FY 2020
Performance Budget
Congressional Justification

NATIONAL SECURITY DIVISION

Table of Contents

I. Overview for National Security Division

A. Introduction

The National Security Division (NSD) works to enhance national security and counter the threat of terrorism, the Department of Justice's (DOJ) top priority. NSD requests for Fiscal Year (FY) 2020 a total of 391 positions (including 265 attorneys), 362 FTE, and $109,585,000.[1]

B. Background

NSD has outlined six areas of focus that will guide its operations in the coming years. NSD will:

- 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;
- Investigate and prosecute the unauthorized disclosure and improper handling of classified information; and
- Ensure that Intelligence Community (IC) agencies have the legal tools necessary to conduct intelligence operations while safeguarding privacy and civil liberties.

Division Structure

NSD strengthens the Department's core national security functions by providing strategic national security policy coordination and development. NSD combines counterterrorism, counterintelligence, export control, and cyber prosecutors with attorneys who oversee the Department's foreign intelligence/counterintelligence operations, as well as attorneys who provide policy and legal advice on a wide range of national security issues. 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 IC. 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);
- Executive Office (EO)

[1] Within the totals outlined above, NSD has included a total of 24 positions, 24 FTE, and $18,780,000 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 (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;
- 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 U.S. 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 of terrorism, since 2013, the Department has charged publicly more than 160 individuals, in more than 45 districts across the country, for foreign fighter, homegrown violent extremist, and ISIS-related conduct. These cases include, among others, aspiring foreign fighters who were arrested before they departed the country, and individuals who were inspired by ISIS to plot violent acts in the U.S. but were disrupted before they could do so.
- Over the past year, the Division, in partnership with USAOs, secured numerous convictions and sentences in significant terrorism-related cases, including: a life sentence handed down for a convicted al Qaeda operative who participated in deadly attacks against U.S. soldiers in Afghanistan; a conviction and life sentence against the terrorist who placed and detonated bombs in New York and New Jersey; a conviction and sentencing of a former police officer who violated his oath to protect the public and became an ISIS supporter; a conviction of one of the perpetrators of the terrorist attacks in Benghazi that resulted in the deaths of four Americans, including our Ambassador to Libya; a conviction of a terrorist who designed, made, and supplied parts for remote-controlled IED initiator switches for roadside bombs used against U.S. military personnel in Iraq in and around 2006; and the conviction of three domestic terrorists who plotted to blow up an apartment complex to target members of an immigrant community who lived and worshipped there.
- The Division, in partnership with USAOs, continued bringing charges in complex national security cyber cases. In the last calendar year alone, the Department has charged more national security-related cyber intrusion or attack cases than the combined number of those charged in the three prior years of the Department's national security cyber program, and for the first time assisted the FBI in obtaining the necessary legal process to carry out disruptive technical operations against nation state cyber threats. One recent notable example of these efforts includes the indictment of nine Iranians for conducting a coordinated campaign of computer intrusions at more than 300 universities and dozens of companies worldwide. Working on behalf of the Islamic Revolutionary Guard Corps (IRGC), the defendants are accused of stealing terabytes of academic data and intellectual property (which cost the U.S. universities more than $3.4 billion to procure and access), some of which they sold for their own profit on websites in Iran. In addition to the charges, NSD worked with the Department of the Treasury to sanction the defendants and the entity they worked for, known as the Mabna Institute, which shuttered its doors shortly thereafter. NSD also worked with the FBI to disrupt a botnet, known as VPNFilter, infecting at least half a million small office and home Internet routers worldwide. Thanks to NSD's efforts (which included obtaining legal process that enabled the FBI to seize control of part of the botnet's

infrastructure and thereby learn the IPs of infected bots), internet service providers and other organizations will be able to notify users of the infection and assist them with mitigating it. Meanwhile, one of the defendants accused of conspiring with Russian Federal Security Service (FSB) officers to hack into Yahoo and other webmail providers was convicted and sentenced to five years' imprisonment in the Northern District of California, and another individual was charged (under seal) in the Central District of California with conspiring with other North Koreans to conduct a number of major computer intrusions and attacks such as the destruction of Sony Pictures Entertainment's corporate network in 2014, the theft of $81 million from the Bank of Bangladesh in 2016, and last year's worldwide ransomware attack known as WannaCry.

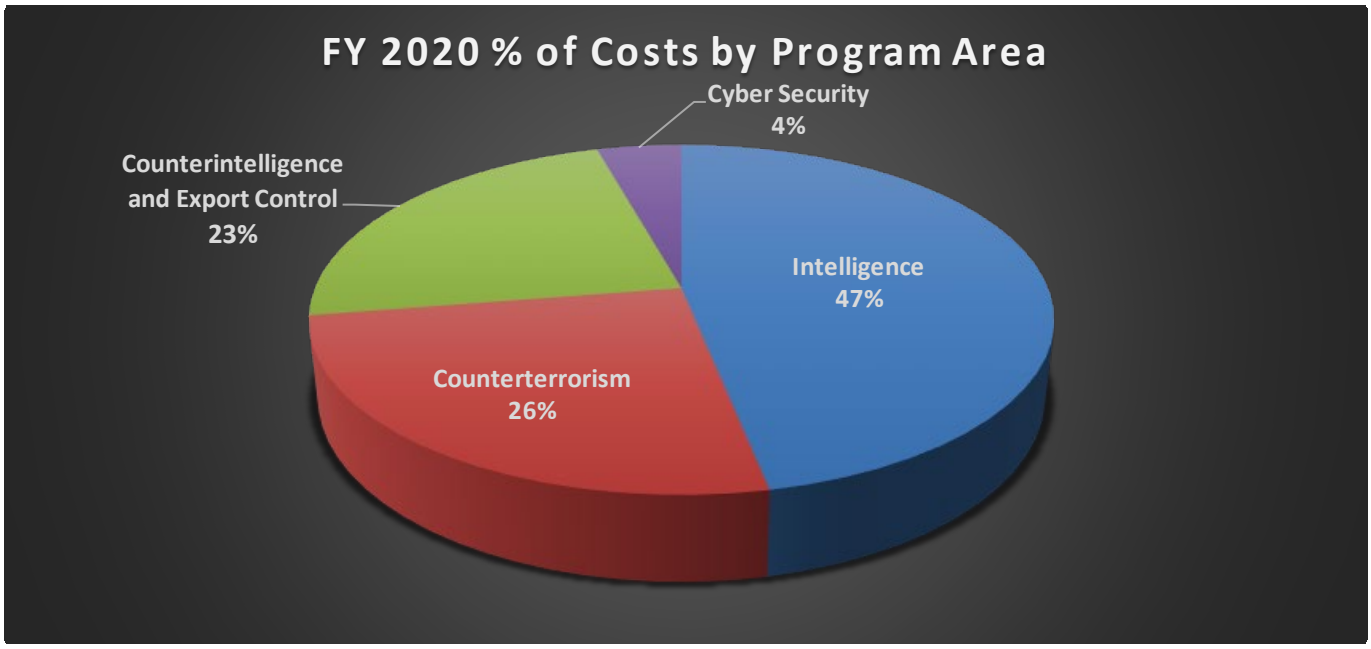
- The Division continued to aggressively pursue and prosecute the theft of sensitive technology from the U.S., utilizing a combination of export control and trade secret laws. In February 2018, in the Central District of California, three men – Yi-Chi Shih, Kiet Ahn Mai, and Ishiang Shih – with a scheme to illegally obtain technology and integrated circuits with military applications, which the men exported to China without the required export license. The men were also charged with unauthorized access to a protected computer, as well as mail fraud, wire fraud, and money laundering. In April 2018, two businessmen, U.S. citizen Shan Shi and Chinese national Gang Liu, were indicted in the District of Columbia on charges alleging that they conspired to commit economic espionage and steal trade secrets from a business in the U.S. on behalf of a company in China that was engaged in manufacturing buoyancy materials for military and civilian uses. Other defendants were previously charged with theft of trade secrets.
- Enforcing sanctions against Iran remains an enforcement priority for the Division, and, since 2016, the Department has charged more than 40 defendants in connection with violations of the Iranian embargo. Illustrative of this effort, the Division, in conjunction with the U.S. Attorney's Office, prosecuted one of the largest proliferation financing cases involving Iran. In January 2018, Mehmet Atilla was convicted of conspiring with others to use the U.S. financial system to conduct transactions totaling over $1 billion on behalf of the Government of Iran and other Iranian entities, which were barred by U.S. sanctions, and to defraud U.S. financial institutions by concealing the true nature of these transactions. His co-conspirator, Reza Zarrab, pleaded guilty in October 2017.
- In 2017, the Division received an unprecedented number of referrals requesting investigations of disclosures of classified information (leaks), and opened an unprecedented number of such investigations, many of which remain active. The Attorney General and the Director of National Intelligence held a press conference to highlight the dangers posed by leaks and the Attorney General has directed NSD to continue to prioritize these investigations. The Division continues to devote additional personnel and significant time and resources to these matters. In recent months, charges were filed against individuals in two districts for unlawfully transmitting classified national defense information, one resulting in a guilty plea.
- The Division's Foreign Investment Review Staff (FIRS) conducted 40% more foreign investment reviews in 2017 than the prior year, with similar numbers in 2018. FIRS led more cases in 2017 than it did in the prior five years combined, and FIRS has been responsible for approximately half of the significant national security actions that CFIUS has taken in the last year. FIRS has also led 90% of the telecommunications application reviews for national security and law enforcement risk in 2017. FIRS also drafted and negotiated two proposed Executive Orders (which we expect to be signed this summer) that would strengthen Executive Branch authorities and procedure for addressing telecommunications license applications and supply chain threats to the telecommunications sector.

- The Office of Justice for Victims of Overseas Terrorism (OVT) successfully assisted numerous U.S. citizen victims of overseas terrorism in exercising rights available to them in foreign criminal justice systems. The number of foreign cases involving U.S. citizen victims that OVT is actively monitoring continues to increase.
- The Division conducted over 30 reviews at IC component headquarter locations to assess compliance with acquisition, retention and/or dissemination requirements of Section 702 authorities during 2017, in addition to its daily activities in furtherance of overseeing implementation of Section 702 authorities. In addition, the Division conducted approximately the same number of reviews at non-headquarters locations during 2017.
- The Division continues to litigate and obtain favorable rulings upholding FISA authorities as lawful, including five such rulings in 2017.
- The Division successfully preserved a lawful and essential tool for the IC by securing Congressional reauthorization of Section 702 of FISA in January 2018. The Division continues its robust oversight efforts to ensure this authority is used in a manner that protects the privacy and civil liberties of individuals. Looking forward, the Division anticipates vigorously advocating for renewal of certain authorities contained within the USA FREEDOM ACT of 2015, provisions of which are scheduled to sunset on December 15, 2019.
- As part of its oversight responsibilities, the Division reviewed NSA targeting decisions for approximately 129,080 targets under Section 702, a 21% increase from the 106,469 targets reviewed in 2016, and a 38% increase from the 94,368 targets reviewed in 2015. As President Trump stated in January 2018 when he signed the bill re-authorizing this program for an additional six years, the intelligence collected under Section 702 "is vital to keeping the Nation safe" and "allows the Intelligence Community, under a robust regime of oversight by all three branches of Government, to collect critical intelligence on international terrorists, weapons proliferators, and other important foreign intelligence targets located outside the United States."
- The Division worked closely with the Criminal Division and Congress to enact the CLOUD Act, which restores the government's authority to use search warrants to compel disclosure of electronic data abroad and authorizes international agreements to reduce conflicts of law and improve the process by which the U.S. and its allies handle cross-border requests for electronic data in investigations of serious crime, including terrorism.
- The Division worked closely with the FBI and the Deputy Attorney General's Office to develop a framework for countering foreign influence operations against the U.S., including a policy regarding the factors to be considered in disclosing such operations to victims, other affected individuals, and the public.

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 for overhead costs associated with management, administration, and law and policy offices. The overhead costs are 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 2020.



D. Performance Challenges

Enhancing national security and countering the threat 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 recent recognition of increasing and changing threats to our national assets, including significant growth of cyber threats to the national security: 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 U.S. are also engaged in an aggressive campaign to acquire superior technologies and commodities that are developed in the U.S., 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 computer networks, as well as through insider threats. The most sophisticated of our adversaries employ multi-faceted campaigns to acquire valuable proprietary technologies and information through a combination of traditional and asymmetric approaches. For example, our nation-state 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, multi-faceted 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 CFIUS and its review of foreign entities' licenses and applications for provision of communications services before the FCC (through the Team Telecom working group)—has also expanded to address the asymmetric threat. For CFIUS in particular, by all reports, including media sources, the volume of filings before CFIUS has increased significantly over the years, with historic numbers of cases filed with the Committee in CY[2] 2017 and 2018. As previously discussed, CY 2017 was a 40% increase over CY 2016.

In addition to the sheer volume of cases, there have been more and new national security concerns that have arisen in CFIUS in recent years, necessitating that NSD work harder to address those novel and evolving national security issues (DOJ led more cases in CY 2017 than DOJ did in the previous five years, combined, because DOJ needed to address the national security concern presented on behalf of the Executive Branch), which have resulted in many more high priority national security reviews (directly related to cyber security). More than three years ago, only about 5% of filings presented serious national security considerations; however, now, more than 30% of the filings present serious and complex national security considerations. NSD has risen to the occasion to address these needs; in CY 2017, NSD was responsible for almost half of all novel or difficult national security adjudications for this forum. Nonetheless, no reassessment of CFIUS resources required has occurred for more than a decade of its statutory existence.

The Foreign Investment Risk Review Modernization Act (FIRRMA) was signed into law on August 13, 2018, as part of the John S. McCain National Defense Authorization Act. This legislation reforms the CFIUS, most markedly by significantly expanding jurisdiction to non-controlling foreign investments and certain real property, and by mandating filings of certain covered transactions; this legislation was enacted to meet some of the needs that NSD has described. To effectuate the law's new provisions, there will be an even greater increase in work in order to secure the nation. Qualitatively, NSD performs nearly every function that supports the CFIUS process. To illustrate, NSD performs reviews and investigations of transactions and serves as the Department's representative on CFIUS and currently expects more than 1,000 cases in future years due to FIRRMA's passage. As part of the review and investigation process, NSD evaluates threat assessments and modifies them as part of the risk assessment that NSD conducts in each case. NSD also monitors compliance with all mitigation agreements (161 and growing) to which DOJ is a party, 34 of which represent an agreement associated with a CFIUS transaction. Further, NSD dedicates personnel to examine non-notified transactions in an interagency process and consistently works to bring those with national security implications before CFIUS; approximately ten percent of the cases that DOJ has co-led in 2018 alone have been brought before CFIUS by NSD as non-notified transactions. Importantly, NSD also performs a legal support function for the Department and for the interagency since NSD represents the Department head and all of its components (including litigating components and others) on CFIUS. As such, NSD must be able to interpret the law governing CFIUS, provide advice, and coordinate the varied legal specialties that impact CFIUS determinations on behalf of DOJ's senior leadership. No other counterpart office performs this integrated function. Moreover, in the immediate several months

2 Work performed by CFIUS and TT is tracked on a CY (rather than FY) basis.

following FIRRMA's passage, NSD expects to devote time and work toward drafting and negotiating regulations, supporting and engaging in pilot programs, and preparing internal legal and operational documentation required to operate under expanded jurisdiction.

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 is prepared to meet the challenge required by these increased responsibilities in effectuating this change. Specifically, in response to Administration tasking and a National Security Council-led process, the Department (through NSD) was tasked with and introduced its initial draft Executive Order for Team Telecom in August of 2017. Pursuant to guidance from the Attorney General, the Department sought to be the Chair of Team Telecom, with specific procedural norms to be detailed in a Memorandum of Understanding required by the Order. After months of input and discussion, the Department drafted a dispute resolution mechanism that received the approval of the interagency in addition to a set of timelines and associated authorities that will formalize Team Telecom and render it more transparent, efficient, and effective in meeting the national security needs of upholding the rule of law as it relates to the use of U.S. telecommunications infrastructure. NSD has the expertise required to chair the Team Telecom process; it now needs the tools to effectuate that chairmanship to achieve top quality results. Similarly, NSD also led the drafting of a telecommunications infrastructure supply chain Executive Order, which is also close to execution. NSD is prepared to represent the Department on this important committee, which will prove to be crucial to securing the nation against digital communications threats introduced via our nation's telecommunications infrastructure.

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 steadfast commitment.

2. <u>An increasing workload in intelligence oversight, operations, and litigation, especially as relates to the 2015 USA Freedom Act and the reauthorization of Section 702 of FISA</u>: 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 IC 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 this type of 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 National Security Agency (NSA) and FBI targeting decisions. While the number of targeting decisions remains classified, the government reported in the 17th Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of FISA, "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 92,707 in CY 2014 to 129,080 in CY 2017, equating to an increase of approximately 39%. The passage of the USA Freedom Act in June 2015 and the reauthorization of Section 702 resulted in many significant amendments to FISA. NSD is playing a leading role in fulfilling additional requirements, including new oversight and amicus provisions. With respect to transparency, the USA Freedom Act requires the declassification (or, where that is not possible, declassified summaries) of opinions by the FISC and Foreign Intelligence Surveillance Court of Review that involve significant or novel issues. 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. Both laws also increase the government's public reporting obligations regarding specific uses of FISA authorities.

NSD expects to see continued 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 attention to these matters to ensure successful outcomes.

3. The changing terrorism threat: As ISIS has lost territory in Iraq and Syria, former fighters have either been detained or have returned to countries where they can safely continue to operate or plan terrorist attacks and continue radicalization activities. In either case, increased and sustained engagement will be necessary to mitigate the threat posed by these individuals to the U.S. In addition, notwithstanding ISIS' loss of territory, ISIS supporters and propaganda continue to assist in the radicalization of others in the U.S. and abroad.

   NSD and the IC predict a continued trend of self-radicalized individuals engaging in terrorist attacks on government and civilian targets in the U.S. Online radicalization is a particular problem and unfortunately, foreign terrorists have targeted youth in the U.S. who are active online, resulting in complex and resource intensive juvenile prosecutions. 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.

As part of this changing threat environment, there continue to be homegrown violent extremists engaging in terrorist attacks on U.S. soil inflicting civilian casualties. Although the number of U.S. persons traveling overseas to Syria to join the conflict has been lower due to the loss of ISIS-held territory, those who traveled there in the past may return to the U.S. trained in the use of improvised explosive devices and other weapons, prepared to conduct attacks. In addition, those who have been detained following the conflict must be prosecuted by their home countries or, in some circumstances, in the U.S., to ensure they do not engage in attack planning, radicalization or recruitment that could pose a threat to the U.S. Moreover, the Department of Defense (DOD) has received and collected an extraordinary amount of enemy material which needs to be culled for possible use as evidence in foreign or U.S. based prosecutions. NSD will need to continue engagement with DOD and foreign partners to ensure that this material is used to the fullest extent possible in foreign and domestic prosecutions.

In on-going terrorism-related investigations and prosecutions, NSD has seen certain coordination within the defense bar with respect to terrorism-related prosecutions and an increase in cases going to trial in the past year. In numerous instances, NSD has been asked for assistance in managing voluminous classified and unclassified discovery in these cases and more resources are needed in order to meet the increasing needs of the USAOs for support. NSD must continue to develop a robust automated litigation services environment in order to quickly process discovery and efficiently support nationwide terrorism-related litigation.

The rising threat posed by Hezbollah and other Iran-backed foreign terrorist organizations and Specially Designated Global Terrorists must also be countered. Investigations and prosecutions involving these actors are complex and pose unique challenges that are resource intensive and frequently involve the use of classified information, resulting in complex litigation.

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. Domestic terrorism involving those seeking to use violence to achieve political goals, including environmental extremists, White Supremacists, anti-government extremists, and others, has been on the rise with acts of domestic terrorism increasing in frequency.

Each of these various threats are complex, frequently involving individuals around the globe taking action on-line using encryption technology. Thus, identifying and disrupting the threat has become increasingly resource-intensive both in terms of time and personnel.

4. <u>The need for continued engagement with, and assistance to, U.S. citizen victims and foreign governments regarding overseas terrorist attacks</u>: Americans have fallen victim in terror attacks arising from the changing terrorist threats identified earlier in this document both at home and abroad. NSD maintains the Office of Justice for Victims of Overseas Terrorism (OVT) to assist U.S. citizen victims harmed in overseas terrorist attacks that result in criminal justice proceedings abroad. This innovative program helps U.S. citizens navigate foreign justice systems by providing information, and supporting attendance and participation in foreign proceedings as permitted under foreign law. OVT faces many challenges to providing U.S. citizens harmed in attacks abroad with the highest quality information and assistance services, including obtaining

information from and about diverse and unpredictable foreign justice systems; lack of foreign government political will, systemic capacity, or security; foreign government sovereignty concerns; and U. S. Government partner coordination.

OVT supports U.S. citizen terrorism victims over the long term, no matter how long the search for justice and accountability takes. The number of cases that are active in foreign systems at any one time can vary depending on many of the factors identified above and others. OVT's monitoring and advocacy for U.S. citizen victims requires sustained and intensive efforts to research and understand foreign laws and directly engage in foreign justice systems despite barriers of unfamiliarity, distance, and language. OVT continues innovative engagement with foreign governments to encourage good practices that will benefit U.S. citizen terrorism victims involved with those systems. OVT seeks to support U.S. citizen victims who live both at home and abroad with comprehensive, efficient and compassionate services. Sufficient resources and access to information are necessary for OVT to meet the U.S. Government's commitment to U.S. citizens who suffer great losses and trauma at the hands of terrorists.

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

Item Name	Description				Page
	National Security Division	Pos.	FTE	Dollars ($000)	
Counterintelligence & Export Control, incl Cyber Threats	To support the growing mission of protecting national assets from cyber threats, including combating economic espionage and efforts by terrorists and nation states to infiltrate and damage our critical infrastructure through computer intrusions and attacks as well as protecting our nation from foreign intelligence threats.	8	4	$1,448	35
Foreign Investment Reviews to Counter Threats to Our Nation's Telecom & Other Critical Infrastructure from Intelligence Services	To support the reviews of foreign investments in U.S. industry that may impact the national security, including new requirements under FIRRMA.	21	11	$5,012	39
	NSD Total Program Changes	**29**	**15**	**$ 6,460**	

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, [$101,369,000] $109,585,000, 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.

Note.—A full-year 2019 appropriation for this account was not enacted at the time the budget was prepared; therefore, the budget assumes this account is operating under the Continuing Appropriations Act, 2019 (Division C of P.L. 115–245, as amended). The amounts included for 2019 reflect the annualized level provided by the continuing resolution.

Analysis of Appropriations Language

No change proposed.

V. Program Activity Justification

A. National Security Division

National Security Division	Direct Pos.	FTE Estimate	Amount
2018 Enacted	362	345 (Actual)	101,031,000
2019 Continuing Resolution	362	347	101,031,000
Adjustments to Base and Technical Adjustments	0	0	2,094,000
2020 Current Services	362	347	103,125,000
2020 Program Increases	29	15	6,460,000
2020 Request	391	362	109,585,000
Total Change 2019-2020	**29**	**15**	**$ 8,554,000**

National Security Division **Information Technology Breakout**	Direct Pos.	FTE Estimate	Amount
2018 Enacted	19	19 (Actual)	18,687,000
2019 Continuing Resolution	20	20	18,093,000
Adjustments to Base and Technical Adjustments	4	4	687,000
2020 Current Services	24	24	19,374,000
2020 Program Increases	0	0	-
2020 Program Offsets	0	0	-
2020 Request	24	24	18,780,000
Total Change 2019-2020	**4**	**4**	**$ 687,000**

Note: The Adjustment to Base and Technical Adjustments direct positions and FTE reflect an internal realignment of resources.

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; through reviewing, investigating, and assessing foreign investment in U.S. business assets; and through investigations and prosecutions relating to the unauthorized disclosure and improper handling of classified information;
- 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.

NSD also 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 National Security Council-led policy committees and the Deputies' Committee processes. NSD also 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 (CIA), the FBI, the DOD, and the State Department concerning questions of law, regulations, and guidelines as well as the legality of domestic and overseas intelligence operations.

NSD serves as the staff-level DOJ representative on 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 associated with transactions, and ultimately the national security risks, if any, of allowing a transaction to proceed as proposed or subject to conditions. NSD tracks and monitors transactions that were 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 license.

Finally, NSD, through its OVT, ensures that American victims of overseas terrorist attacks receive the services and support needed to navigate foreign judicial systems. 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, among other responsibilities.

IV. Program Activity Justification Performance and Resource Tables

2. Performance and Resource Tables

PERFORMANCE AND RESOURCES TABLE												
Decision Unit: National Security Division												
DOJ Strategic Goal/Objective: 1: Enhance National Security and Counter the Threat of Terrorism. Objective 1.1: Disrupt and defeat terrorist operations. Objective 1.2: Combat cyber-based threats and attacks. Objective 1.3: Combat unauthorized disclosures, insider threats, and hostile intelligence activities.												
RESOURCES		**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)**		
		FY 2018		**FY 2018**		**FY 2019**		**Current Services Adjustments and FY 2020 Program Changes**		**FY 2020 Request**		
Workload[1]												
Defendants Charged		**148**		**165**		**148**		**3**		**151**		
Defendants Closed		**128**		**163**		**128**		**3**		**131**		
Matters Opened		**130,650**		**241,825**		**175,670**		**20**		**175,690**		
Matters Closed		**130,520**		**241,850**		**175,532**		**20**		**175,552**		
FISA Applications Filed[2]		**CY 2018:**	**2,200**	**CY 2018:** Not available until April 2019		**CY 2019:**	**2,200**	**0**		**CY 2020:**	**2,200**	
National Security Reviews of Foreign Acquisitions[3]		**CY 2018:**	**300**	**CY 2018:**	**472**	**CY 2019:**	**300**	**400**		**CY 2020:**	**700**	
Total Costs and FTE		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	
		345	101,031	345	101,031	347	101,031	15	8,554	362	109,585	
TYPE	**PERFORMANCE**	**FY 2018**		**FY 2018**		**FY 2019**		**Current Services Adjustments and FY 2020 Program Changes**		**FY 2020 Request**		
Activity	**Disrupt and defeat terrorist operations**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	
		265	79,671	265	79,671	266	79,671	-6	-217	260	79,454	
Output Measure	Intelligence Community Oversight Reviews	**CY 2018:**	**105**	**CY 2018:**	Avail Apr 2019	**CY 2019:**	**105**	0		**CY 2020:**	**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.

[3]NSD has increased its CY 2020 due to the enactment of FIRRMA, which will (1) significantly expand jurisdiction to non-controlling foreign investments and certain real property and (2) mandate filings of certain covered transactions.

PERFORMANCE AND RESOURCES TABLE												
Decision Unit: National Security Division												
DOJ Strategic Goal/Objective: 1: Enhance National Security and Counter the Threat of Terrorism. Objective 1.1: Disrupt and defeat terrorist operations. Objective 1.2: Combat cyber-based threats and attacks. Objective 1.3: Combat unauthorized disclosures, insider threats, and hostile intelligence activities.												
RESOURCES		**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)**		
TYPE	**PERFORMANCE**	**FY 2018**		**FY 2018**		**FY 2019**		**Current Services Adjustments and FY 2020 Program Changes**		**FY 2020 Request**		
Outcome Measure	Percentage of CT defendants whose cases were favorably resolved	90%		91%		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%		
Activity	**Combat cyber-based threats and attacks**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	
		23	3,932	23	3,932	23	3,932	2	850	25	4,782	
Outcome Measure	Percentage of Cyber defendants whose cases were favorably resolved	90%		100%		90%		0		90%		
Activity	**Combat unauthorized disclosures, insider threats, and hostile intelligence activities**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	
		57	17,428	57	17,428	58	17,428	19	7,921	77	25,349	
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		15		14		0		14		
Output Measure	High priority national security reviews completed	CY 2018:	45	CY 2018:	100	CY 2019:	45	75		CY 2020:	120	

PERFORMANCE MEASURE TABLE										
Decision Unit: National Security Division										
DOJ Strategic Goal/Objective: 1: Enhance National Security and Counter the Threat of Terrorism. Objective 1.1: Disrupt and defeat terrorist operations. Objective 1.2: Combat cyber-based threats and attacks. Objective 1.3: Combat unauthorized disclosures, insider threats, and hostile intelligence activities.										
Strategic Objective	**Performance Report and Performance Plan Targets**		**FY 2014**	**FY 2015**	**FY 2016**	**FY 2017**	**FY 2018**		**FY 2019**	**FY 2020**
			Actual	**Actual**	**Actual**	**Actual**	**Target**	**Actual**	**Target**	**Target**
Prevent Terrorism	**Output Measure**	Intelligence Community Oversight Reviews	CY 2014: 124	CY 2015: 100	CY 2016: 110	CY 2017: 102	CY2018: 105	CY2018: Avail. April 2019	CY2019: 105	CY2020: 105
Prosecute Terrorism	**Outcome Measure**	Percentage of CT defendants whose cases were favorably resolved	92%	98%	99%	91%	90%	91%	90%	90%
Prosecute Terrorism	**Outcome Measure**	Percentage of CT cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	100%	100%	100%	100%	99%	100%	99%	99%
Investigate and Prosecute Espionage	**Outcome Measure**	Percentage of CE defendants whose cases were favorably resolved	98%	100%	100%	100%	90%	100%	90%	90%
Investigate and Prosecute Espionage	**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%
Investigate and Prosecute Espionage	**Output Measure**	FARA inspections completed	14	14	14	15	14	15	14	14
Investigate and Prosecute Espionage	**Output Measure**	High priority national security reviews completed	CY 2014: 35	CY 2015: 38	CY 2016: 43	CY 2017: 65	CY 2018: 45	CY 2018: 100	CY 2019: 45	CY 2020: 120
Combat Cyber-Based Threats and Attacks	**Outcome Measure**	Percentage of Cyber defendants whose cases were favorably resolved	N/A	100%	100%	100%	90%	100%	90%	90%

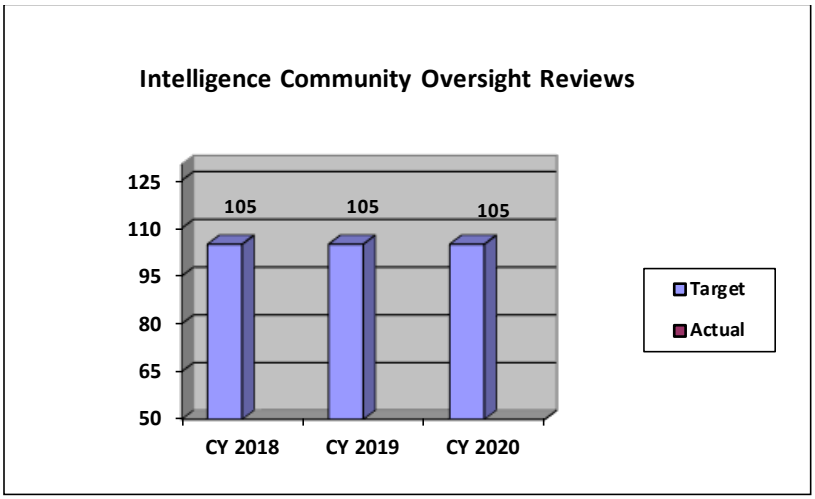
3. Performance, Resources, and Strategies

For performance reporting purposes, resources for NSD are included under DOJ Strategic Goal 1: Enhance National Security and Counter the Threat of Terrorism. Within this Goal, NSD resources address all three Objectives.

A. Performance Plan and Report for Outcomes

Objective 1.1: Disrupt and Defeat Terrorist Operations Performance Report

Measure: Intelligence Community Oversight Reviews
CY 2018 Target: 105
CY 2018 Actual: Not available until April 2019.
CY 2019 Target: 105
CY 2020 Target: 105
Discussion: CY 2020 - The CY 2020 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 IC's increased use of certain national security tools.

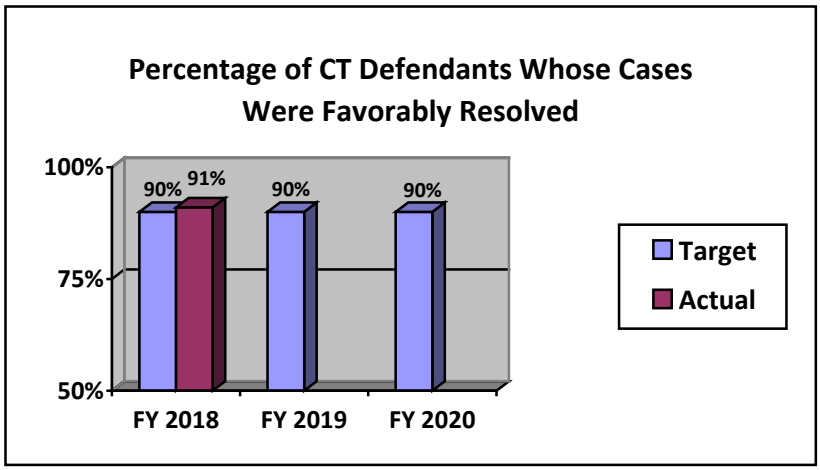


Data Definition: NSD attorneys are responsible for conducting oversight of certain activities of IC components. The oversight process involves numerous site visits to review intelligence collection activities and compliance with the Constitution, statutes, AG Guidelines, and relevant Court orders. Such 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.

Measure: Percentage of CT Defendants whose Cases Were Favorably Resolved
FY 2018 Target: 90%
FY 2018 Actual: 91%
FY 2019 Target: 90%
FY2020 Target: 90%
Discussion: The FY 2020 target is consistent with previous fiscal years. The strategies NSD will pursue in this area include 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: Data is stored and tracked in NSD's Case Management System (CMS).
Data Validation and Verification: Data validation and verification is accomplished via quarterly review by CTS management.
Data Limitations: None identified at this time.

Highlights from Recent Counterterrorism Cases
The following are highlights from recent counterterrorism cases.

U.S. v. Al Farekh: In March 2018, in the Eastern District of New York, Muhanad Mahmoud Al Farekh was sentenced to 45 years in prison following his September 2017 trial conviction of nine counts, including conspiracy to murder U.S. nationals, conspiracy to use a weapon of mass destruction, conspiracy to bomb a government facility, and conspiracy to provide material support to terrorists.

Farekh was born in the U.S. and went to college in Canada. In December 2006, he and two other men traveled from Canada to Pakistan with the intent to train for violent jihad against U.S. personnel operating in Afghanistan. Farekh was arrested in Pakistan in October 2014. After Farekh was transferred to the U.S.' custody, his fingerprints were matched to latent prints taken from an undetonated vehicle-borne improvised explosive device (VBIED) that had been used against the U.S.' Forward Operating Base Chapman in Khost Province, Afghanistan, on January 19, 2009.

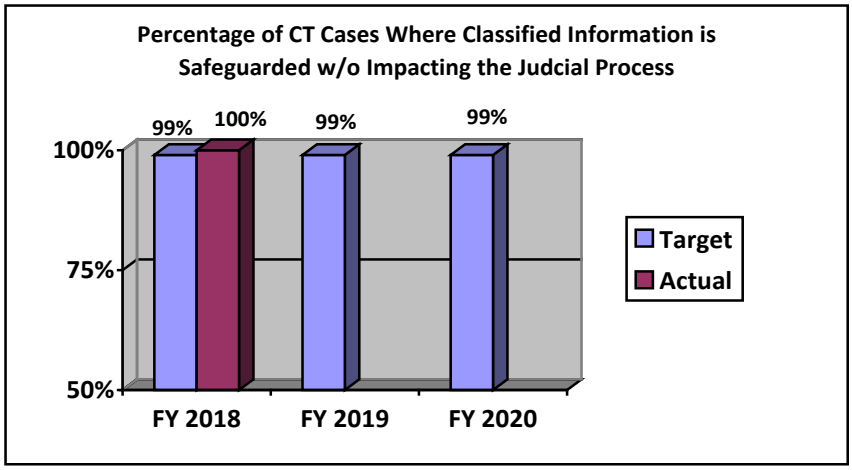
U.S. v. Nicholas Young: In February 2018, in the Eastern District of Virginia, Nicholas Young, a former police officer, was sentenced to 15 years in prison. In December 2017, Young was convicted of attempting to provide material support to the Islamic State of Iraq and al-Sham (ISIS), a designated foreign terrorist organization. According to court records and evidence presented at trial, Young was formerly employed as a police officer with the Metro Transit Police Department. In July 2016, Young attempted to provide material support and resources to ISIS by purchasing and sending gift card codes that he believed would allow ISIS recruiters to securely communicate with potential ISIS recruits.

Between December 3, 2015, and December 5, 2015, Young attempted to obstruct and impede an official proceeding. Specifically, Young believed as associate of his, who was actually an FBI confidential human source ("CHS") had successfully joined ISIS in late 2014. During an FBI interview, Young was told the FBI was investigating the attempt of his associate (the CHS) to join ISIS. Nevertheless, in an attempt to thwart the prosecution of the CHS and himself, Young attempted to deceive the investigators as to the destination and purpose of the CHS's travel. On December 15, 2016, a Grand Jury returned a four-count indictment charging Young with one count of attempting to provide material support or resources to a Foreign Terrorist Organization and three counts of obstruction of justice, specifically: (1) an attempt to obstruct and impede an official proceeding; (2) attempt to corruptly persuade another person to engage in misleading conduct to delay and hinder an investigation; and (3) attempt to provide misleading information about another's whereabouts. The Court dismissed one count of obstruction of justice during pre-trial proceedings and Young was convicted on all counts presented to the jury.

US v. Alahmedalabdaloklah: In November 2018, in the District of Arizona, Ahmed Alahmedalabdaloklah, a/k/a Ahmad Ibrahim Al-Ahmad, a Syrian national, was sentenced to life plus 30 years in prison for terrorism-related crimes.

On March 16, 2018, after a six-week jury trial, Alahmedalabdaloklah was found guilty of conspiring to use a weapon of mass destruction, conspiring to maliciously damage or destroy U.S. property by means of an explosive, aiding and abetting other persons' possession of a destructive device in furtherance of a crime of violence, and conspiring to possess a destructive device in furtherance of a crime of violence. Between approximately 2005 and 2011, Alahmedalabdaloklah designed, made, and supplied components parts for IEDs (improvised explosive devices) for members and associates of an armed Iraqi insurgent group that opposed the U.S. military presence in Iraq. The component parts were intended to be used in IEDs against U.S. military personnel and property in Iraq.

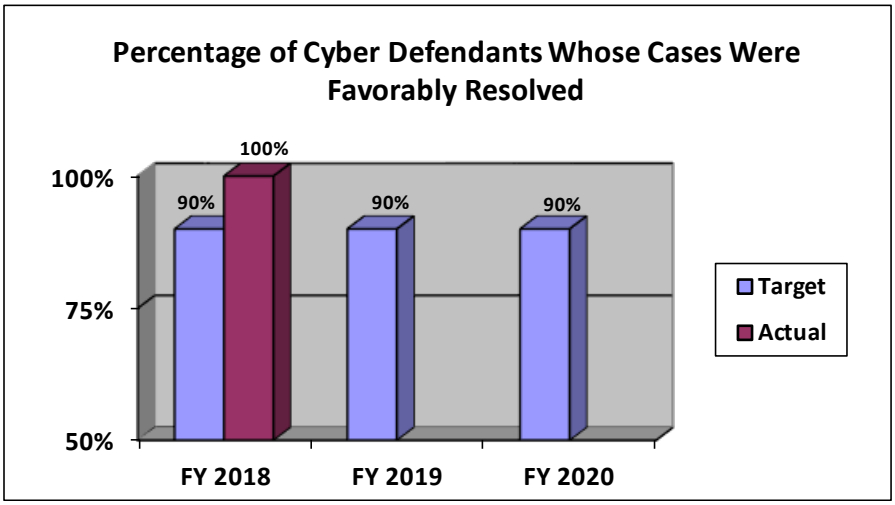
Measure: **Percentage of CT Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2018 Target: 99%
FY2018 Actual: 100%
FY 2019 Target: 99%
FY2020 Target: 99%
Discussion: The FY 2020 target is consistent with previous fiscal years. 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 is stored and tracked in CMS.
Data Validation and Verification: Data validation and verification is accomplished via quarterly review by CTS management.
Data Limitations: None identified at this time.

Objective 1.2: Combat Cyber-based Threats and Attacks Performance Report

Measure: Percentage of Cyber Defendants Whose Cases Were Favorably Resolved
FY 2018 Target: 90%
FY 2018 Actual: 100%
FY 2019 Target: 90%
FY 2020 Target: 90%
Discussion: The FY 2020 target is consistent with previous fiscal years. The strategies NSD will pursue in this area include 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, such as convictions after trial or guilty pleas. Cases dismissed based on government-endorsed motions were not categorized as either favorable or unfavorable for purposes of this calculation. Such motions may be filed for a variety of reasons to promote the interest of justice.
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 by CES management.
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.

United States v. Zhu, et al.: On December 20, 2018, in the Southern District of New York, an indictment was unsealed charging two Chinese nationals, Zhu Hua and Zhang Shilong, in relation with a decade long campaign of computer intrusions. Zhu and Zhang were members of a hacking group operating in China known within the cyber security community as Advanced Persistent Threat 10 (the APT10 Group). The defendants worked for a company in China called Huaying Haitai Science and Technology Development Company and acted in association with the Chinese

Ministry of State Security's Tianjin State Security Bureau. Through their involvement with the APT10 Group, from at least in or about 2006 up to and including in or about 2018, Zhu and Zhang conducted global campaigns of computer intrusions targeting, among other data, intellectual property and confidential business and technological information at managed service providers (MSPs), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, more than 45 technology companies in at least a dozen U.S. states, and U.S. government agencies. The APT10 Group targeted the MSPs in order to leverage the MSPs' networks to gain unauthorized access to the computers and computer networks of the MSPs' clients and to steal, among other data, intellectual property and confidential business data on a global scale. The APT10 Group targeted a diverse array of commercial activity, industries and technologies, including aviation, satellite and maritime technology, industrial factory automation, automotive supplies, laboratory instruments, banking and finance, telecommunications and consumer electronics, computer processor technology, information technology services, packaging, consulting, medical equipment, healthcare, biotechnology, pharmaceutical manufacturing, mining, and oil and gas exploration and production.

United States v. Zhang, et al.: On October 30, 2018, in the Southern District of California, an indictment was unsealed charging ten Chinese nationals, Zhang Zhang-Gui, Zha Rong, Chai Meng, Liu Chunliang, Gao Hong Kun, Zhaung Xiaowei, Ma Zhiqui, Li Xiao, Gu Gen, and Tian Xi, in relation to repeated intrusions over five years into private companies' computer systems in the United States and abroad. The conspirators included Chinese intelligence officers (Zha and Chai), both of whom worked for the Chinese Ministry of State Security's (MSS) Jiangsu Province Ministry of State Security (JSSD) in Nianjing, China, and hackers and co-opted company insiders working under the officers' direction and control. The conspiracy's alleged ultimate goal was to steal, among other data, intellectual property and confidential business information. For example, from at least January 2010 to May 2015, JSSD intelligence officers and their team of hackers focused on the theft of technology underlying a turbofan engine used in U.S. and European commercial airliners. This engine was being developed through a partnership between a French aerospace manufacturer with an office in Suzhou, Jiangsu province, China, and a company based in the United States. Members of the conspiracy, assisted and enabled by JSSD-recruited insiders, hacked the French aerospace manufacturer. The hackers also conducted intrusions into other companies that manufactured parts for the turbofan jet engine, including aerospace companies based in Arizona, Massachusetts and Oregon. At the time of the intrusions, a Chinese state-owned aerospace company was working to develop a comparable engine for use in commercial aircraft manufactured in China and elsewhere.

United States v. Khusyaynova: On October 19, 2018, in the Eastern District of Virginia, a complaint was unsealed charging a Russian national, Elena Alekseevna Khusyaynova, for her alleged role in a Russian conspiracy to interfere in the U.S. political system, including the 2018 midterm election. Khusyaynova served as the chief accountant of "Project Lakhta," a Russian umbrella effort funded by Russian oligarch Yevgeniy Viktorovich Prigozhin and two companies he controls, Concord Management and Consulting LLC, and Concord Catering. Khusyaynova allegedly managed the financing of Project Lakhta operations, including what they referred to as "information warfare against the United States." Specifically, Khuyaynova and her conspirators used social media platforms to create thousands of social media and email accounts that appeared to be operated by U.S. persons, and used them to create and amplify divisive social and political content targeting U.S. audiences. Members of the conspiracy were directed, among other things, to create "political intensity through supporting radical groups" and to "aggravate the conflict

between minorities and the rest of the population." The conspiracy also used its social media accounts to advocate for the election or electoral defeat of particular candidates in the 2016 and 2018 U.S. elections. This effort was not only designed to spread distrust towards candidates for U.S. political office and the U.S. political system in general, but also to defraud the United States by impeding the lawful functions of government agencies in administering relevant federal requirements. In addition to these criminal charges, the Department of the Treasury's Office of Foreign Assets Control (OFAC) designated Khusyaynova for sanctions for the malicious cyber-enabled activity outlined in the complaint.

United States v. Morenets, et al.: On October 4, 2018, in the Western District of Pennsylvania, an indictment was unsealed charging seven Russian nationals Aleksei Morenets, Evgenii, Serebriakov, Ivan Yermakov, Artem Malyshev, and Dmitriy Badin, Oleg Sotnikov, and Alexey Minin, all officers in the GRU, a Russian Military Federation Intelligence agency within the Main Intelligence Directorate of the Russian military. The charges pertained to the defendants' roles in a conspiracy to conduct persistent and sophisticated computer intrusions affecting U.S. persons, corporate entities, international organizations, and their respective employees located around the world, based on their strategic interest to the Russian government. Among the goals of the conspiracy was to publicize stolen information as part of an influence and disinformation campaign designed to undermine, retaliate against, and otherwise delegitimize the efforts of international anti-doping organizations and officials who had publicly exposed a Russian state-sponsored athlete doping program and to damage the reputations of athletes around the world by falsely claiming that such athletes were using banned or performance-enhancing drugs. Specifically, after compromising the systems of anti-doping organizations and officials in the United States and abroad, the defendants stole credentials, medical records, and other data, including information regarding therapeutic use exemptions (TUEs), which allow athletes to use otherwise prohibited substances. Then, using social media accounts and other infrastructure, the conspiracy publicly released selected items of stolen information, in many cases in a manner that did not accurately reflect their original form, under the false auspices of a hacktivist group calling itself the "Fancy Bears' Hack Team." As part of its influence and disinformation efforts, the Fancy Bears' Hack Team engaged in a concerted effort to draw media attention to the leaks through a proactive outreach campaign. The conspirators exchanged e-mails and private messages with approximately 186 reporters in an apparent attempt to amplify the exposure and effect of their message. In addition to these criminal charges, the Department of the Treasury's Office of Foreign Assets Control (OFAC) designated the defendants for sanctions for the malicious cyber-enabled activity outlined in the indictment.

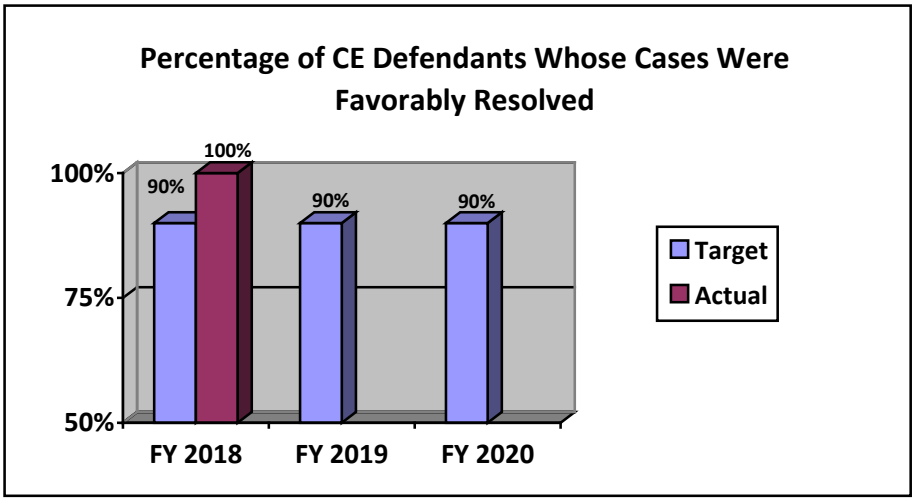
United States v. Park.: On September 6, 2018, in the Central District of California, a complaint was unsealed charging a North Korean national, Park Jin Hyok, for his alleged role in a conspiracy to conduct multiple destructive cyberattacks around the world resulting in damage to massive amounts of computer hardware, and the extensive loss of data, money and other resources. The complaint alleges that Park was a member of a North Korean government-sponsored hacking team known to the private sector as the "Lazarus Group," and worked for a front company, Chosun Expo Joint Venture, to support the North Korean government's malicious cyber actions. The conspiracy's malicious activities include the creation of the malware used in the 2017 WannaCry 2.0 global ransomware attack; the 2016 theft of $81 million from Bangladesh Bank; the 2014 attack on Sony Pictures Entertainment (SPE); and numerous other attacks or intrusions on the entertainment, financial services, defense, technology, and virtual currency industries, academia,

and electric utilities. In addition to these criminal charges, the Department made other efforts to disrupt the conspiracy's efforts. In September 2018, the Department of the Treasury's Office of Foreign Assets Control (OFAC) designated Park and the front company for which he worked, the Korea Expo Joint Venture, for sanctions for the malicious cyber-enabled activity outlined in the indictment. Also, starting in July 2018, the Department obtained court authorization to technically infiltrate a botnet used by the Lazarus Group, known as "Joanap," identify infected victim computers, and partner with the private sector and foreign partners to remediate the botnet.

United States v. Rafatnejad et al.: In March 2018, in the Southern District of New York, an indictment was unsealed charging nine Iranian nationals Gholamreza Rafatnejad, Ehsan Mohammadi, Abdollah Karima, Mostafa Sadeghi, Seyed Ali Mirkarimi, Mohammed Reza Sabahi, Roozbeh Sabahi, Abuzar Gohari Moqadam, and Sajjad Tahmasebi, with a massive cyber theft campaign. The defendants were each leaders, contractors, associates, hackers-for-hire, or affiliates of the Mabna Institute, an Iran-based company that, since at least 2013, conducted a coordinated campaign of cyber intrusions into computer systems belonging to 144 U.S. universities, 176 universities across 21 foreign countries, 47 domestic and foreign private sector companies, the U.S. Department of Labor, the Federal Energy Regulatory Commission, the State of Hawaii, the State of Indiana, the United Nations, and the United Nations Children's Fund. In targeting the universities, the defendants targeted more than 100,000 accounts of professors, leading to approximately 8,000 successful compromises. Through the defendants' activities, the Mabna Institute stole more than 31 terabytes of academic data and intellectual property from universities, which cost the universities approximately $3.4 billion to procure and access. The defendants conducted many of these intrusions on behalf of Iran's Islamic Revolutionary Guard Corps (IRGC), one of several entities within the government of Iran responsible for gathering intelligence, as well as other Iranian government and university clients. In addition to these criminal charges, the Department of the Treasury's Office of Foreign Assets Control (OFAC) designated the Mabna Institute and the nine defendants for sanctions for the malicious cyber-enabled activity outlined in the indictment.

Objective 1.3: Combat Unauthorized Disclosures, Insider Threats, and Hostile Intelligence Activities Performance Report

Measure: Percentage of CE Defendants Whose Cases Were Favorably Resolved
FY 2018 Target: 90%
FY 2018 Actual: 100%
FY 2019 Target: 90%
FY 2020 Target: 90%
Discussion: The 2020 target is consistent with previous fiscal years. The strategies NSD will pursue in this area include consulting, advising, and collaborating with prosecutors nationwide on espionage and related prosecutions and prosecutions for the unlawful export of military and strategic commodities and technology, and violations of U.S. economic sanctions.



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: Data is stored and tracked in CMS.
Data Validation and Verification: Data validation and verification is accomplished via quarterly reviews by CES management.
Data Limitations: Reporting lags.

Highlights from Recent Counterintelligence and Export Cases

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

U.S. v. Lee: In May 2018, in the Eastern District of Virginia, Jerry Chun Shing Lee was indicted by a federal grand jury on one count of conspiracy to gather or deliver national defense information to aid a foreign government, and two counts of unlawfully retaining documents related to the national defense. Lee had been arrested in January 2018 after arriving at John F. Kennedy International Airport in New York. Lee is a U.S. citizen who speaks fluent Chinese. According to the indictment, Lee was a case officer for the CIA until 2007. After leaving the CIA, Lee resided in Hong Kong. The indictment alleges that in April 2010, two Chinese intelligence officers (IOs) approached Lee and offered to pay him for information. The indictment alleges that Lee received taskings from the IOs until at least 2011. The taskings allegedly requested that Lee provide documents and information relating to the national defense of the United States. According to the indictment, the IOs provided Lee with a series of email addresses so that he could communicate covertly with them. The indictment further alleges that Lee prepared documents responsive to the taskings, made numerous unexplained cash deposits, and repeatedly lied to the U.S. government during voluntary interviews when asked about travel to China and his actions overseas. A jury trial has been scheduled for April 2019.

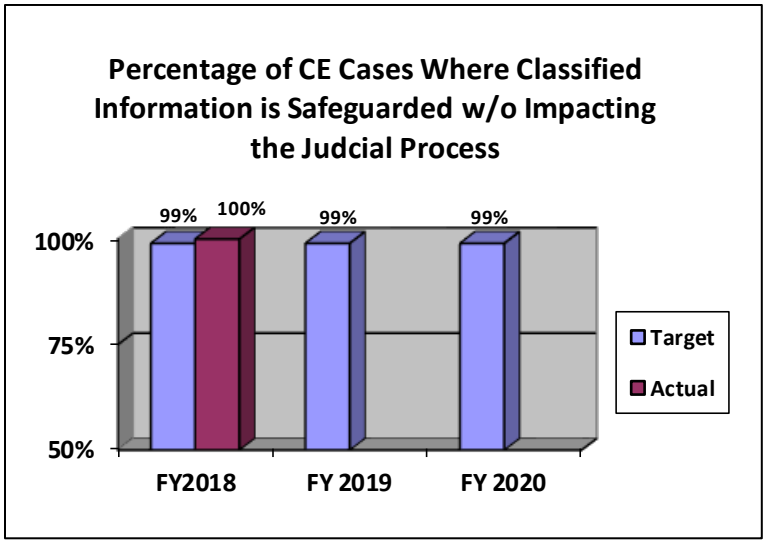
U.S. v. Albury: In April 2018, in the District of Minnesota, former FBI agent Terry J. Albury pled guilty to one count of unauthorized transmission of national defense information and one count of unauthorized retention of national defense information. According to the plea agreement, Albury used his access to classified FBI systems to copy and photograph Secret level and other sensitive materials from the FBI and other government agencies. Certain of these materials were then sent

to a reporter for a national news organization, who was not entitled to receive them. During the execution of a search in August 2017, additional materials were discovered on an electronic storage device in Albury's home with the same reporter's telephone number affixed to it. Albury was not authorized to disclose any of the materials, nor was he authorized to retain any of the materials found in his house. In October 2018, Albury was sentenced to 48 months in prison.

U.S. v. Mallory: In July 2017, in the Eastern District of Virginia, a Grand Jury issued a four-count indictment charging Kevin Patrick Mallory with delivery and attempted delivery of national defense information to aid a foreign nation; conspiracy to deliver national defense information to aid a foreign government; and materially false statements. Mallory, a self-employed consultant with GlobalEx LLC, is a U.S. citizen who speaks fluent Mandarin Chinese. For over 20 years he held positions with various U.S. Government agencies and defense contractors. Mallory obtained a Top Secret security clearance, which was active during various assignments in his career. Mallory was arrested in June 2017, after being charged by complaint with transmitting classified documents to an agent of the People's Republic of China (PRC) and making false statements during an FBI interview. The district court judge ordered Mallory detained without bond pending trial. According to the indictment, Mallory traveled to Shanghai in March and April 2017, and met with an individual (unindicted co-conspirator or UCC) he believed was working for the PRC Intelligence Service. After Mallory consented to a review of a device he had been using for private communications with UCC, the FBI viewed a message from Mallory in which he stated that he had blacked out security classification markings on documents transmitted to UCC. Analysis of the device also revealed a handwritten index describing eight different documents. Four of the eight documents listed in the index were found stored on the device, and contained information classified Secret and Top Secret. In June 2018, a trial jury found Mallory guilty on all four counts of the indictment. Sentencing scheduled for September 21, 2018, was postponed due to a potential appeal to the U.S. Court of Appeals for the Fourth Circuit.

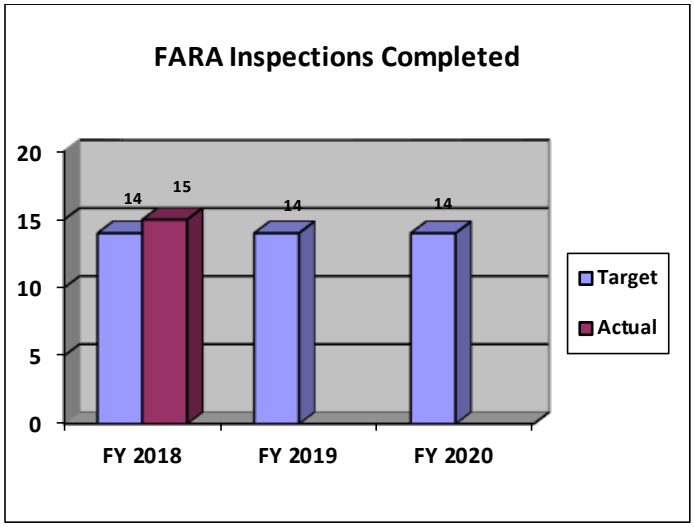
U.S. v. Winner: In June 2017, in the Southern District of Georgia, a federal grand jury returned a one-count indictment charging Reality Leigh Winner with removing classified material from a government facility and transmitting it to a news outlet. The Court ordered Winner to be detained pending trial. According to documents filed in the case, Winner was a contractor with Pluribus International Corporation assigned to a U.S. Government agency facility in Georgia. She had been employed at the facility since February 2017, and held a Top Secret/SCI clearance during that time. In May 2017, Winner printed and improperly removed intelligence reporting, which contained classified national defense information, from a U.S. IC agency, and unlawfully retained it. A few days later, Winner unlawfully transmitted by mail the intelligence reporting to an online news outlet. Once investigative efforts identified Winner as a suspect, the FBI obtained and executed a search warrant at her residence. In a conversation with FBI agents, Winner reportedly admitted intentionally identifying and printing the classified intelligence reporting at issue despite not having a "need to know," and with knowledge that the intelligence reporting was classified. Winner further admitted removing the classified intelligence reporting from her office space, retaining it, and mailing it from Augusta, Georgia, to the news outlet, which she knew was not authorized to receive or possess the documents. In August 2018, Winner was sentenced to 63 months in prison.

Measure: **Percentage of CE Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2018 Target: 99%
FY 2018 Actual: 100%
FY 2019 Target: 99%
FY 2020 Target: 99%
Discussion: The FY 2020 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 CIPA.



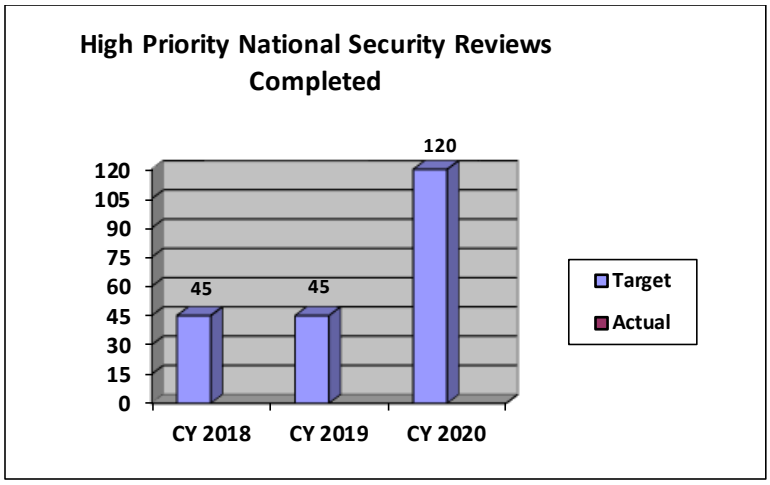
Data Definition: Classified information - information that has been determined by the United State Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data as defined by the 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: Data is stored and tracked in CMS.
Data Validation and Verification: Data validation and verification is accomplished via quarterly reviews by CES management.
Data Limitations: Reporting lags.

Measure: FARA Inspections Completed
FY 2018 Target: 14
FY 2018 Actual: 15
FY 2019 Target: 14
FY 2020 Target: 14
Discussion: The FY 2020 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 FARA Unit management.
Data Limitations: None identified at this time

Measure: High Priority National Security Reviews Completed
CY 2018 Target: 45
CY 2018 Actual: 100
CY 2019 Target: 45
CY 2020 Target: 120
Discussion: CY 2020: NSD has increased its CY 2020 due to the enactment of FIRRMA, which will (1) significantly expand jurisdiction to non-controlling foreign investments and certain real property and (2) mandate filings of certain covered transactions.
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 FIRS management.
Data Limitations: Given the expanding nature of the program area – a more centralized data system is desired.

B. Strategies to Accomplish Outcomes

NSD's performance goals support the Department's Strategic Goal 1: Enhance National Security and Counter the Threat of Terrorism. NSD takes a strategic, threat-driven, and multi-faceted approach to disrupting national security threats. Strategies for accomplishing outcomes within each of the three Strategic Objectives are detailed below:

Strategic Objective 1.1: Disrupt and defeat terrorist operations

Intelligence: NSD will continue to ensure 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 IC, 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 CIPA; 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. In addition, NSD is an integral part of the Department's Hezbollah Task Force. NSD is the focal point of domestic terrorism efforts as well through its Domestic Terrorism Executive Committee and sustained engagement on the part of its Counsel for Domestic Terrorism.

Strategic Objective 1.2: Combat cyber-based threats and attacks

Strategies that NSD will pursue in this area include recruiting, hiring, and training additional skilled professionals to work on cyber matters; prioritizing 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, regulatory, and intelligence methods; supporting and supervising the investigation and prosecution of national security-related computer intrusion cases through coordinated efforts and close collaboration with Department leadership, the FBI, the IC, other inter-agency partners, and the 94 Offices of the U.S. Attorneys; developing relationships with private sector entities, primarily online service or incident response providers, to increase the volume and speed of lawful threat information-sharing regarding national security cyber threats; coordinating and providing advice in connection with national security-related cyber intrusion cases involving the application of CIPA; promoting legislative priorities that adequately safeguard national cyber security interests; and implementing NSD's Strategic Plan for Countering the National Security Cyber Threat, which was adopted in January 2017.

Strategic Objective 1.3 Combat Unauthorized Disclosures, Insider Threats, Hostile Intelligence Activities

Strategies that NSD will pursue in this area include 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 Offices of the U.S. Attorneys; leading the review and investigation of national security-related computer-intrusion risk analyses through coordinated interagency fora such as CFIUS, Team Telecom, emerging technology councils, and supply chain regulatory bodies; implementing national strategies for combating the evolving threat of cyber-based espionage and state-sponsored cyber intrusions; overseeing and assisting with 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 support prosecutions by providing advice and assistance with application of CIPA; and enforcing FARA and related disclosure statutes.

C. Priority Goals

NSD is assisting with DOJ's efforts to meet its FY 2018 – FY 2022 Cybercrime Agency Priority Goal through the disruption of cyber threat actors and the dismantlement of their networks. Specifically, NSD tracks data that relates the percentage of cyber defendants whose cases were favorably resolved. At the end of fiscal year 2018, NSD exceeded its 90% target with a 100% actual performance. NSD opened one cyber case and closed one cyber case, which was favorably resolved.

FY18 Quarter #1= 0
FY18 Quarter #2= 0 (1 cyber case opened.)
FY18 Quarter #3= 1 (100% of cyber cases opened were favorable resolved.)
FY18 Quarter #4= 0

VI. Program Increases by Item

A. Counterintelligence and Export Control, including Cyber Threats to the National Security

Strategic Goal: Goal 1: Enhance National Security and Counter the Threat of Terrorism

Strategic Objective: 1.2: Combat cyber-based threats and attacks, and
1.3: Combat unauthorized disclosures, insider threats, and hostile intelligence activities

Budget Decision Unit(s): National Security Division

Organizational Program: Counterintelligence and Export Control Section

Program Increase: Positions 8 Atty 6 FTE 4 Dollars $1,448,000

Description of Item

NSD requests eight (8) positions, including six (6) attorneys, and two (2) paralegals and funding for 1 reimbursable detailee for its Counterintelligence and Export Control Section (CES) to support the growing mission of protecting national assets from cyber threats, including combating economic espionage and efforts by terrorists and nation states to infiltrate and damage our critical infrastructure through computer intrusions and attacks, as well as protecting our nation from foreign intelligence threats. The additional resources will also support the ongoing investigations and prosecutions of unauthorized disclosures of classified information.

Justification

National Security Cyber Investigations and Prosecutions (3 Attorneys, 1 Paralegal)

Foreign nation states increasingly use cyberspace to steal export-controlled technology, trade secrets, and intellectual property and to hold our critical infrastructure at risk to destructive or disruptive attacks. Since 2012, NSD has led a transformation in the federal government's response to significant cyber incidents by using traditional law enforcement tools to develop prosecutable cases against state actors, arresting and prosecuting them where possible, and otherwise using the resulting charges to other government agencies' tools (such as sanctions, trade remedies, and diplomacy), educate the American public about cyber threats, and encourage victim reporting and cooperation. Our ability to respond to significant incidents and develop criminal cases depends on resources, however, and those investigations must be balanced against other, high-priority counterintelligence investigations (namely, espionage and proliferation) that compete for the same resources.

NSD requires the requested additional dedicated resources to address this threat for several reasons:

(1) In addition to the extraterritorial evidential challenges present in almost every significant cyber matter, national security cyber investigations often implicate foreign policy ramifications and intelligence community equities. Those latter considerations add additional time and

coordination requirements, at a minimum, and can make it even less certain whether the investigation, which can easily span several years, will lead to criminal charges. Given other pressing criminal justice priorities, many USAOs are hesitant to devote resources to such investigations, especially in the early stages when it is least clear whether the investigation will result in a prosecutable case. Accordingly, NSD attorneys typically take the lead (or at least work jointly with AUSAs) during such investigations.

(2) Due to their pace, complexity, and data and legal process-intensive nature, national security cyber investigations often require multiple prosecutors to devote the majority of their time during the investigation period to engage with the victims and their counsel, support the FBI, marshal the evidence, and prepare charges. Two investigations that were charged in 2017 provide illustrative examples:

a. From October 2016 to March 2017, two trial attorneys from CES and one AUSA from the USAO for the Northern District of California worked with the FBI to bring charges against four hackers, including two who were officers in the Russian intelligence services, for their role in a conspiracy to hack into Yahoo's systems and webmail accounts, which led to the conspirators gaining access to account information regarding 500 million Yahoo users. During the five month period, the two CES trial attorneys devoted 85% to 100% of their time to the investigation, which translated to approximately 10 hours per business day, as well as weekends, working the investigation.

b. From February to November 2017, two trial attorneys from CES and one AUSA from the USAO for the Western District of Pennsylvania worked with the FBI to bring charges against three Chinese hackers, all of whom worked for a purported China-based Internet security firm Guangzhou Bo Yu Information Technology Company Limited (a/k/a "Boyusec"), for computer hacking, theft of trade secrets, conspiracy and identity theft directed at U.S. and foreign employees and computers of three corporate victims in the financial, engineering and technology industries. During the ten month period, one of the two CES attorneys devoted approximately 80% of her time to the investigation, which translated to approximately 7 hours per business day working the investigation.

(3) NSD will also seek a reimbursable detailee to assist/support this enhancement. Cyber detailees are a "win-win" deal for both NSD and USAOs. First, the detailees provide NSD with a necessary resource to surge towards the most high-profile and complex national security-related investigations, which as discussed above are time and resource intensive. Even though detailees often lack experience working national security investigations (hence the appeal of the detail to the detailees), they contribute other invaluable prosecutorial skills to NSD based on their years of experience in the field. Second, when the detailees return to their U.S. Attorney's Offices at the end of the detail, they bring the experience of their detail back to their districts, where they can support the relevant squads in their local FBI field offices and serve as a resource within their offices regarding the specific challenges and opportunities of national security-related cyber investigations. This exchange has a proven track record, with capable national security-related cyber practices established by detailees in their home district.

To better address the increasing caseload of significant cyber matters, CES would commit to devote five (5) attorneys (including an existing supervisor) to work almost exclusively on cyber matters, full-time, in a specially designed office suite.

Foreign Intelligence Threats (3 Attorneys, 1 Paralegal)

In recent years, NSD has seen increasingly aggressive efforts by foreign powers, particularly China, to steal U.S. national defense information and trade secrets. In FY 2018 alone, NSD had three active espionage prosecutions. The nature of these cases are very labor intensive, requiring close coordination with the IC and extensive classified litigation before a case is even ready to go to trial. The number of economic espionage investigations and prosecutions has increased, in addition to cases involving non-traditional collectors, such as covert foreign intelligence officers or their co-optees, in the U.S. Government. In one of the active espionage prosecutions, the defendant was also charged with receiving taskings from foreign intelligence officers to acquire large amounts of sensitive, but unclassified information. There have been increased efforts by foreign powers to carry out influence campaigns through representatives in the U.S. who engage in political activities or lobbying. These activities give rise to an obligation to register under the Foreign Agents Registration Act (FARA), and willful failures to register under FARA are a crime. NSD has begun initiating more criminal FARA investigations, and expects this trend to continue.

In 2017, the Division received an unprecedented number of referrals requesting investigations of disclosures of classified information (leaks), and opened an unprecedented number of such investigations, many of which remain active. The Attorney General has directed NSD to continue to prioritize these investigations. The Division continues to devote additional personnel and significant time and resources to these matters. In recent months, charges were filed against individuals in two districts for unlawfully transmitting classified national defense information, one resulting in a guilty plea.

Impact on Performance

As described above, these requests for resources are critical so that NSD can keep pace with the growing areas of protecting national assets from cyber threats and protecting our nation from foreign intelligence threats. These resources directly relate to Strategic Objectives 1.2. Combat cyber-based threats and attacks and 1.3 Combat unauthorized disclosures, insider threats, and hostile intelligence activities. The performance goals that best track success in these programs are the Percentage of Cyber Defendants whose Cases are Favorably Resolved, Percentage of Counterintelligence and Export Control Defendants whose Cases are Favorably Resolved, and FARA Inspections Completed.

Funding

Base Funding

FY 2018 Enacted				FY 2019 Continuing Resolution				FY 2020 Current Services			
Pos	Atty	FTE	$(000)	Pos	Atty	FTE	$0	Pos	Atty	FTE	$(000)
39	28	37	$10,885	39	28	37	$10,885	39	28	37	$ 11,146

Personnel Increase Cost Summary

Type of Position/Series	Full-year Modular Cost per Position ($000)	1st Year Annual-ization	Number of Positions Requested	FY 2020 Request ($000)	2nd Year Annual-ization (2021)	FY 2021 Net Annualization (change from 2020) ($000)	FY 2022 Net Annualization (change from 2021) ($000
Attorneys (0905)	$ 295	$ 176	6	$ 1,056	$ 1,625	$ 569	$ -
Paralegals / Other Law (0900-0999)	$ 164	$ 108	2	$ 217	$ 310	$ 93	$ -
Total Personnel	**$ 459**	**$ 284**	**8**	**$ 1,273**	**$ 1,934**	**$ 662**	**$ -**

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2020 Request ($000)	FY 2021 Net Annualization (change from 2020) ($000)	FY 2022 Net Annualization (change from 2021) ($000)
Reimbursable Detailee	$ 176	1	$ 176	$ 95	0
Total Non-Personnel	**$ 176**	**1**	**$ 176**	**$ 95**	**0**

Total Request for this Item

	Pos	Atty	FTE	Personnel ($000)	Non-Personnel ($000)	FY2020 Total Request ($000)	FY 2021 Net Annualization (change from ($000)
Current Services	39	28	37			$ 11,146	
Increases	8	6	4	$ 1,273	$ 176	$ 1,449	819
Grand Total	**47**	**34**	**41**	**$ 1,273**	**$ 176**	**$ 12,595**	**819**

Affected Crosscuts

National Security Division

Cyber

B. Foreign Investment Reviews to Counter Threats to Our Nation's Telecommunications & Other Critical Infrastructure from Intelligence Services

Strategic Goal: Goal 1: Enhance National Security and Counter the Threat of Terrorism
Strategic Objective: 1.3: Combat unauthorized disclosures, insider threats, and hostile intelligence activities
Budget Decision Unit(s): National Security Division
Organizational Program: Foreign Investment Review Staff

Program Increase: Positions 21 Atty 16 FTE 10 Dollars $5,012,000

	Pos	*Atty*	*FTE*	*Dollars*
Foreign Investment Review Resource Requirement	*10*	*6*	*5*	*$2,545,000*
FIRRMA Resource Requirement	*11*	*10*	*6*	*$2,467,000*
Total	*21*	*16*	*11*	*$5,012,000*

Description of Item
NSD requests twenty-one (21) positions, including sixteen (16) attorneys, one (1) senior technical expert, two (2) risk analysts, and two (2) administrative support positions, as well as funding for travel and contractor support for its Foreign Investment Review Staff (FIRS).

Justification
NSD works to prevent and disrupt national security threats, not merely to react to them after the fact. It is particularly critical that we do so in the field of counterintelligence---preventing foreign intelligence services from access to sensitive information and technology. We do this in part through FIRS, which reviews foreign investments in the U.S. for national security risks, mitigates those risks through contractual agreements with the parties to the transaction, and monitors compliance with those mitigation agreements going forward. NSD prioritizes those transactions that could pose a risk to the security of the telecommunications sector, to law enforcement or intelligence community equities (e.g., tools, techniques, facilities, and jurisdiction), to personal information or privacy (e.g., PII and PHI), or that which may otherwise give a foreign intelligence service access to a collection platform in the U.S. Our increasing reliance on computer and telecommunications networks means that cybersecurity is a significantly increasing component of FIRS's reviews.

FIRS reviews transactions in two capacities, as the Department's representative on the Committee on Foreign Investment in the United States (CFIUS), and as the *de facto* chair of Team Telecom (an *ad hoc* Executive Branch committee that advises the FCC on whether to grant certain telecommunications license applications). The number of CFIUS case filings have continued to increase dramatically (affecting the entire Committee's workload), and FIRS has been even more aggressive in leading an increasing share of that workload. For example, although CFIUS reviewed a record number of transactions in 2016 (a total of 172), the total in 2017 was 40% greater, and there was a similar number reviewed in 2018. In addition to a surge in *volume*, the *complexity* of the cases is increasing, with larger numbers of cases involving companies with potential connections to determined foreign adversaries. Such cases have increased from about 3% of the docket in 2010 to almost consistently 30% of the docket in the

last three years. FIRS has risen to the challenges posed from this increase by leading more cases in 2017 than in the prior five years *combined*, and FIRS has been responsible for approximately half of the significant national security actions that CFIUS took in the last year. This trend was expected to continue prior to the passage of FIRRMA. As previously described, FIRRMA significantly expands the jurisdiction of CFIUS, and in order to effectuate the law's new provisions, there will be an even greater stark increase in work in order to secure the nation. NSD performs nearly every function that supports the CFIUS process, and therefore, a further expansion of resources is needed to meet the requirements of the new statute.

In addition to a surge in *volume*, the *complexity* of the cases is increasing, with larger numbers of cases involving companies with potential connections to determined foreign adversaries. Such cases have increased from about 3% of the docket in 2010 to almost consistently 30% of the docket in the last three years. FIRS has risen to the challenges posed from this increase by leading more cases in 2017 than in the prior five years *combined*, and FIRS has been responsible for approximately half of the significant national security actions that CFIUS took in the last year. FIRS anticipates this historic pace to continue or even increase into FY 2020. Unlike counterpart offices in other agencies, NSD performs nearly every function that supports the CFIUS process. To illustrate, NSD performs reviews and investigations of transactions and represents the Department on the Committee; NSD expects the number of filings to exceed 1,000 in future years due to FIRRMA's passage. As part of the review and investigation process, NSD evaluates threat assessments and modifies them as part of the risk assessment that NSD conducts in each case. NSD also monitors compliance with all mitigation agreements (161 and growing) to which DOJ is a party, 34 of which represent an agreement associated with a CFIUS transaction.

NSD also performs a legal support function for the Department and for the interagency since NSD represents the head of the agency and all of its components (including litigating components and others) on CFIUS. As such, NSD must be able to interpret the law governing CFIUS, provide advice, and coordinate the varied legal specialties that impact CFIUS determinations on behalf of DOJ's senior leadership. No other counterpart office performs this integrated function. Moreover, in the immediate several months following FIRRMA's passage, NSD expects to devote time and work toward drafting and negotiating regulations, supporting and engaging in pilot programs, and preparing internal legal and operational documentation required to operate under expanded jurisdiction.

In Team Telecom, a group of challenging license applications before the Federal Communications Commission (FCC) have highlighted difficulties with the *ad hoc* process that FIRS runs on behalf of DOJ and other security agencies. Pressure from industry and the FCC to review license applications within 180 days (or less)---far below the committee's current average of more than 200 days to close a review (not counting reviews that have remained pending for years)---has led the Administration to seek to formalize this process with stricter timelines, an administrative chair, and a more structured interagency process. In response to Administration tasking, in August of 2017, the Department (through NSD) drafted an Executive Order to formalize Team Telecom and (under guidance from the Attorney General) in which it sought to be its Chair. After months of negotiation in the interagency, the Executive Order was approved by Deputies in June, 2018. The Order is poised to be signed by the President in CY18, at which point NSD will become formally responsible for ensuring all transactions, even the most complex, are initially reviewed within 120 days and resolved within a year. Chairing Team

Telecom and shepherding roughly 40 new applications per year through its process will require additional administrative, technical, and legal resources, as the Department will be more formally responsible for the recommendations the Executive Branch makes to the FCC. NSD has the expertise required to chair the Team Telecom process; it now needs the tools to effectuate that chairmanship to achieve top quality results for the nation.

As to both processes, NSD is unique among operational foreign investment components in the interagency, because it offers legal advice as well as policy views. As such, it was NSD that the National Security Council (NSC) tasked to draft a telecommunications infrastructure supply chain Executive Order (which was also approved by Deputies in June, 2018). We anticipate NSC will continue to look to the Department as regulations are promulgated.

Finally, to meet all of the needs and mission critical activities described above, NSD requires additional funds for travel to continue to monitor compliance with existing national security agreements. These agreements were developed as a result of case reviews, and technical contract support to allow for increased contract time spent in assisting the government to review active case matters, monitor deliverables and support site visits already required by existing agreements.

Impact on Performance

Additional personnel resources dedicated to foreign acquisitions oversight and critical infrastructure protection will enhance the NSD's ability to ensure that our Nation's sensitive technologies and critical infrastructure are protected from foreign ownership or control, particularly in light of the recent passage of FIRRMA. While NSD anticipates a significant increase in workload directly resulting from FIRRMA, the extent of this increase in out years may be difficult to predict. Therefore, NSD will continue to assess the need for additional resources in the future.
This request supports the Strategic Objective 1.3 Combat unauthorized disclosures, insider threats, and hostile intelligence activities, and its success is measured in part by the High Priority National Security Reviews Completed performance goal.

Funding

Base Funding

FY 2018 Enacted				FY 2019 Continuing Resolution				FY 2020 Current Services			
Pos	Atty	FTE	$(000)	Pos	Atty	FTE	$(000)	Pos	Atty	FTE	$(000)
13	9	12	$3,628	13	9	12	$3,628	13	9	12	$ 3,715

Foreign Investment Review Resource Requirement

Personnel Increase Cost Summary

Type of Position/Series	Full-year Modular Cost per Position ($000)	1st Year Annualization	Number of Positions Requested	FY 2020 Request ($000)	2nd Year Annualization (2021)	FY 2021 Net Annualization (change from 2020) ($000)	FY 2022 Net Annualization (change from 2021) ($000)
Senior Technical Expert	$ 295	$ 176	1	$ 176	$ 271	$ 95	$ -
Risk Analysts	$ 235	$ 146	2	$ 291	$ 421	$ 130	$ -
Adminstrative Support/Clerical and Office Services (0300-0399)	$ 100	$ 63	1	$ 63	$ 90	$ 27	$ -
Attorneys (0905)	$ 295	$ 176	6	$ 1,056	$ 1,625	$ 569	$ -
Total Personnel	**925**	**561**	**10**	**1,586**	**2,406**	**820**	**$ -**

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2020 Request	FY 2021 Net Annualization (change from 2020)	FY 2022 Net Annualization (change from 2021)
			$(000)	$(000)	$(000)
Travel	$ 50		$ 50		$ -
Contractor Support	$ 909		$ 909		$ -
Total Non-Personnel	**$ 959**		**$ 959**		**$ -**

FIRRMA Resource Requirement

Personnel Increase Cost Summary

Type of Position/Series	Full-year Modular Cost per Position ($000)	1st Year Annual-ization	Number of Positions Requested	FY 2020 Request ($000)	2nd Year Annual-ization (2021)	FY 2021 Net Annualization (change from 2020) ($000)	FY 2022 Net Annualization (change from 2021) ($000
Clerical and Office Services (0300-0399)	$ 100	$ 63	1	$ 63	$ 89	$ 26	$ -
Attorneys (0905)	$ 295	$ 176	10	$ 1,760	$ 2,708	$ 948	$ -
Total Personnel	**$ 395**	**$ 239**	**11**	**$ 1,823**	**$ 2,796**	**$ 974**	**$ -**

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2020 Request ($000)	FY 2021 Net Annualization (change from 2020) ($000)	FY 2022 Net Annualization (change from 2021) ($000)
Contractor Support	$ 644	N/A	$ 644	$ -	0
Total Non-Personnel	**$ 644**	**0**	**$ 644**	**$ -**	**0**

Total Request for this Item

	Pos	Atty	FTE	Personnel ($000)	Non-Personnel ($000)	FY2020 Total Request ($000)	FY 2021 Net Annualization (change from 2020) ($000)
Current Services	13	9	12			$ 3,715	
Increases	21	16	12	$ 4,368	$ 644	$ 5,012	$ 1,794
Grand Total	**34**	**25**	**24**	**$ 4,368**	**$ 644**	**$ 8,727**	**$ 1,794**

Affected Crosscuts

National Security Division

VII. Program Offsets by Item (Not Applicable)

VIII. Exhibits