remains classified, the government reported in the 15th Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, "Since the inception of the program, the total number of facilities under collection during each reporting period has steadily increased with the exception of two reporting periods that experienced minor decreases." The unclassified estimated number of targets reported in the Statistical Transparency Report Regarding Use of National Security Authorities provides a helpful parallel. The number of targets grew from 89,138 in CY2013 to 106,469 in CY2016, equating to an increase of approximately 19%. In addition, for multiple agencies involved in Section 702 collection, the estimated number of USP queries increased from 9,500 in CY2013 to 30,355 in CY2016, which was an increase of over 200%.

The passage of the USA FREEDOM Act in June 2015 resulted in many significant amendments to FISA. NSD is playing a leading role in fulfilling the Act's requirements, including new oversight and amicus provisions. With respect to transparency, the Act requires the declassification (or, where that is not possible, declassified summaries) of opinions by the Foreign Intelligence Surveillance Court (FISC) and Foreign Intelligence Surveillance Court of Review that involve significant or novel issues. It also increases the government's public reporting obligations regarding specific uses of FISA authorities. The Act further requires that the FISC generally appoint an amicus curiae in FISA cases involving significant or novel issues—a requirement that we expect to result in additional legal briefings. Likewise, possible changes to Section 702 of FISA, which expires at the end of 2017, may well place additional burdens on the Division's limited resources.

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, including some involving individuals indicted for terrorism-related charges. The government has successfully litigated issues relating to Section 702 information in both federal district and appellate courts, and NSD expects continued growth in these challenges and the need to dedicate significant resources to these matters to ensure successful outcomes.

4. Difficulties inherent in supporting the continued development of a relatively new Division in an ever-changing environment: NSD, the newest litigating component of the Department, faces challenges associated with having to build an infrastructure and systems to support a developing Division. When it was created in 2006, NSD lacked certain policies and procedures that had to be developed over time, and indeed created an office to assist in fulfilling the Department's mandate to institute enterprise risk management. Likewise, NSD is in the process of building case management and document management systems that will allow NSD employees to efficiently and effectively carry out their mission. Requirements for these systems are complicated given the evolving nature of the work NSD performs and the ever-changing threats to the nation's security that NSD works daily to address. Similarly, NSD possesses a significant amount of classified and sensitive information, and it is therefore necessary to have in place the information technology systems to protect this information and a robust program to guard against the threats posed by insiders who misuse information or improperly disclose it without authorization. This creates unique challenges both in terms of information technology infrastructure and support, as well as document management. NSD's funding requests have not always been fully approved, however, which creates challenges for a Division that is just more than 10 years old.

Because of the nature of its work and the critical role it plays in protecting the nation against terrorism and threats to national security, NSD also faces particular challenges relating to emergency preparedness. The vast majority of NSD's work relates to classified material, and more than 80% of its workforce is housed in sensitive compartmented information facilities. NSD plays a pivotal role in providing operational and policy support to the intelligence community, law enforcement, and the Department and other government agencies in the event of a local or national emergency. Continuity of operations and continuity of government plans, therefore, must account for the circumstances in which NSD must be able to operate, which can lead to significant additional costs.

5. Challenges associated with victims outreach: NSD also maintains the Office of Justice for Victims of Overseas Terrorism (OVT) to assist U.S. citizen victims when the terrorist attack and criminal proceedings occur overseas. OVT faces challenges in obtaining foreign litigation information, which includes security challenges; lack of political will by the foreign government; unpredictable foreign justice mechanisms; sovereignty concerns of the foreign government; and bureaucratic issues within the United States Government.

   This caseload is defined as cases involving U.S. citizens that are in a foreign litigation process, and this caseload number is fluid as cases are resolved. This type of monitoring and advocacy requires additional time and effort on behalf of a very small staff. U.S. citizens who are injured by terrorists abroad deserve the best advocacy and information services that can be provided. It is the goal of OVT to do exactly that; however, the proper resources and access to this information must be available in order for OVT to fully achieve its mission.

E. Environmental Accountability

NSD continues to be committed to environmental wellness and, to that end, is involved in a variety of programs and activities that promote environmental responsibility. Examples include:

- Developing and implementing automated systems in an effort to become as paperless as possible. This effort has also significantly decreased daily toner and paper usage as well as other various costs associated with printers and copier machines.
- Administering a comprehensive recycling program. NSD distributes individual recycling containers to each employee and contractor and provides larger recycling containers in common areas such as breakrooms. The Division also recycles all toner cartridges.
- Participating in DOJ environmental initiatives, including the Transit Subsidy and Bicycle Commuter Fringe Benefits programs.

II. Summary of Program Changes *(No Program Changes)*

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, [$97,337,000] *$101,031,000*, 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
2016 Enacted	393	353	$95,000,000
2017 Continuing Resolution	393	359	$94,819,000
Adjustments to Base and Technical Adjustments	-31	3	6,212,000
2018 Current Services	362	362	101,031,000
2018 Program Increases	0	0	0
2018 Program Offsets	0	0	0
2018 Request	362	362	101,031,000
Total Change 2017-2018	**-31**	**3**	**$6,212,000**

National Security Division-Information Technology Breakout	Direct Pos.	Estimate FTE	Amount
2016 Enacted	18	18	15,758,000
2017 Continuing Resolution	18	18	16,859,000
Adjustments to Base and Technical Adjustments	0	0	0
2018 Current Services	18	18	16,313,000
2018 Program Increases	0	0	0
2018 Program Offsets	0	0	0
2018 Request	18	18	16,313,000
Total Change 2017-2018	**0**	**0**	**-$546,000**

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											
WORKLOAD/ RESOURCES		**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)**	
		FY 2016		**FY 2016**		**FY 2017**		**Current Services Adjustments and FY 2018 Program Changes**		**FY 2018 Request**	
Workload[1]											
Defendants Charged		137		190		142		0		142	
Defendants Closed		117		138		122		0		122	
Matters Opened		72,596		115,687		72,611		58,020		130,631	
Matters Closed		72,473		115,705		72,483		58,012		130,495	
FISA Applications Filed[2]		CY 2016: 2,200		CY 2016: 1,743		CY 2017: 2,200		0		CY 2018: 2,200	
National Security Reviews of Foreign Acquisitions		CY 2016: 225		CY 2016: 229		CY 2017: 300		0		CY 2018: 300	
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**
		353	95,000	353	95,000	359	94,819	3	6,212	362	101,031
		FY 2016		**FY 2016**		**FY 2017**		**Current Services Adjustments and FY 2018 Program Changes**		**FY 2018 Request**	
Program Activity	**Intelligence**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		197	47,178	193	47,178	197	47,088	1	3,085	198	50,173
Output Measure	Intelligence Community Oversight Reviews	CY 2016: 100		CY 2016: 110		CY 2017: 105		0		CY 2018: 105	

[1]Workload measures are not performance targets, rather they are estimates to be used for resource planning.

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

PERFORMANCE AND RESOURCES TABLE											
Decision Unit: National Security Division											
WORKLOAD/ RESOURCES		**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)**	
		FY 2016		**FY 2016**		**FY 2017**		**Current Services Adjustments and FY 2018 Program Changes**		**FY 2018 Request**	
Program Activity	**Counterterrorism**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		89	22,225	89	22,225	90	22,182	1	1,454	91	23,636
Efficiency Measure	Percentage of OVT responses to victims within 3 business days of victim request for information from OVT	80%		100%		80%		N/A		N/A-Discontinued	
Outcome Measure	Percentage of services/rights OVT successfully provided to victims of attacks identified within the fiscal year	95%		98%		95%		N/A		N/A-Discontinued	
Outcome Measure	Percentage of CT defendants whose cases were favorably resolved	90%		99%		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	**Counterintelligence and Export Control**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		49	22,125	49	22,125	49	22,083	1	1,447	50	23,529
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 2016: 35		CY 2016: 43		CY 2017: 45		0		CY 2018: 45	
Program Activity	**Cyber**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		22	3,472	22	3,472	22	3,466	1	227	23	3,693
Outcome Measure	Percentage of Cyber defendants whose cases were favorably resolved	90%		100%		90%		0		90%	

PERFORMANCE MEASURE TABLE									
Performance Report and Performance Plan Targets		**FY 2012**	**FY 2013**	**FY 2014**	**FY 2015**	**FY 2016**	**FY 2016**	**FY 2017**	**FY 2018**
		Actual	**Actual**	**Actual**	**Actual**	**Target**	**Actual**	**Target**	**Target**
Performance Measure	Intelligence Community Oversight Reviews	CY 2012: 99	CY 2013: 112	CY 2014: 109	CY 2015: 124	CY 2016: 100	CY 2016: 110	CY 2017: 105	CY2018: 105
Efficiency Measure	Percentage of OVT responses to victims within 3 business days of victim request for information from OVT	89%	100%	100%	80%	80%	100%	80%	N/A Discontinued
Outcome Measure	Percentage of services/rights OVT successfully provided to victims of attacks identified within the fiscal year	N/A	94%	99%	95%	95%	98%	95%	N/A Discontinued
Outcome Measure	Percentage of CT defendants whose cases were favorably resolved	98%	94%	92%	100%	90%	99%	90%	90%
Outcome Measure	Percentage of CT cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	100%	99%	100%	98%	99%	100%	99%	99%
Outcome Measure	Percentage of CE defendants whose cases were favorably resolved	100%	100%	98%	100%	90%	100%	90%	90%
Performance Measure	FARA inspections completed	15	15	12	14	14	14	14	14
Performance Measure	High priority national security reviews completed	CY 2012: 37	CY 2013: 30	CY 2014: 32	CY 2015: 35	CY 2015: 38	CY 2016: 43	CY 2017: 45	CY 2018: 45
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%	90%	90%
Outcome Measure	Percentage of Cyber defendants whose cases were favorably resolved	N/A – new in FY 2014	N/A – new in FY 2014	NA[1]	100%	90%	100%	90%	90%

[1] NSD did not report an actual for this measure because no cyber cases were resolved during the fiscal year.

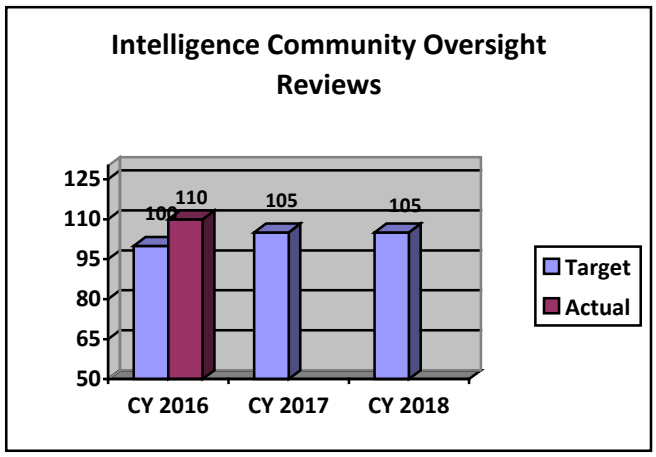
3. Performance, Resources, and Strategies

For performance reporting purposes, resources for NSD are allocated to four program activities: Intelligence, Counterterrorism, Counterintelligence and Export Control, and Cyber Security.

A. Performance Plan and Report for Outcomes

Intelligence Performance Report

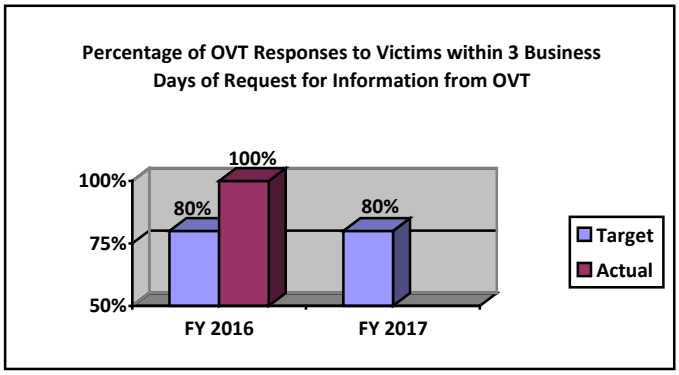
Measure: Intelligence Community Oversight Reviews
CY 2016 Target: 100
CY 2016 Actual: 110
CY 2017 Target: 105
CY 2018 Target: 105
Discussion: The CY 2018 target is consistent with the previous targets. Although the overall work of the Division assessing and ensuring compliance is expected to continue to increase in future years due to the growth of current oversight programs, this is largely reflected in the targets for matters opened and closed. The scope and resources required to prepare for, and conduct, existing reviews is expected to continue to increase due to the Intelligence Community's increased use of certain national security tools.



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.

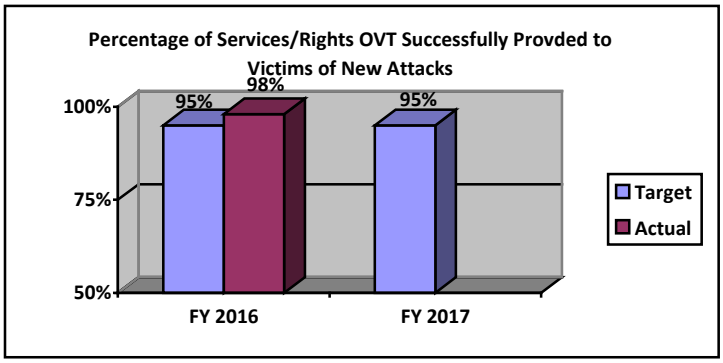
Counterterrorism Performance Report

Measure: Percentage of OVT Responses to Victims within 3 Business Days of Victim Request for Information from OVT
FY 2016 Target: 80%
FY 2016 Actual: 100%
FY 2017 Target: 80%
FY 2018 Target: N/A- measure will be discontinued.
Discussion: This measure will be discontinued starting in FY 2018.



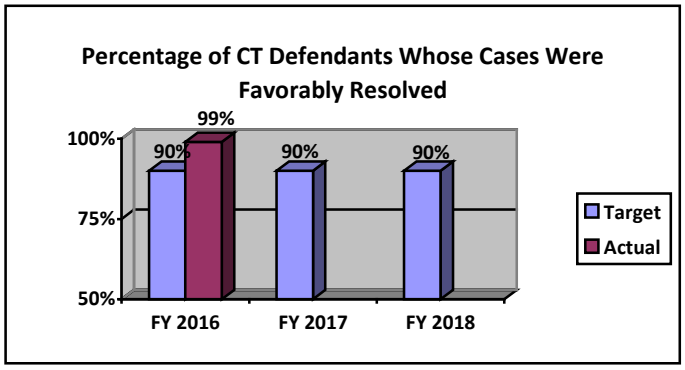
Data Definition: Victims: American citizens who are the victims of terrorism outside the borders of the U.S. This measure reflects OVT's efficiency in providing information to victims after they have contacted OVT.
Data Collection and Storage: Data is collected and stored in an electronic database.
Data Validation and Verification: Data is validated by management and staff.
Data Limitations: None.

Measure: Percent of services/rights OVT successfully provided to victims of attacks identified within the fiscal year.
FY 2016 Target: 95%
FY 2016 Actual: 98%
FY 2017 Target: 95%
FY 2018 Target: N/A- measure will be discontinued.
Discussion: This measure will be discontinued in FY 2018



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 2016 Target: 90%
FY 2016 Actual: 99%
FY 2017 Target: 90%
FY 2018 Target: 90%
Discussion: The FY 2018 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.

Highlights from Recent Counterterrorism Cases

The following are highlights from recent counterterrorism cases.

United States v. Ibrahim Suleiman Adnan Adam Harun, aka "Spin Ghul": Beginning in 2001, the defendant traveled from Saudi Arabia to Afghanistan intending to fight violent jihad. He joined al-Qaeda, received military-type training at al-Qaeda training camps, and ultimately fought against United States and Coalition forces in Afghanistan with an al-Qaeda fighting group based in Pakistan.

Harun attempted to kill U.S. military personnel in Afghanistan between 2002 and 2003. In 2003, in Pakistan, Harun received further al-Qaeda training and traveled to Africa intending to conduct attacks on U.S. diplomatic facilities in Nigeria. While in Nigeria, Harun conspired with others to bomb such facilities. Harun then went to Libya in late 2004 with the intention of going to Europe so he could conduct an attack there. He was later arrested in Libya and, in June 2011, the Libyans deported him to Italy where he was arrested by Italian authorities. Harun was extradited to the United States in October 2012.

On March 20, 2013, the district court in the Eastern District of New York unsealed a six-count indictment, which was filed on February 21, 2012, charging Harun with (1) conspiracy to murder United States nationals, in violation of 18 U.S.C. § 2332(b)(2); (2) conspiracy to attack a government facility, in violation of 18 U.S.C. §§ 2332f(a)(2), 2332f(b)(2) and 2332f(c); (3) conspiracy to provide material support to a foreign terrorist organization, in violation of 18 U.S.C. §§ 2339B(a)(1) and 2339B(d); (4) provision and attempted provision of material support to a foreign terrorist organization, in violation of 18 U.S.C. §§ 2339B(a)(1), 2339B(d) and 2; (5) use of firearms, in violation of 18 U.S.C. §§ 924(c)(1)(A)(iii), 924(c)(1)(B)(ii) and 2; and (6) use of explosives, in violation of 18 U.S.C. §§ 844(h)(1), 844(h)(2) and 2. In March 2016, after a ten-day trial, Harun was convicted of all counts.

United States v. Ardit Ferizi: On September 23, 2016, in the Eastern District of Virginia, Ardit Ferizi was sentenced to 20 years' imprisonment followed by 10 years of supervised release. On June 15, 2016, Ferizi pled guilty to one count of providing material support to the Islamic State of Iraq and al-Sham (ISIS), in violation of 18 U.S.C. § 2339B, and one count of computer hacking, in violation of 18 U.S.C. § 1030(a)(2). On February 26, 2016, Ferizi was arraigned on an indictment returned February 16, 2016, charging him with one count of conspiring to provide material support to the Islamic State of Iraq and al-Sham (ISIS), in violation of 18 U.S.C. § 2339B, one count of providing material support to ISIS, in violation of 18 U.S.C. § 2339B, one count of computer hacking, in violation of 18 U.S.C. § 1030, and one count of aggravated identity theft, in violation of 18 U.S.C. § 1028A.

Ferizi, the leader of a Kosovo-based hacking group, gained unauthorized access to a U.S. company's server and stole personally identifiable information (PII) belonging to more than 1,000 United States government employees, including military and law enforcement personnel. Ferizi provided the PII to ISIS member Junaid Hussain, knowing that the information would be used by ISIS to target the identified individuals for terrorist attacks. On August 11, 2015, ISIS, acting through the "Islamic State Hacking Division," published a "kill list" on the internet containing the PII for the United States government employees obtained by Ferizi from the U.S. company's server.

Kampala Bombing Case: On July 11, 2010, during the World Cup Final, two members of al-Shabaab detonated suicide bomb devices at two locations in Kampala, Uganda, killing more than 76 people, including one American, and wounding scores of others, including four Americans. Since shortly after the bombing and up until a final verdict and sentencing in 2016, FBI personnel and DOJ prosecutors

assisted Ugandan authorities in the investigation and prosecution of this attack. Through committed investigative case work, the investigative team of the FBI JTTF, CIA, Ugandan, Kenyan, and Tanzanian law enforcement and intelligence services identified and arrested 15 individuals who planned, facilitated, and executed the attacks. In May 2016, a court in Uganda convicted eight defendants for their involvement in the attacks.

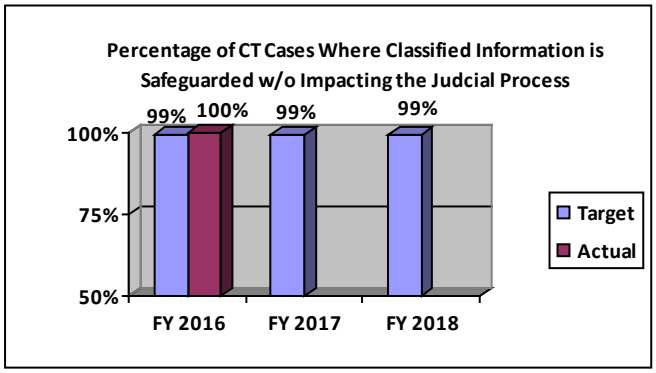
United States v. Sullivan: In November 2016, in the Western District of North Carolina, Justin Nolan Sullivan pled guilty to attempting to commit acts of terrorism transcending national boundaries, in violation of 18 U.S.C. §§ 2332b(a)(1) and (2). The plea agreement was submitted to the court under Rule 11(c)(1)(C) and Sullivan agreed to serve a term of life in prison.

On January 20, 2016, a grand jury returned an indictment charging Sullivan with attempting to provide material support to Islamic State of Iraq and al-Sham (ISIS), in violation of 18 U.S.C. § 2339B; transporting and receiving a silencer in interstate commerce with the intent to commit a felony, in violation of 18 U.S.C. § 924(b); receiving and possessing an unregistered silencer, unidentified by a serial number, in violation of 26 U.S.C. § 5861(d); possessing a stolen firearm, in violation of 18 U.S.C. §§ 922(j) and 924(a)(2); using interstate facilities in the attempted commission of a murder-for-hire, in violation of 18 U.S.C. § 1958; and two counts of making a false statement to an agency of the United States, in violation of 18 U.S.C. § 1001(a)(2). Subsequently, on August 16, 2016, a nine-count superseding indictment was returned. The Superseding Indictment added a count of conspiring to commit an act of terrorism transcending national boundaries and a count of attempting to commit an act of terrorism transcending national boundaries, both in violation of 18 U.S.C. § 2332b. The additional charges arose from Sullivan's coordination with the now-deceased, Syria-based ISIS member and attack facilitator, Junaid Hussain, regarding Sullivan's planned terrorist attack.

On or about June 6, 2015, an FBI undercover employee (UC) made contact with Sullivan. Sullivan told the UC that "the war is here," and gave the UC the opportunity to join what he called the "Islamic State of North America." During conversations over the ensuing days, Sullivan discussed his various attack concepts, and he stated his intention to obtain an AR-15 from a gun show on June 20-21, 2015. Sullivan asked the UC whether the UC would be able to construct a homemade silencer that could attach to an AR-15. When the UC responded affirmatively, Sullivan told the UC that he would need to have it made by the following week because he planned to use it that month. Sullivan further explained that he intended to conduct assassinations in order to train for his planned mass casualty attack on a bar, concert, or nightclub. Sullivan also told the UC about his plan to create a video of their attack to send to ISIS, in response to a tasking from Hussain. On June 19, 2015, Sullivan received the package containing the silencer at the home which he shared with his parents. After the package arrived, Sullivan's parents questioned him about the nature and purpose of the silencer. Sullivan hid the silencer in a crawl space where he had previously hidden a stolen .22 caliber rifle, mask, and lock-pick kit. A few hours later, Sullivan offered to compensate the UC for killing Sullivan's parents. Sullivan was arrested shortly thereafter.

Measure: **Percentage of CT Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2016 Target: 99%
FY 2016 Actual: 100%
FY 2017 Target: 99%
FY 2018 Target: 99%

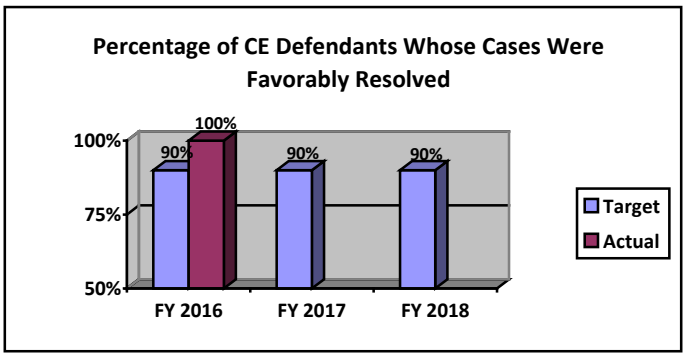
Discussion: The FY 2018 target is consistent with previous fiscal years. NSD will support successful prosecutions by providing advice and assistance on the use of classified evidence through the application of the Classified Information Procedures Act (CIPA).



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.

Counterintelligence and Export Control (CE) Performance Report

Measure: Percentage of CE Defendants Whose Cases Were Favorably Resolved
FY 2016 Target: 90%
FY 2016 Actual: 100%
FY 2017 Target: 90%
FY 2018 Target: 90%
Discussion: The FY 2018 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.

Highlights from Recent Counterintelligence and Export Control Cases

The following are highlights from recent counterintelligence and export control cases.

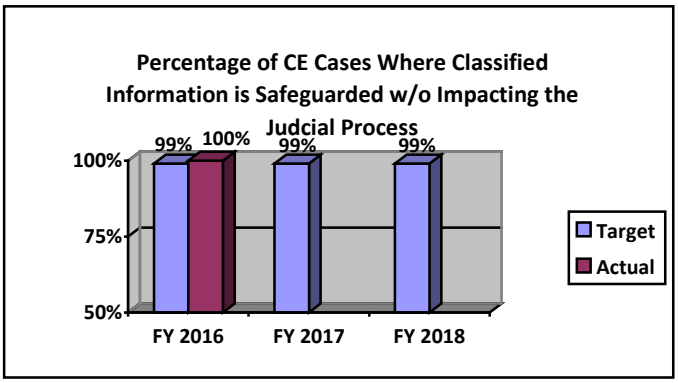
U.S. v. Mo Hailong et al.: In January 2016, in the Southern District of Iowa, Mo Hailong a/k/a "Robert Mo" pleaded guilty to conspiracy to steal trade secrets. Mo was employed as director of international business of the Beijing Dabeinong Technology Group Company. Mo admitted to participating in a long-term conspiracy to steal trade secrets from U.S. companies DuPont Pioneer and Monsanto. Mo further admitted to participating in the theft of inbred – or parent – corn seeds from fields in Iowa for the purpose of transporting those seeds to China. The stolen inbred seeds constituted valuable intellectual property of DuPont Pioneer and Monsanto. Mo was sentenced to 36 months' imprisonment.

U.S. v. Buryakov (Conspiracy to Work for Russian Intelligence): In March 2016, in the Southern District of New York, Evgeny Buryakov pleaded guilty to conspiring to act in the United States as an agent of the Russian Federation without providing prior notice to the Attorney General. Beginning in at least 2012, Buryakov worked in the United States as an agent of Russia's foreign intelligence service, known as the SVR. Buryakov operated under non-official cover, meaning he entered and remained in the United States as a private citizen, posing as an employee in the New York office of Vnesheconombank, a Russian bank. Buryakov worked in New York with at least two other SVR officers serving under official cover, exchanging intelligence-related information while shielding their associations with one another as SVR officers. Buryakov was sentenced to 30 months' imprisonment.

U.S. v. Kun Shan Chun: In August 2016, in the Southern District of New York, Kun Shan Chun a/k/a "Joey Chun" pleaded guilty to acting in the United States as an agent of China without prior notification to the Attorney General. Chun worked at the FBI's New York Field Office as an electronics technician with a Top Secret security clearance. Beginning in 2006, Chun received and responded to taskings from Chinese nationals (and at least one Chinese government official), some, if not all, of whom were aware that Chun worked at the FBI. On multiple occasions, at the direction of Chinese officials, Chun collected sensitive FBI information and caused it to be transmitted to the Chinese government official and others,

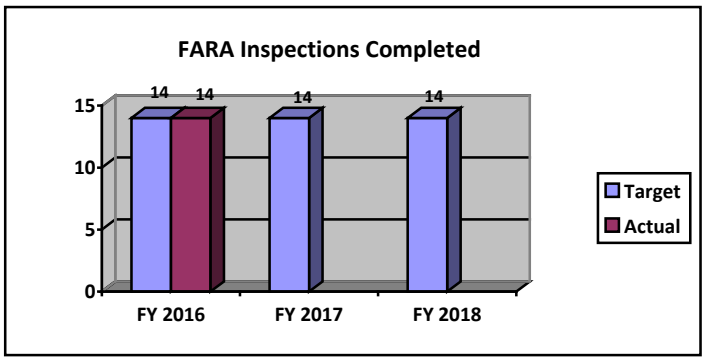
while at the same time engaging in a prolonged and concerted effort to conceal from the FBI his illicit relationships with these individuals. Chun was sentenced to 24 months' imprisonment and fined $10,000.

Measure: **Percentage of CE Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2016 Target: 99%
FY 2016 Actual: 100%
FY 2017 Target: 99%
FY 2018 Target: 99%
Discussion: The FY 2018 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).



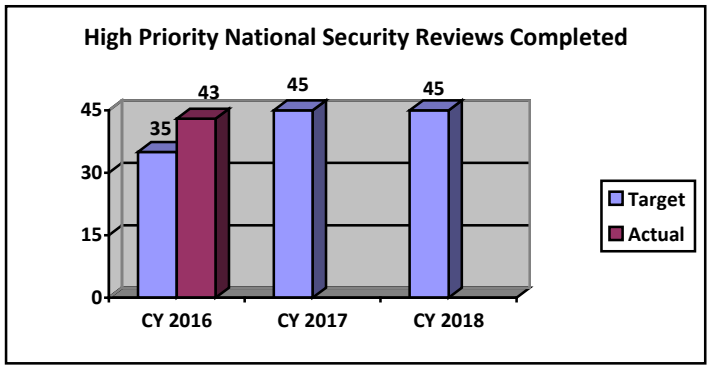
Data Definition: Classified information - information that has been determined by the United State Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data as defined by the 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 2016 Target: 14
FY 2016 Actual: 14
FY 2017 Target: 14
FY 2018 Target: 14
Discussion: The FY 2018 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 2016 Target: 35
CY 2016 Actual: 43
CY 2017 Target: 45
CY 2018 Target: 45
Discussion: The CY 2018 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.

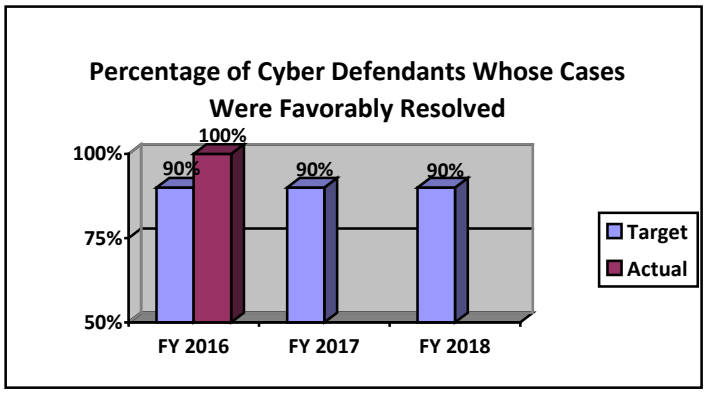


Data Definition: High Priority National Security Reviews include: (1) CFIUS case reviews of transactions in which DOJ is a co-lead agency in CFIUS due to the potential impact on DOJ equities; (2) CFIUS case reviews which result in a mitigation agreement to which DOJ is a signatory; (3) Team Telecom case 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 2016 Target: 90%
FY 2016 Actual: 100%
FY 2017 Target: 90%
FY 2018 Target: 90%
Discussion: The FY 2018 target is consistent with previous fiscal years. Among the strategies that NSD will pursue in this area are: recruiting, hiring, and training additional cyber-skilled professionals. NSD also has substantially increased its engagement with potential victims of cyber attacks and the private sector in an effort to further detect, disrupt, and deter cyber threats targeting U.S. companies and companies operating in the U.S.



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.

Highlights from Recent National Security Cyber Cases

The following are highlights from recent cyber cases.

U.S. v. Su Bin: In July 2016, in the Central District of California, Chinese national Su Bin was sentenced to 46 months in prison. In March 2016, Su pleaded guilty to one count of conspiring to gain unauthorized access to a protected computer and to violate the Arms Export Control Act by exporting defense articles on the U.S. Munitions List contained in the International Traffic in Arms Regulations. Su admitted that he conspired with two persons in China from October 2008 to March 2014 to gain unauthorized access to protected computer networks in the United States – including computers belonging to the Boeing Company in Orange County, California – to obtain sensitive military information and to export that information illegally from the United States to China.

U.S. v. Peter Romar et al: In September 2016, Peter Romar, a Syrian national affiliated with the Syrian Electronic Army (SEA), pleaded guilty to felony charges of conspiring to receive extortion proceeds and conspiring to unlawfully access computers. According to the plea, beginning in approximately 2013, Romar and a co-conspirator engaged in an extortion scheme that involved hacking online businesses in the U.S. and elsewhere for personal profit. Court documents further alleged that the conspiracy gained unauthorized access to the victims' computers and then threatened to damage computers, delete data, or sell stolen data unless the victims provided extortion payments to the co-conspirator or Romar. If a victim could not make extortion payments to the conspiracy's Syrian bank accounts due to sanctions targeting Syria, Romar acted as an intermediary in Germany to evade those sanctions.

U.S. v. Ardit Ferizi: In September 2016, Ardit Ferizi, a citizen of Kosovo, was sentenced to 20 years in prison for providing material support to the Islamic State in Iraq and ash-Sham (ISIS), a designated foreign terrorist organization, and accessing a protected computer without authorization and obtaining information in order to provide material support to ISIS. In June 2016, Ferizi pleaded guilty to gaining system administrator-level access to a server that hosted the website of a U.S. victim company. The website contained databases with personally identifiable information (PII) belonging to tens of thousands of the victim company's customers, including members of the military and other government personnel. Ferizi subsequently culled the PII belonging to U.S. military members and other government personnel, which totaled approximately 1,300 individuals. Ferizi then provided the PII belonging to the 1,300 U.S. military members and government personnel to Junaid Hussain, a now-deceased ISIS recruiter and attack facilitator. Ferizi and Hussain discussed publishing the PII of those 1,300 victims in a hit list.

B. Strategies to Accomplish Outcomes

Strategies for accomplishing outcomes within each of NSD's four program activities - Intelligence, Counterterrorism, Counterintelligence and Export Control, and Cyber Security - are detailed below.

Intelligence

NSD will continue to ensure that the IC is able to make efficient use of foreign intelligence information collection authorities, particularly pursuant to 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.

Counterterrorism

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 Intelligence Community, and the 94 U.S. Attorneys' Offices; develop national strategies for combating emerging and evolving terrorism threats, including the threats of homegrown violent extremists and 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; share information with and provide advice to international prosecutors, agents, and investigating magistrates to assist in addressing international threat information and litigation initiatives; through international training programs provide capacity building for international counterparts; provide case mentoring to international prosecutors and law enforcement agents; 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.

Counterintelligence and Export Control

Among the strategies that the National Security Division will pursue in this area are: supporting and supervising the investigation and prosecution of espionage and related cases through coordinated efforts and close collaboration with Department leadership, the FBI, the Intelligence Community, and the 94 Offices of the U.S. Attorneys; implementing national strategies for combating the evolving threat of cyber-based espionage and state-sponsored cyber intrusions; overseeing and assisting the expansion of investigations and prosecutions for 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 prosecutions by providing advice and assistance with application of the Classified Information Procedures Act; and enforcing the Foreign Agents Registration Act of 1938 and related disclosure statutes.

Cyber Security

Among the strategies that NSD will pursue in this area are: recruit, hire, and train additional skilled professionals to work on cyber matters; prioritize disruption of cyber threats to the national security through the use of the U.S. Government's full range of tools, including law enforcement, diplomatic, and intelligence methods; support and supervise the investigation and prosecution of national security-related computer intrusion cases through coordinated efforts and close collaboration with Department leadership, the FBI, the Intelligence Community, other inter-agency partners, and the 94 Offices of the U.S. Attorneys; coordinate and provide advice in connection with national security-related cyber intrusion cases involving the application of the Classified Information Procedures Act; promote legislative priorities that adequately safeguard national cyber security interests; and implement NSD's Strategic Plan for Countering the National Security Cyber Threat, which was adopted in January 2017.



VII. Exhibits