FY 2021
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) 2021 a total of 402 positions (including 269 attorneys), 353 FTE, and $117,451,000.[1]

B. Background

1. Operational Focus Areas.

- 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.

2. Division Structure.

NSD strengthens DOJ'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 DOJ'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 DOJ'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 following sections:

- Office of Intelligence (OI);
- Counterterrorism Section (CTS);
- Counterintelligence and Export Control Section (CES);

[1] Within the totals outlined above, NSD has included a total of 26 positions, 24 FTE, and $18,249,000for Information Technology (IT).

- Office of Law and Policy (L&P);
- Foreign Investment Review Staff (FIRS);
- Office of Justice for Victims of Overseas Terrorism (OVT);
- Executive Office (EO)

C. NSD Major Responsibilities.

1. 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 DOJ 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 DOJ's primary liaison to the Director of National Intelligence and the IC.

2. Counterterrorism

- Promoting and overseeing a coordinated national counterterrorism enforcement program, through close collaboration with DOJ 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 DOJ 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.

3. Counterintelligence and Export Control.

- Developing, and supervising the investigation and prosecution of espionage and related cases through coordinated efforts and close collaboration with DOJ 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.

4. Victims of Terrorism.

- Supporting U.S. citizen victims of terrorism overseas by helping them navigate foreign criminal justice systems and advocating for their voices to be heard around the world.;
- Collaborating closely with interagency, foreign governmental, and private partners to assist U.S. citizen terrorism victims;
- Participating in the Council of Europe's 24/7 counterterrorism network for victims of terrorism to provide timely and coordinated communication between designated government points of contact; and,
- Participating in the informal International Network to Support Victims of Terrorism and Mass Violence (INVICTM), which is composed of government and non-government direct service providers to cross border victims of international terrorism attacks worldwide.

5. 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 NSD and DOJ leadership;

- Providing legal assistance and advice on matters arising under national security laws and policies, and overseeing the development, coordination, and implementation of DOJ-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 DOJ's participation in the National Security Council (NSC).

6. Foreign Investment.

- Performing the DOJ'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 DOJ's views relating to the national security implications of certain transactions relating to FCC licenses;

- Tracking and monitoring certain transactions approved pursuant to this process; and,

- Conducting community outreach and corporate engagement relating to national security issues in coordination with law enforcement and IC partners.

- Providing legal advice and policy support on legislative and policy matters involving national security issues, including developing and commenting on legislation, executive orders, and NSC policy committees at the intersection of national security, international trade, law, policy, and high and emerging technology.

D. Recent Accomplishments (UNCLASSIFIED only).

- **Evolving threat of terrorism.** Since 2014, DOJ has charged publicly more than 170 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, and individuals inspired by ISIS to plot violent acts in the United States, but were arrested before leaving the United States or disrupted before they could take action. In addition, NSD prosecutors have provided technical assistance and case mentoring to foreign counterparts for cases involving returned foreign fighters. Further, NSD has provided case mentoring on other terrorism-related matters to prosecutors in Peru, Kenya, the Maldives, and other locations.

- **Terrorism-Related Convictions.** Over the past year, NSD, in partnership with USAOs, secured numerous convictions and sentences, including:
  - Conviction against a Hizballah operative who conducted surveillance on potential targets in the United States;
  - Conviction of BOP inmate for attempting to provide material support to a Foreign Terrorist Organization (FTO) (conduct occurred while the inmate was serving a sentence for a 2012 conviction for conspiring to provide material support to another FTO).
  - Conviction and life sentence against a terrorist who carried out a knife attack in an airport in Michigan;
  - Conviction and 20 year sentence for an individual who sent packages with explosives to a

number of public figures;

- Life sentence for a terrorist who supplied improvised explosive devices to Iraqi insurgents who used the devices against U.S. military personnel from 2005 to 2010;
- Multiple convictions of individuals who attempted to purchase chemical or biological weapons through the Dark Web;
- 27 year sentence for an individual who attempted to bomb a police station in Colorado;
- Conviction and 20 year sentence for an individual who published bomb making instructions and advocated for violence against Americans; and,
- Conviction against an ISIS-supporter who joined an online hacking group that pledged allegiance to ISIS and disseminated ISIS propaganda online.

- **Countering Terrorism Financing and Support.** NSD engaged in a wide range of legal and policy work to counter terrorist financing and support sanctions programs. NSD worked closely with the Department of State to designate Foreign Terrorist Organizations, or to review, amend, or revoke existing designations as required by law. NSD reviewed 13 such Foreign Terrorist Organization designations, amendments, or revocations. NSD reviewed over 500 potential targets for sanctions designations under relevant Executive Orders.

- **China Initiative.** In November 2018, the DOJ announced the China Initiative, which is led by the NSD's Assistant Attorney General. This initiative prioritizes resources to combat the wide-ranging national security threats posed by the People's Republic of China (PRC). The China Initiative emphasizes threats of economic espionage and theft of trade secrets in sectors where the PRC government is seeking global dominance. Over the last year, NSD has pursued a number of high-priority economic espionage and trade secret theft cases, each of which involved China. Recent examples of these prosecutions include:

  - First extradition of a Chinese foreign intelligence officer to the United States, Yanjun Xu. XU was charged in the Southern District of Ohio with attempting and conspiring to commit economic espionage and steal trade secrets from U.S. aviation companies;
  - Charging Xioaorong You, a Chinese national, in the Eastern District of Tennessee with theft of trade secrets related to formulations of bisphenol-A-free (BPA-free) coatings, as part of a plan to set up a competing business in China;
  - July 2019 conviction Shan Shi by a jury in the District of Columbia for conspiring to steal trade secrets from a Houston-based company related to syntactic foam, which has commercial and military uses.

- In addition, the DOJ has leveraged other agencies' enforcement authorities to counter the threat posed by China in stealing U.S. technology. Recent examples of this include:

  - Charges against United Microelectronics Corp., a Taiwanese company, and Fujian Juihua Integrated Circuit Co, a state owned Chinese company, in the Northern District of California, for economic espionage related to their theft of dynamic random access (DRAM) technology from a major U.S. corporation.
  - DOJ worked with Department of Commerce to add the Chinese companies to entity list and brought a civil suit to bar the companies from exporting any goods that infringe upon

the U.S. victim company's intellectual property (IP) to the United States.

- **Espionage Act Enforcement.** Over the past year, NSD continued its enforcement of the Espionage Act by successfully prosecuting three defendants for espionage offenses related to the PRC.

  - In 2018, following a jury trial, Kevin Mallory was convicted in the Eastern District of Virginia for conspiring to commit espionage and was sentenced to 20 years of imprisonment in 2019.
  - In 2019, Ron Hansen pled guilty in the District of Utah for attempting to commit espionage and was sentenced to 10 years of imprisonment.
  - In 2019, Jerry Lee pled guilty in the Eastern District of Virginia for conspiring to commit espionage and was sentenced to 19 years of imprisonment.

- **Combatting Malign Foreign Influence.** NSD significantly increased its efforts to combat malign foreign influence, primarily through rigorous FARA enforcement. In 2018 alone, more than twenty individuals and entities were criminally charged with violations involving FARA.

  - In July 2019, Bijan Rafiekian was convicted by a jury of conspiring to make false statements in a FARA filing and acting as an agent of the government of Turkey without notifying the Attorney General. The judge later overturned that conviction, and it is currently under appeal.
  - In 2019, DOJ obtained a court order that required the registration of a U.S. agent of a Russian state-owned media enterprise. This was DOJ's first successful utilization of its civil enforcement authority since 1991.
  - DOJ also obtained a civil settlement with a prominent law firm, Skadden, Arps, Slate, Meagher & Flom LLP, for failing to register under FARA in 2012 for its work on behalf of the government of Ukraine. As part of the settlement, Skadden agreed to pay the U.S. Treasury more than $4.6 million, which reflected the fees and expenses Skadden received for its work with Ukraine.
  - During FY 2019, NSD also conducted 30% more inspections of registrant books and records than the prior year.

- **Export Controls and Sanctions Enforcement.** NSD continued its rigorous enforcement of export controls and sanctions, including sanctions against Iran and North Korea. Recent examples cases include:
  - In January 2019, NSD and the USAO in the Eastern District of New York charged Chinese telecommunication company Huawei with, among other charges, violating Iran sanctions. The indictment alleges Huawei was using the U.S. financial system in support of its business in Iran and lying to its banks about this conduct;
  - In May 2019, NSD and the USAO for the Southern District of New York seized a North Korean bulk carrier ship, the Wise Honest. The ship was being used to export coal from North Korea to foreign purchasers and to import machinery to North Korea;
  - In October 2019, NSD and the USAO for the Southern District of New York announced charges against Halkbank, a Turkish state-owned bank, for offenses related to the bank's participation in a multibillion-dollar scheme to evade U.S. sanctions on Iran.

- **National Security Cyber Cases.** NSD continued to focus resources on bringing charges in complex national security cyber cases and on disrupting adversaries' efforts to harm U.S. national security through cyber intrusions and attacks. Recent example cases include:

  - NSD and the USAO for the Southern District of New York charged two Chinese nationals with criminal offenses based on their involvement in the hacking group associated with the Chinese Ministry of State Security (known as APT 10), which conducted global campaigns of computer intrusions targeting managed service providers.

- **Combatting Russian Hacking and Disinformation.** NSD is actively prioritizing efforts to combat Russian efforts to hack and conduct disinformation campaigns. NSD has conducted investigations of malicious "hack-and-dump" misinformation schemes perpetrated by the Russian Main Intelligence Directorate (GRU). Recent case examples include:

  - In July 2018, NSD's efforts led to the Special Counsel's Office's charges in the District of Columbia against 12 GRU officers for their roles in interference efforts directed towards the 2016 U.S. presidential election.
  - Separate indictment in the Western District of Pennsylvania against seven GRU officers for their role in the targeting of international anti-doping organizations and the subsequent leak of Olympic athletes' private medical data through a false flag website hacktivist group, the "Fancy Bears Hacking Team." NSD's efforts led to the seizure of GRU's online infrastructure that they were using to disseminate the stolen data and peddle anti-doping-related disinformation.

- **Foreign Interference in U.S. Elections.** NSD played a significant role in developing policies and decision frameworks to address foreign interference in U.S. elections. Working with the NSC and other agencies, NSD helped develop and implement Executive Order (EO) 13848, Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election, including helping develop sanctions pursuant to the EO. NSD also helped lead efforts to develop frameworks to respond to election interference, including guidance for the collection and disclosure of information relating to election interference.

- **Unauthorized Public Disclosures.** NSD has also continued to prioritize cases involving unauthorized disclosures to the media. In 2018, it obtained the highest sentences to date in such cases:
  - 63 months for Reality Winner in the Southern District of Georgia;
  - 48 months for Terry Albury in the District of Minnesota.
  - In 2019, NSD has charged three individuals for unauthorized disclosures to the media or organizations.

- **Foreign Investment Review.** NSD's robust engagement in foreign investment review supports DOJ's China Initiative as well as NSD's general responsibilities to enhance national security.

  - NSD reviewed approximately 40% more submissions in 2019 than the previous year regarding mergers, acquisitions, and investments.
  - NSD led (on behalf of DOJ) approximately 18% of the cases in which a Joint Voluntary

Notice was filed with CFIUS in 2019. In approximately 38% of those cases, the transaction was prohibited, abandoned, or mitigated (or anticipated to require prohibition or mitigation, for pending cases), based on national security risk identified by NSD.

- NSD also led (on behalf of DOJ) approximately 10% of the cases in which a declaration was filed with CFIUS pursuant to the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) pilot program for critical technologies.

- **Regulations Implementing FIRRMA.** NSD also worked closely with the Department of the Treasury to draft proposed regulations implementing FIRRMA. These regulations were published for comment in October 2019 and will be promulgated in early 2020.

- **FCC Referrals to Team Telecom.** NSD serves as the informal chair of the Team Telecom, an interagency group that reviews telecommunications, submarine cable landing, wireless, and broadcast license applications for national security and law enforcement interests.

  - NSD led or co-led approximately 91% of the reviews for licenses from the FCC referrals to Team Telecom in 2019.
  - In 2019, Team Telecom recommended to the FCC that 38 of the total authorizations, licenses, and petitions for declaratory relief (stemming from 12 FCC referrals) be granted contingent on mitigation measures. NSD led or co-led approximately 87% of the cases that led to those dispositions.

- **Efforts in CFIUS and Team Telecom Cases.** NSD led four CFIUS cases and seven Team Telecom cases in 2019 that resulted in national security agreements that NSD negotiated and entered into with companies, and that NSD will monitor for compliance going forward. The total number of such agreements monitored by NSD is 175, which reflects an approximate 27% increase in priority national security risk areas for DOJ. NSD also conducted approximately 35 site visits in 2019 to monitor companies' compliance, and investigated a significant breach by a company of a national security mitigation agreement, which led to a penalty assessment.

- **Section 702 Compliance.** As part of its oversight responsibilities, NSD reviews all taskings under the Section 702 program to ensure compliance with the law. While the number of targeting decisions remains classified, the unclassified estimated number of targets reported in the Statistical Transparency Report Regarding Use of National Security Authorities provides a helpful parallel. Section 702 targets have significantly increased in scope over the last several years: CY 2014 reported 92,707 targets; CY 2017 reported 129,080 targets; and, CY 2018 reported 164,770 targets, which represents a growth of 27.6% from CY2017. Additionally, in CY2019, NSD conducted over 30 reviews at IC agency headquarters locations and just under 30 reviews at non-IC headquarters locations to assess compliance with acquisition, retention and/or dissemination requirements of Section 702 authorities.

- **FISA Activities.** NSD litigated and obtained seven favorable rulings upholding FISA authorities as lawful in 2018-2019. NSD reviewed and authorized requests to use FISA-obtained or -derived information in various criminal prosecutions, including the recent CES cases against Shan Shi, Ron Rockwell Hansen, Jerry Lee, and Huawei, and the recent CTS cases against Ali Kourani, Muhanad Mahmoud al Farekh, Erick Jamal Hendricks, and

Nicholas Young (all described below).

- **Threats to Information and Telecommunications Supply Chains.** In 2019, NSD worked closely with the NSC, Department of Commerce, and other agencies to draft regulations implementing EO 13873. NSD originally drafted this EO, which the President signed in May 2019. EO 13873 strengthens Executive Branch authorities and procedures for addressing supply chain threats to the telecommunications and information communications technology sectors. NSD has worked closely with the Department of Commerce to draft implementing regulations pursuant to this EO.

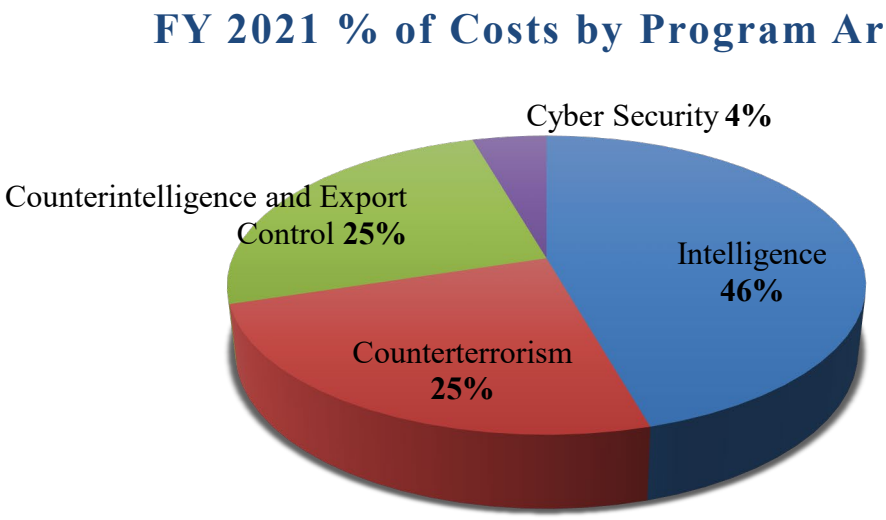
- **Assisting Victims of Overseas Terrorism.** NSD OVT continued to assist U.S. citizen victims of overseas terrorism to attend proceedings and participate in foreign criminal justice systems. Since the beginning of FY 2017, NSD OVT has provided travel support for U.S. victim attendance and/or court accompaniment at seven foreign proceedings, including proceedings in Israeli Military Court, Jordanian Military Court, United Kingdom Coroner's Inquests, and Dutch civilian criminal court. In all these cases, U.S. victims chose to provide victim impact statements to the courts, consistent with their rights under foreign law.

- **Supporting International Cooperation on Victims of Terrorism.** NSD OVT partnered with the U.S. Mission to the United Nations (UN) in the inception, development and drafting of the UN draft resolution "Enhancement of International Cooperation to Assist Victims of Terrorism," which the UN General Assembly adopted by consensus on June 28, 2019.

- **Countering UAS Threats.** NSD led DOJ's implementation of 2018 legislation granting DOJ the authority to use counter and mitigate the threat of Unmanned Aircraft Systems (UAS) technologies to designated facilities and assets. While DOJ-wide guidance was being developed, NSD worked closely with the FBI to develop required Attorney General guidelines specifically to use the new counter-UAS authority to protect the Super Bowl LIII event. Using the authority, the FBI detected and seized dozens of drones flying near the Super Bowl stadium.

E. 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.



F. Performance Challenges

1. Increasing And Changing Threats To U.S. National Assets, Including Significant Cyber Threat Growth.

One of NSD's top priorities 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 United States national and economic security.

Foreign governments and other non-state adversaries of the United States are engaged in aggressive campaigns to acquire superior technologies and commodities developed in the United States, in contravention of export control and sanctions laws. The United States confronts increasing threats from the unlawful shipments and deliveries of physical commodities and equipment, and also threats from the theft of proprietary information and export-controlled technology. These threats often manifest through cyber-attacks and intrusions of computer networks, as well as through insider threats.

The most sophisticated of the United States' adversaries employ multi-faceted campaigns to acquire valuable proprietary technologies and information through a combination of traditional and asymmetric approaches. For example, the United States' nation-state adversaries increasingly rely on

commercial and other non-state entities to conduct economic espionage, which is creating a new threat vector that is especially difficult to investigate. NSD plays a central role in addressing these threats through comprehensive, multi-faceted approaches that leverage the full array of options under existing legal authorities.

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, 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. In CY2019 (and even without the impact yet of forthcoming regulations, discussed below), overall NSD reviewed approximately 40 percent more submissions than in 2018 regarding mergers, acquisitions, and investments.

In 2019, NSD (on behalf of DOJ) led approximately 18 percent of CFIUS cases in which a Joint Voluntary Notice was filed, and of those cases led by NSD, approximately 38 percent resulted in the transaction being prohibited, abandoned, or mitigated, based on national security risk identified by NSD. NSD (on behalf of DOJ) also led approximately 10 percent of the cases in which a declaration was filed with CFIUS pursuant to the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) pilot program for critical technologies. With respect to Team Telecom, in addition to serving as the informal chair of that interagency group, NSD also led or co-led approximately 91 percent of the group's reviews in 2019. Of the group's total number of reviews in 2019, Team Telecom recommended to the FCC that 38 of the total authorizations, licenses, and petitions for declaratory relief (stemming from 12 FCC referrals) be granted contingent on mitigation measures. Of the total number of cases that led to those dispositions, approximately 87 percent were cases led or co-led by NSD.

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 new and evolving national security issues. DOJ led more cases in CY 2017 than it had in the previous 5 years, combined, because NSD needed to address the national security concern presented on behalf of the Executive Branch, and DOJ continued that sharply increased pace in 2018 and 2019, which has resulted in higher priority national security reviews (directly related to cyber security).

FIRRMA was enacted in 2018, as part of the John S. McCain National Defense Authorization Act. This legislation reforms 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 enact 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. NSD performs reviews and investigations of transactions, serves as DOJ's representative on CFIUS, and currently expects more than 1,000 cases in CY 2021 due to the passage of FIRRMA. 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

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

agreements (approximately 175 and growing) to which DOJ is a party, 40 of which represent an agreement associated with a CFIUS transaction.

As time goes on and the volume of CFIUS and Team Telecom cases increase, the volume of mitigation agreements that NSD must monitor will also steadily increase. Of the CFIUS and Team Telecom cases discussed above, 4 CFIUS cases and 7 Team Telecom cases led or co-led by NSD in 2019 resulted in national security agreements that NSD negotiated and entered into with companies, and that NSD will monitor for compliance going forward. Of the approximately 175 mitigation agreements monitored by NSD, priority agreements increased by 27 percent from 2018 to 2019. 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 11 percent of the cases that DOJ co-led in 2019 alone have been brought before CFIUS by DOJ as non-notified transactions.

Importantly, NSD also performs a legal support function for DOJ 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 approximately one-and-a-half years following passage of the FIRRMA, NSD devoted significant time and work toward drafting and negotiating regulations, supporting and engaging in a pilot program, and preparing internal legal and operational documentation required to operate under expanded jurisdiction.

With respect to Team Telecom, 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 effecting this change, and is actively developing ways to achieve the goal of institutionalizing the governance of Team Telecom, including by formalizing DOJ's role as chair of the group.

Now that the President has signed Executive Order 13873 in May 2019, NSD has been actively involved in helping the Department of Commerce draft regulations to implement this new authority, and is prepared to represent DOJ on this important new committee, which will prove to be crucial to securing the nation against digital communications threats introduced via the United States' 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. IC representatives have assessed that cyber threats may soon surpass traditional terrorism threats. NSD must be prepared to continue to take lessons learned over the past decade and adapt them to this new threat. Highly technical cyber threats require time-intensive and complex investigative and prosecutorial work. Cyber threat investigation challenges include their novelty, difficulties of attribution, challenges presented by electronic evidence, the cyber activity speed and global span, 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 and to recruit and hire personnel with cyber skills and full-time focus on these issues. 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. 2015 USA Freedom Act And The Reauthorization Of Section 702 Of FISA - Increasing Workload In Intelligence Oversight, Operations, And Litigation.

NSD's intelligence-related work supports the U.S. Government's national security mission fully, including combating the threats posed by terrorists, threats to the United States' cybersecurity, espionage, economic espionage, and weapons of mass destruction. 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 this threat increase over the last few years, with ISIS recruiting and radicalizing online an increasing number of U.S. persons. This threat will likely to continue for some time.

NSD's oversight work is an essential 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 indicate that the work in this area will continue to experience unparalleled growth in the coming years. Over the last several years, NSD has experienced a significant growth in the volume and complexity of the work related to Section 702. NSD plays a primary role in implementing and overseeing Section 702 of FISA. As President Trump stated in January 2018 when he signed the bill re-authorizing this program for an additional 6 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."

All taskings under the Section 702 program are reviewed by NSD to ensure compliance with the law, and as reflected below, there has been a significant increase in the number of Section 702 targets over the last several years, which shows no signs of abating. 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 78 percent from 92,707 in CY 2014 to 164,770 in CY 2018. The substantial growth of NSD's Section 702 oversight program and the resulting impact on NSD's resources is also apparent from the 251 percent increase in the number of matters handled by the NSD component that oversees this program between FY 2014 and FY 2019.

The passage of the USA Freedom Act in June 2015 and the reauthorization of Section 702 resulted in many significant amendments to FISA. NSD has played a leading role in fulfilling these 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 NSD expects will continue 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 traditional FISA and 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 traditional FISA and 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. Continually Evolving Terrorism Threats.

International and domestic terrorism-related actors remain a continually evolving threat to the United States. NSD therefore requires resources to support DOJ's highest priority of preventing and disrupting acts of terrorism.

Despite ISIS' loss of territory in Syria and Iraq, ISIS supporters and propaganda continue to assist in the radicalization of others in the United States and abroad. While many ISIS fighters were killed or detained, many other former fighters returned to countries where they may continue to operate, plan terrorist attacks, and pursue radicalization activities. In either case, increased and sustained engagement will be necessary to mitigate the threat posed to the United States by these individuals.

NSD is assisting the USAOs with a number of prosecutions of U.S. citizens, who have been repatriated from the custody of the Syrian Democratic Forces. In the coming months, NSD may see additional repatriations as additional U.S. citizens are identified among the detainees or found in other countries.

In addition, NSD and the IC predict a continued threat of self-radicalized individuals engaging in terrorist attacks on government and civilian targets in the United States. Online radicalization is a particular problem as terrorists and other criminals increasingly use technology, including encryption, to conceal their crimes and avoid 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, NSD remains vigilant in its efforts to identify and disrupt former ISIS fighters who may seek to return to the United States, while also addressing the continuing threat posed by homegrown violent extremists who seek to conduct terrorist attacks on U.S. soil.

As part of the battle against ISIS, the Department of Defense (DOD) has received and collected a large amount of enemy materials, which must be reviewed for both intelligence and evidence to potentially be used in foreign or U.S. prosecutions. NSD continues to provide advice and support on the dissemination and potential use of such materials to the FBI and DOD as part of efforts to encourage partner nations to repatriate and, where appropriate, prosecute their citizens. NSD also

provides critical training to foreign partners in order to build their capacity to prosecute terrorism offenses, including those committed by repatriated foreign fighters.

NSD assists USAOs with managing voluminous classified and unclassified discovery in terrorism-related cases. More resources are needed in order to meet the increasing needs of the USAOs for this important support. NSD must continue efforts to develop a robust automated litigation services environment in order to quickly process discovery and efficiently support nationwide terrorism-related litigation.

NSD must also work to counter the rising threat posed by Hezbollah, the Islamic Revolutionary Guard Corps ("IRGC"), and other Iran-backed foreign terrorist organizations and Specially Designated Global Terrorists. 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 recent designation of IRGC may also increase the volume of these cases.

The United States faces threats of domestic terrorism, including acts by racially motivated violent extremists, as demonstrated by recent fatal shootings in synagogues and the August 2019 mass shooting in El Paso, Texas. Domestic terrorism actors 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. This threat will continue to pose unique challenges for the foreseeable future.

Each of these various threats are complex, frequently involving individuals 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. Expanding Need For Assistance To U.S. Citizen Victims Of Overseas Terrorist Attacks And Support For Foreign Governments Terrorism Prosecutions.

Americans have fallen victim in terror attacks arising from the changing terrorist threats identified earlier in this document both at home and abroad. As the terrorism threat from ISIS and others evolves and inspires attacks in numerous other countries, the incidence of foreign attacks harming U.S. victims continues to increase. Moreover, terrorist attacks in Israel and areas under its control continue to harm Americans living in and visiting that region.

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 international model program helps U.S. citizens navigate foreign justice systems by providing information, and supporting attendance to and participation in foreign proceedings as permitted under foreign law. OVT faces many challenges to providing U.S. citizen victims of overseas terrorism with the highest quality information and assistance services, including obtaining information from and about diverse and sometimes unpredictable foreign justice systems, the lack of foreign government political will, systemic capacity, security, and foreign government sovereignty concerns.

In addition to its direct victim services and international training and technical assistance, NSD OVT also plays a role in U.S. government financial support programs for U.S. victims of overseas terrorism. For example, OVT administers the attack designation process for the International Terrorism Expense Reimbursement Program (ITVERP), which provides reimbursement for some victims' expenses related to overseas terror attacks. Further, OVT operates the Criminal Justice Participation Assistance Fund (CJPAF), a victim foreign travel funding program. There is a significant administrative burden in operating the CJPAF program. NSD's program requires adequate resources to effectively meet the needs of victims.

NSD OVT supports U.S. citizen terrorism victims over the long term, no matter how long the search for justice and accountability takes. Its caseload is cumulative with new attacks occurring at a steady pace. It also continues to assist victims in cases going back 30 years or more (such as the 1988 Lockerbie/Pan Am 103 case). The number of cases active in foreign systems at any one time can vary. 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. OVT provides quite intensive victims' services during and leading up to foreign criminal justice proceedings and is committed to offering trauma-informed methods of interacting with victims. It is increasingly clear that victims continue to suffer significant effects from terrorist attacks over the mid- and long-term while OVT is most frequently assisting them. 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 profound and life-altering trauma at the hands of terrorists.

G. 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. NSD 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	Pos.	FTE	Dollars ($000)	Page
Counterintelligence and Export Control	Requesting additional resources for NSD's work related to Counterintelligence and Export Control, including the China Initiative and FARA enforcement activities.	2	1	$ 550	44
Foreign Investment Reviews to Counter Threats to Our Nation's Telecommunications & Other Critical Infrastructure from Intelligence Services	Requesting additional resources for NSD's work related to the review of foreign investments in U.S. industry that may impact the national security.	1	1	$ 175	47
Intelligence Collection, and Oversight	Requesting additional resources for the NSD's work related to intelligence collection and oversight.	2	1	$ 1,060	50
Insider Threat Prevention and the Protection of National Security Classified Systems	Requesting additional resources for NSD's work related to deterring, detecting, and mitigating insider threats and protection national security classified systems.	4	2	$ 1,038	56
Victims Outreach and Support	Requesting additional resources for the NSD's work related to outreach and support provided to US victims of overseas terrorism.	2	1	$ 206	59
	Grand Total: NSD 2021 Enhancement Request	**11**	**6**	**$ 3,029**	

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, [$110,000,000] $117,451,000, 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 504 of this Act and shall not be available for obligation or expenditure except in compliance with the procedures set forth in that section.

Analysis of Appropriations Language

No change proposed.

IV. Program Activity Justification

A. National Security Division

National Security Division	Direct Pos.	Estimate FTE	Amount
2019 Enacted	362	318	$101,369,000
2020 Enacted	391	333	$110,000,000
Adjustments to Base and Technical Adjustments	0	14	$4,422,000
2021 Current Services	391	347	$114,422,000
2021 Program Increases	11	6	$3,029,000
2021 Request	402	353	$117,451,000
Total Change 2020-2021	**11**	**20**	**$ 7,451,000**

National Security Division -Information Technology Breakout	Direct Pos.	Estimate FTE	Amount
2019 Enacted	20	20	16,089,000
2020 Enacted	22	22	14,603,000
Adjustments to Base and Technical Adjustments	0	0	2,608,000
2021 Current Services	22	22	17,211,000
2021 Program Increases	4	2	1,038,000
2021 Program Offsets	0	0	0
2021 Request	26	24	18,249,000
Total Change 2020-2021	**4**	**2**	**3,646,000**

1. Program Description

The National Security Division (NSD) is responsible for:

- Overseeing terrorism investigations and prosecutions;
- Protecting critical national assets from national security threats, including through handling counterespionage, counterproliferation, and national security cyber cases and matters; 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 DOJ's liaison to the DNI;
- 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 DOJ 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 United States, including counterintelligence threats and cyber threats to the national security.

- The NSD also serves as DOJ's liaison to the DNI, advises the Attorney General on all matters relating to the national security activities of the United States, and develops strategies for emerging national security threats – including cyber threats to the national security.

- 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 NSC-led policy committees and the Deputies' Committee processes. NSD also represents the DOJ on a variety of interagency committees such as 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.

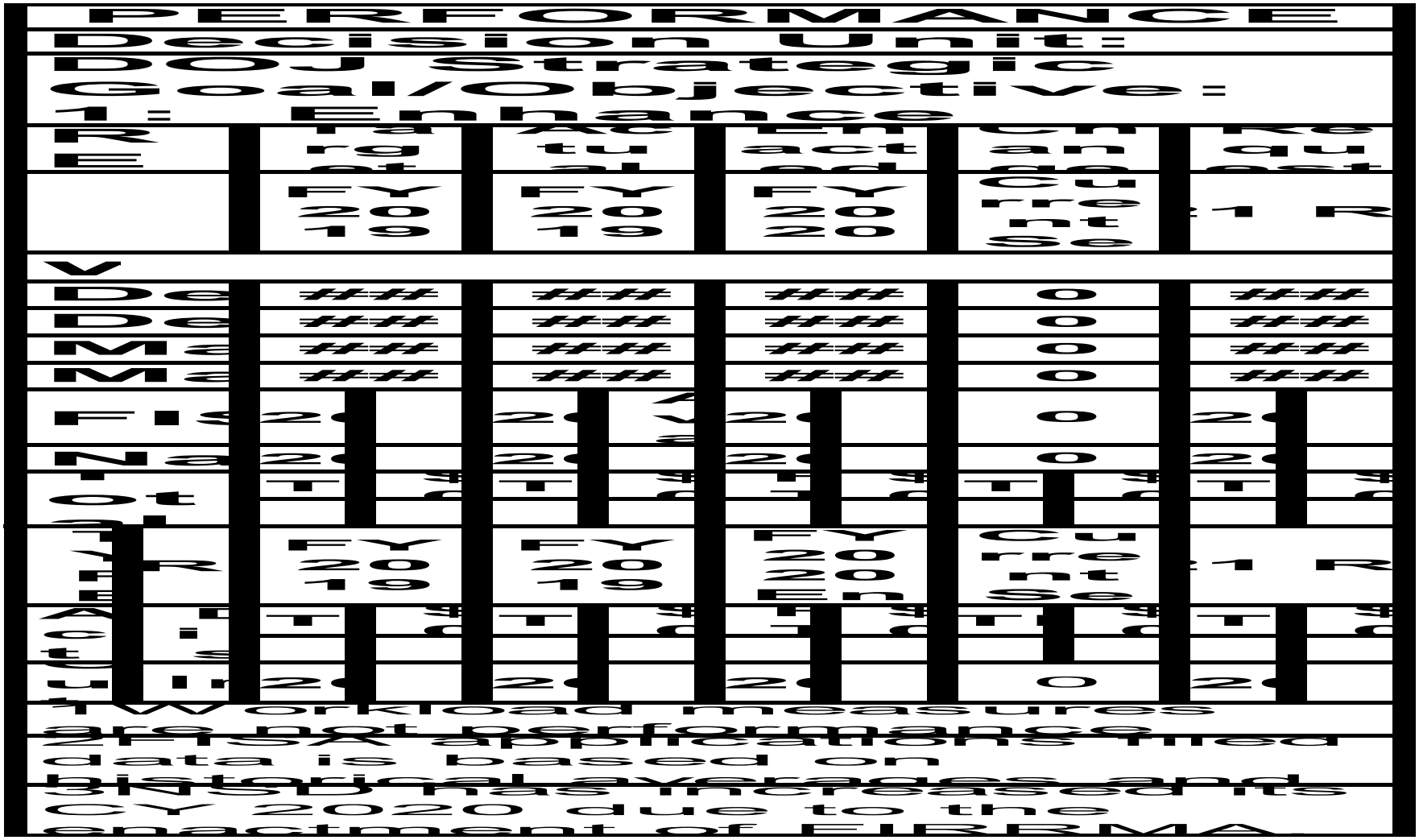
- NSD serves as the staff-level DOJ representative on CFIUS, which reviews foreign acquisitions of domestic entities affecting national security. In this role, NSD evaluates information relating to the structure of transactions, foreign government ownership or control, threat assessments provided by 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 DOJ, 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, provides American victims of overseas terrorist attacks the services and support needed to navigate foreign judicial systems. Services include providing foreign system information and case notification, assistance for victim attendance and participation in foreign criminal justice systems as permitted by foreign law, and referrals to U.S. and foreign government and non-government services providers. OVT further provides expertise and guidance within DOJ and to U.S. government partners on issues important to U.S. victims of overseas terrorism. OVT also works with government and international organizations to deliver international training and technical assistance to encourage recognition of rights for victims of terrorism around the world. Grounded in U.S. victims' rights and international best practices, OVT supports a role for terrorism victims in foreign partners' justice systems. .

IV. Program Activity Justification

2. Performance and Resource Tables



PERFORMANCE AND RESOURCES TABLE

Decision Unit: National Security

DOJ Strategic Goal/Objective: 1: Enhance National Security and Counter…

RESO…		Target	Actual	Enacted	Changes	Requested
T… Y… E…	R…	FY 2019	FY 2019	FY 2020	Current …	21 R…
O… u… t…	P… e… r…	###	###	###	0	###
O… u… t… c… o… m…	P… e… r… c… e… n…	###	###	###	0	###
A… c… t… i…	O… c… n… b…	T… $… c… n…	T… $… c… n…	T… $… c… n…	T… $… c… n…	T… $… c… n…
O… u… t…	P… e… r…	###	###	###	0	###
A… c… t…	O… c… n… b…	T… $… c…	T… $… c…	T…	T… $… c…	T… $… c…
O… u… t…	P… e… r…	###	###	###	0	###
O… u… t… c… o… m…	P… e… r… c… e… n…	###	###	###	0	###
O… u… t…	P… A…	14	20	18	0	18
O… u… t…	H… i… g…	C…	C…	C…	0	C…

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 disclosur										
Strategic Objective	**Performance Report and**		**FY 2015**	**FY 2016**	**FY 2017**	**FY 2018**	**FY 2019**		**FY 2020**	**FY2021**
	Performance Plan Targets		**Actual**	**Actual**	**Actual**	**Actual**	**Target**	**Actual**	**Target**	**Target**
Prevent Terrorism	**Output Measure**	Intelligence Community Oversight Reviews	CY 2015: 100	CY 2016: 110	CY 2017: 102	CY 2018: 110	CY2019: 105	CY2019: 97	CY2020: 102	CY2021: 102
Prosecute Terrorism	**Outcome Measure**	Percentage of CT defendants whose cases were favorably resolved	98%	99%	91%	91%	90%	96%	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	100%	100%	100%	100%	90%	99%	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	15	15	14	20	18	18
Investigate and Prosecute Espionage	**Output Measure**	High priority national security reviews completed	CY 2015: 38	CY 2016: 43	CY 2017: 65	CY 2018: 100	CY 2019: 45	CY2019: 129	CY 2020: 122	CY 2021: 122
Combat Cyber-Based Threats and Attacks	**Outcome Measure**	Percentage of Cyber defendants whose cases were favorably resolved	100%	100%	100%	100%	90%	100%	90%	90%

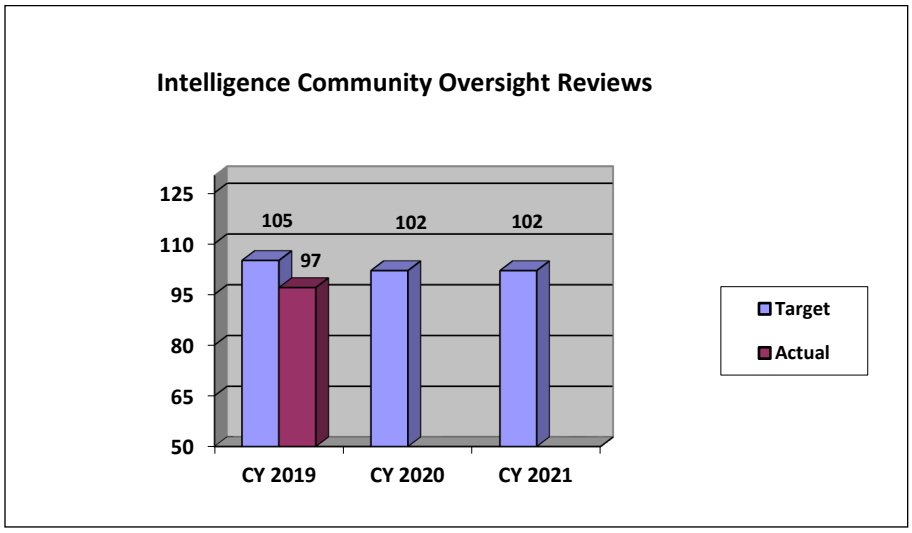
3. Performance, Resources, and Strategies

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

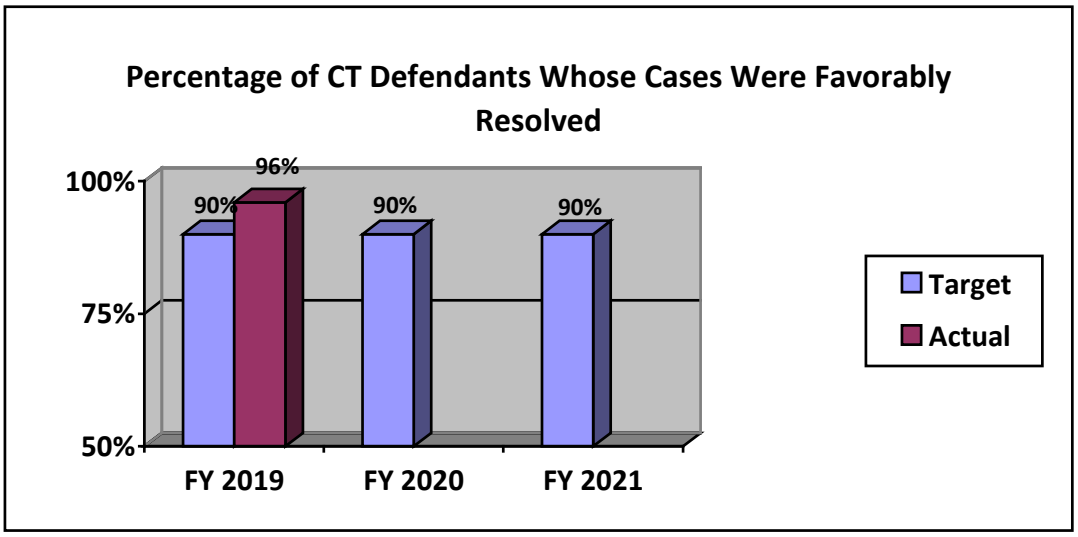
Measure: **Intelligence Community Oversight Reviews**
CY 2019 Target: **105**
CY 2019 Actual: **97**
CY 2020 Target: **102**
CY 2021 Target: **102**
Discussion: CY 2021- The CY 2021 target is consistent but slightly decreased from previous targets due to the discontinuation of a certain program. Although the overall work of NSD 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 2019 Target: **90%**
FY 2019 Actual: **96%**
FY 2020 Target: **90%**
FY 2021Target: **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.

United States v. Kourani: In December 2019, in the Southern District of New York, Ali Kourani ("Kourani") was sentenced to 40 years in prison and 5 years of supervised release. In May 2019, a jury returned a guilty verdict against Kourani on all eight counts in his indictment, which charged him with terrorism, sanctions, and immigration offenses for his illicit work as an operative for Hizballah's external attack-planning component, the Islamic Jihad Organization (IJO).

Kourani, who was born in Lebanon, attended Hizballah-sponsored weapons training in Lebanon in 2000 when he was approximately 16 years old. He lawfully entering the United States in 2003. By 2008, IJO recruited Kourani to its ranks. In August 2008, Kourani submitted an application for naturalization in the United States in which he falsely claimed, among other things, that he was not affiliated with a terrorist organization. In April 2009, Kourani became a naturalized citizen.

IJO assigned Kourani an IJO handler who was responsible for providing him with taskings, debriefings, and arranging training. Based on taskings from IJO personnel, which IJO personnel conveyed during periodic in-person meetings when Kourani returned to Lebanon, Kourani conducted operations, which he understood to be aimed at preparing for potential future Hizballah attacks. These covert activities included searching for weapons suppliers in the United States who could provide firearms to support IJO operations; identifying individuals affiliated with the Israeli Defense Force whom the IJO could either recruit or target for violence; gathering information regarding operations and security at airports in the United States and elsewhere, including JFK International Airport in New York; and surveilling U.S. military and law enforcement facilities in New York City, including a federal building in Manhattan. Kourani transmitted some of the products of his surveillance and intelligence-gathering efforts back to IJO personnel in Lebanon using digital storage media.

Kourani was convicted of providing material support to a designated foreign terrorist organization; conspiracy to provide material support and resources to a designated foreign terrorist organization; receiving military-type training from a designated foreign terrorist organization; conspiracy to receive military-type training from a designated foreign terrorist organization; conspiracy to possess, carry, and use firearms and destructive devices during and in relation to crimes of violence; making and receiving a contribution of funds, goods, and services to and from Hizballah, in violation of IEEPA; conspiracy to make and receive a contribution of funds, goods, and services to and from Hizballah, in violation of IEEPA; and naturalization fraud in connection with an act of international terrorism.

United States v. Ahmed: In December 2019, in the Eastern District of Texas, a jury returned a guilty verdict against Mohamed Ibrahim Ahmed ("Ahmed") on one count of attempting to provide material support to ISIS and one count of making a material false statement. According to charging documents, Ahmed, who had been in prison on prior conviction for conspiring to provide material support to al Shabaab, made attempts to provide material support to ISIS between late 2014 and May 2017. During interviews with the FBI, Ahmed denied knowledge of how to construct a bomb or that he discussed bomb making with another inmate. Ahmed faces a maximum of 25 years in prison when he is sentenced.

United States v. Ftouhi: In April 2019, in the Eastern District of Michigan, Amor M. Ftouhi ("Ftouhi"), of Quebec, Canada, was sentenced to life in prison for committing an act of terrorism transcending national boundaries and two other offenses in conjunction with his attack on an airport police officer on June 21, 2017. Ftouhi was convicted by a federal jury on November 13, 2018.

Ftouhi entered the United States from Canada on a professed "mission" for the purpose of killing American police officers in the United States. Before entering the United States on June 16,

2017, while in Canada, Ftouhi conducted online research of American gun laws and for gun shows in Michigan. Ftouhi subsequently traveled to Michigan where he was unsuccessful in repeated attempts to purchase a gun and purchased a knife instead. On June 20, 2017, Ftouhi approached the victim, who is a lieutenant with the Flint Bishop Airport police and was in full uniform, and stabbed the police officer in the neck twice with a knife. Ftouhi referenced killings in Syria, Iraq, and Afghanistan, and yelled "Allahu Akbar." After his arrest, Ftouhi told law enforcement that he was a "soldier of Allah," subscribed to the ideology of Al Qaeda and Usama bin Laden and that his plan had been to kill the victim, steal his gun and kill other police officers in the airport. The police officer sustained life-threatening injuries, but survived the attack.

United States v. Sayoc: In August 2019, in the Southern District of New York, Cesar Altieri Sayoc ("Sayoc") was sentenced to 20 years in prison after pleading guilty to 65 felony counts and admitted to mailing 16 improvised explosive devices (IEDs) to 13 victims throughout the country, including 11 current or former U.S. government officials, and that he intended to use the IEDs as weapons and to cause injuries.

In October 2018, Sayoc mailed from Florida 16 padded envelopes, each containing an IED, to addresses in New York, New Jersey, Washington, D.C., Delaware, Atlanta, and California. Sayoc packed each IED with explosive material and glass shards that would function as shrapnel if the IED exploded. Sayoc also attached to the outside of each IED a picture of the intended victim marked with a red "X." Sayoc admitted during his plea that he designed the IEDs for use as weapons and mailed them understanding that they were capable of exploding and causing injuries and property damage. In alphabetical order, Sayoc's intended victims were former Vice President Joseph Biden, Senator Cory Booker, former CIA Director John Brennan, former DNI James Clapper, former Secretary of State Hillary Clinton, CNN, Robert De Niro, Senator Kamala Harris, former Attorney General Eric Holder, former President Barack Obama, George Soros, Thomas Steyer, and Representative Maxine Waters. Between October 22 and November 2, 2018, the FBI and the U.S. Postal Service recovered all of the 16 IEDs mailed by Sayoc.

Sayoc pled guilty to four sets of charges related to each of the 16 IEDs: (1) sixteen counts of using a weapon of mass destruction; (2) sixteen counts of interstate transportation of an explosive device; (3) sixteen counts of conveying a threat in interstate commerce; and (4) sixteen counts of the illegal mailing of explosives with the intent to kill or injure another. Sayoc also pled guilty to using an explosive to commit a felony, which relates to felonies committed in connection with the use and mailing of all 16 IEDs.

United States v. Ullah: In November 2018, in the Southern District of New York, a jury returned a guilty verdict against Akayed Ullah, a lawful permanent resident from Bangladesh, on all six counts in his indictment. Ullah was charged with offenses related to the detonation and attempted detonation of a bomb in a subway station in New York City. Ullah is scheduled to be sentenced on February 19, 2020.

On December 11, 2017, Ullah detonated an improvised explosive device ("IED") inside a subway terminal near the New York Port Authority Bus Terminal located in New York City. Surveillance footage captured Ullah walking through the subway terminal and detonating his IED. Ullah stated that he was inspired by ISIS (the Islamic State of Iraq and Al-Sham) and that he carried out the attack in the name of the foreign terrorist organization. Ullah also stated that he carried out the attack in part because of the United States Government's policies in the Middle

East, and that he wanted to terrorize as many people as possible and chose work day for his attack so there would be more people present.

Ullah was convicted of one count of providing and attempting to provide material support to a designated foreign terrorist organization; one count of using and attempting to use a weapon of mass destruction; one count of bombing and attempting to bomb a place of public use; one count of destruction of property by means of fire or explosives; and use of a destructive device in furtherance of a crime of violence.

Unites States v. Alahmedalabdaloklah: In November 2018, in the District of Arizona, Ahmed Alahmedalabdaloklah, aka Ahmad Ibrahim Al-Ahmad ("Alahmedalabdaloklah"), of Syria, was sentenced to life plus 30 years in prison. Alahmedalabdaloklah was found guilty by a federal jury on March 16, 2018 of conspiracy 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 to possess a destructive device in furtherance of a crime of violence, and conspiracy to possess a destructive device in furtherance of a crime of violence.

Between January 2005 and July 2010, Alahmedalabdaloklah designed, made and supplied components parts for Improvised Explosive Devices (IEDs) for members and associates of the 1920 Revolution Brigades, 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.

On August 30, 2006, U.S. military personnel discovered a large cache of IEDs in Baghdad, Iraq, including a completed IED triggering device that had three of Alahmedalabdaloklah's fingerprints on the tape wrapped around the device. The U.S. military also seized raw material, tools, test equipment, schematics, and other items related to IED construction, including components for various types of IEDs and bomb making training aids. One document, which had numerous latent prints belonging to Alahmedalabdaloklah, described how to employ remote technology to command a mobile phone, wireless device and landline phone to detonate explosives.

Alahmedalabdaloklah subsequently moved to China and continued to support the 1920 Revolution Brigades by providing component parts for IEDs. In May 2011, Alahmedalabdaloklah was detained in the Republic of Turkey while transiting from China. He was extradited to the United States in August 2014.

United States v. Al Farekh: In March 2018, in the Eastern District of New York, Muhanad Mahmoud al Farekh ("Farekh"), a United States citizen, was sentenced to 45 years following his September 29, 2017 trial conviction of multiple offenses covering seven years of terrorist conduct, including conspiracy to murder American military personnel in Afghanistan, conspiracy to use a weapon of mass destruction, conspiracy to bomb a government facility and providing material support to al-Qaeda.

In March 2007, Farekh and two co-conspirators, all of whom were students at the University of Manitoba, departed Canada for Pakistan with the intention of fighting against American forces overseas. Before traveling overseas, Farekh and his co-conspirators watched video recordings encouraging violent jihad, listened to jihadist lectures by now-deceased al-Qaeda in the Arabian

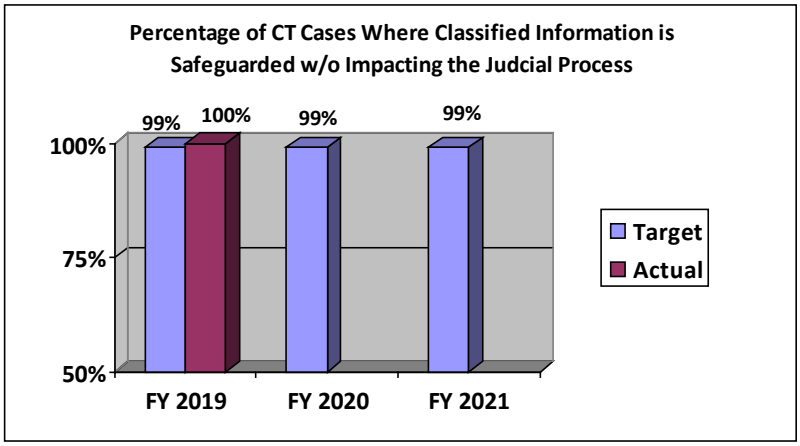
Peninsula leader Anwar al-Awlaqi, and came to embrace a violent, extremist view of Islam. Farekh and his co-conspirators traveled to the Federally Administered Tribal Areas of Pakistan, an area in the northern part of Pakistan that borders Afghanistan, where they joined and received training from al-Qaeda. Taking advantage of his familiarity with the West, Farekh became a member of, and ultimately ascended to, a leadership role within al-Qaeda's external operations group, which specialized in planning and executing attacks against the U.S. and its Western allies.

In January 2009, Farekh helped to build a vehicle-borne, improvised explosive device (VBIED) that was used in an attack on Forward Operating Base Chapman, a U.S. military installation in Khost, Afghanistan. On January 19, 2009, two explosives-laden vehicles approached the fence line of FOB Chapman. At the gate, the first vehicle, a pickup-sized truck, exploded after its operator detonated the VBIED. The second vehicle, a truck that was carrying approximately 7,500 pounds of explosives, became stuck in the blast crater caused by the first explosion. The driver abandoned his vehicle without detonating the VBIED, and was shot and killed by local security personnel. The initial detonation of the first vehicle injured one U.S. serviceman and numerous Afghan nationals. Forensic technicians recovered 18 latent fingerprints that were determined to be a match to Farekh from adhesive packing tape used to bind together the explosive materials of the second, undetonated VBIED.

United States v. Hendricks: In March 2018, in the Northern District of Ohio, a jury found Erick Jamal Hendricks ("Hendricks") guilty of attempting and conspiring to provide material support to the Islamic State of Iraq and al-Sham (ISIS). In February 2019, Hendricks was sentenced to 15 years' imprisonment. The conviction stems from Hendricks' attempt to recruit people to train together and conduct terrorist attacks in the United States on behalf of ISIS.

United States v. Nicholas Young: In February 2018, in the Eastern District of Virginia, Nicholas Young ("Young"), a former police officer, was sentenced to 15 years in prison for attempting to provide material support to the Islamic State of Iraq and al-Sham (ISIS), a designated foreign terrorist organization. Young was formerly employed as a police officer with the Metro Transit Police Department. In late July 2016, Young attempted to provide material support to ISIS by purchasing and sending gift card codes that he believed would allow ISIS recruiters to securely communicate with potential ISIS recruits.

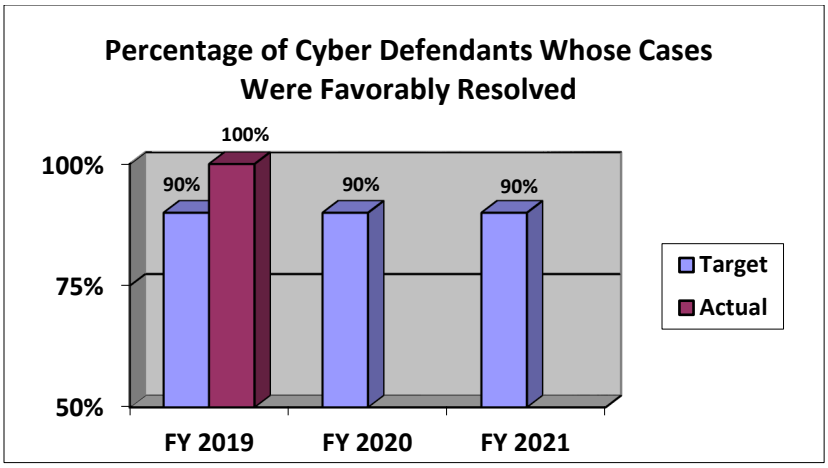
Measure: **Percentage of CT Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2019 Target: **99%**
FY 2019 Actual: **100%**
FY 2020 Target: **99%**
FY 2021 Target: **99%**
Discussion: The FY 2021 target is consistent with previous 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 2019 Target: **90%**
FY 2019 Actual: **100%**
FY 2020 Target: **90%**
FY 2021 Target: **90%**
Discussion: The FY 2021 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.

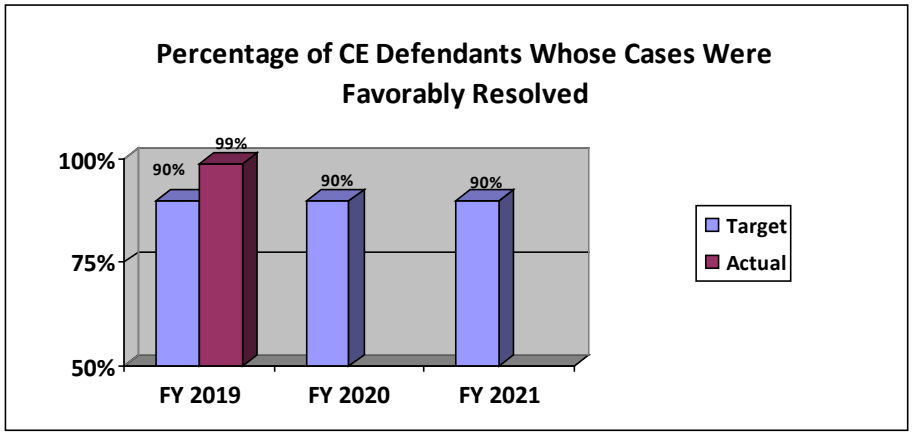
United States v. Morenets et al.: On October 4, 2018, in the Western District of Pennsylvania, DOJ unsealed an indictment charging seven officers in the Russian Main Intelligence Directorate (GRU) for computer hacking, wire fraud, aggravated identity theft, and money laundering. As alleged, beginning in or around December 2014 and continuing until at least May 2018, the conspiracy conducted persistent and sophisticated computer intrusions, sometimes aided by on-site GRU hacking teams, 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. Along with the criminal charges, DOJ seized the websites that the GRU was using to publicize athletes' personal health information and related disinformation.

United States v. Zhu Hua et al.: On December 20, 2018, in the Southern District of New York, DOJ unsealed an indictment charging Chinese nationals Zhu Hua and Zhang Shilong with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft. As alleged, the defendants, through their involvement in a hacking group associated with the Chinese Ministry of State Security from 2006 to in or about 2018, conducted

global campaigns of computer intrusions targeting, among other data, intellectual property and confidential business and technological information at managed service providers, which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, more than 45 technology companies in the United States, and U.S. government agencies.

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 2019 Target: **90%**
FY 2019 Actual: **99%**
FY 2020 Target: **90%**
FY 2021 Target: **90%**
Discussion: The 2021 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 Control Cases

The following are highlights from recent Export Control Cases.

United States v. Huawei Technologies, et al.: On January 28, 2019, in the Eastern District of New York, a 13-count indictment was unsealed charging a conspiracy involving China's largest telecommunications equipment manufacturer. The defendants are Huawei Technologies Co. Ltd. (Huawei), two Huawei affiliates – Huawei Device USA Inc. (Huawei USA) and Skycom Tech Co. Ltd. (Skycom) – and Huawei's Chief Financial Officer (CFO) Wanzhou Meng a/k/a Cathy Meng. Huawei and Skycom were charged with bank fraud and conspiracy to commit bank fraud, wire fraud and conspiracy to commit wire fraud, violations of the International Emergency Economic Powers Act (IEEPA) and conspiracy to violate IEEPA, and conspiracy to commit money laundering. Huawei and Huawei USA were charged with conspiracy to obstruct justice related to the grand jury investigation in the Eastern District of New York. Meng was charged with bank fraud, wire fraud, and conspiracies to commit bank and wire fraud. According to the indictment: The charges relate to a long-running scheme by Huawei, its CFO, and other employees to deceive numerous global financial institutions and the U.S. Government regarding Huawei's business activities in Iran. Beginning in 2007, Huawei employees lied about Huawei's relationship to a company in Iran called Skycom, falsely asserting it was not an affiliate of Huawei. The company further claimed that Huawei had only limited operations in Iran and that Huawei did not violate United States or other laws related to Iran. Most significant, after news publications in late 2012 and 2013 disclosed that Huawei operated Skycom as an unofficial affiliate in Iran and that Meng had served on the board of directors of Skycom, Huawei employees, and in particular Meng, continued to lie to Huawei's banking partners about Huawei's relationship with Skycom. They falsely claimed that Huawei had sold its interest in Skycom to an unrelated third party in 2007 and that Skycom was merely Huawei's local business partner in Iran. In reality, Skycom was Huawei's longstanding Iranian affiliate, and Huawei orchestrated the 2007 sale to appear as an arm's length transaction between two unrelated parties, when in fact Huawei actually controlled the company that purchased Skycom.

United States v. M/V Wise Honest: On May 9, 2019, in the Southern District of New York, the United States filed a civil forfeiture complaint against M/V Wise Honest, a cargo vessel registered in the Democratic People's Republic of Korea (DPRK or North Korea). Indonesian maritime authorities had intercepted and detained the Wise Honest in April 2018. The United States subsequently sought and was granted a seizure warrant in July 2018. Pursuant to that warrant, Indonesia turned over custody of the vessel to the United States. According to court documents: The Wise Honest, one of the DPRK's largest bulk carriers, was used to ship coal illicitly from North Korea and to deliver heavy machinery to North Korea. Payments for maintenance, equipment, and improvements of the Wise Honest were made in U.S. dollars through unwitting U.S. banks. This conduct violated longstanding U.S. law and U.N. Security Council resolutions. From at least November 2016 through April 2018, the Wise Honest was used by Korea Songi Shipping Company, an affiliate of Korea Songi General Trading Corporation (Songi Trading), to export coal from North Korea to foreign purchasers and import machinery to North Korea (the "Korea Songi Scheme"). In June 2017, the U.S. Treasury Department, pursuant to Executive Order 13722, designated Songi Trading for its involvement in the sale, supply, or transfer of coal from North Korea. Participants in the Korea Songi Scheme attempted to conceal the Wise Honest's DPRK affiliation by falsely listing different countries for the Wise Honest's nationality and the origin of the illicit coal in shipping documentation. In connection with the Korea Songi Scheme, Korea Songi Shipping paid for numerous improvements, equipment purchases, and service expenditures for the Wise Honest in U.S. dollars. Such dollar transfers constitute a provision of services by U.S. banks to both the sender and recipient of the funds, and U.S. sanctions prohibit banks from providing such services to

North Korean parties. Payments totaling more than $750,000 were transmitted through accounts at a U.S. financial institution in connection with the March 2018 shipment of coal on board the Wise Honest. On October 21, 2019, in the Southern District of New York, the Court issued a Judgment of Forfeiture in favor of the United States.

The following are highlights from recent Counterintelligence Cases.

United States v. Witt et al.: On February 13, 2019, in the District of Columbia, DOJ unsealed an indictment charging four Iranian nationals working on behalf of the Islamic Revolutionary Guard Corps (IRGC) for computer hacking and aggravated identity theft in relation to their targeting of former co-workers and colleagues of a former U.S. service member and counterintelligence agent, Monica Witt, who had defected to Iran in 2013. Witt was also charged in relation to her delivery of national defense information to Iranian intelligence services, specifically her assistance in targeting her former fellow agents in the U.S. IC. The charged Iranians used fictional and imposter social media accounts in an effort to deploy malware that would provide them covert access to Witt's former US IC colleagues' computers and networks. Along with the criminal charges, the Department of Treasury designated the charged Iranian nationals and others pursuant to Executive Order 13224.

United States v. Khusyaynova: On October 19, 2018, in the Eastern District of Virginia, DOJ unsealed a criminal complaint 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. As alleged, 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. Khusyaynova managed the financing of Project Lakhta operations, including foreign influence activities directed at the United States that were referred to internally as "information warfare against the United States." This effort was not only designed to spread distrust toward 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.

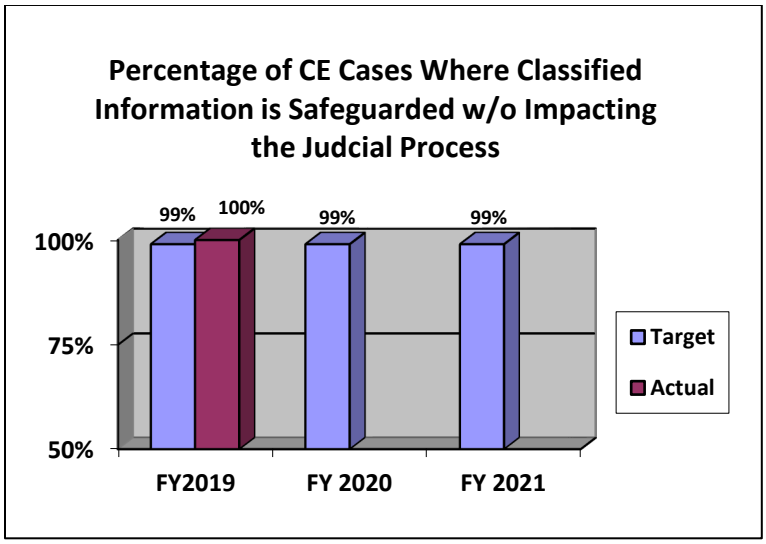
United States v. Ron Rockwell Hansen: On March 15, 2019, in the District of Utah, Ron Rockwell Hansen, a former Defense Intelligence Agency (DIA) officer, pled guilty to Count 1 of an indictment charging him with attempting to gather or deliver national defense information. FBI agents arrested Hansen in June 2018, as he was on his way to board a flight to the People's Republic of China (PRC). Hansen was indicted on June 20, 2018, and charged with attempting to gather or deliver national defense information; acting as an agent of a foreign government; bulk cash smuggling; structuring monetary transactions; and smuggling goods from the United States. According to court documents: Hansen retired from the U.S. Army as a Warrant Officer, with a background in signals intelligence and human intelligence. He speaks fluent Chinese and Russian. Upon retirement from the Army, DIA hired Hansen as a civilian intelligence case officer. Between 2013 and 2017, Hansen regularly traveled between the United States and China, attending U.S. military and intelligence conferences and providing information he learned at the conferences to contacts in China associated with the PRC intelligence services. Hansen received payments for this information by a variety of methods, including cash, wires, and credit card transactions. He also improperly sold export-controlled technology to persons in China. From May of 2013 to June 2018, Hansen received not less than $800,000 in funds originating from China. On September 24, 2019, Hansen was sentenced to 10 years in prison.

United States v. Jerry Chun Shing Lee: On May 1, 2019, in the Eastern District of Virginia, Jerry Chun Shing Lee, a former Central Intelligence Agency (CIA) case officer, pled guilty to Count 1 of an indictment charging a conspiracy to deliver national defense information to aid a foreign government. Lee was arrested in January 2018 and indicted in May 2018. The indictment alleges that Lee received and responded to taskings from two intelligence officers (IOs) from China's Ministry of State Security, including requests that Lee provide documents and information relating to the national defense of the United States. According to the indictment: Lee is a U.S. citizen who speaks fluent Chinese, and served as a case officer for the CIA until 2007. After leaving the CIA, Lee resided in Hong Kong. In April 2010, two Chinese IOs approached Lee and offered to pay him for information. Lee received taskings from the IOs until at least 2011. The IOs provided Lee with a series of email addresses so that he could communicate covertly with them. Lee prepared documents responsive to the taskings, made numerous unexplained cash deposits, and repeatedly lied to the United States government during voluntary interviews when asked about travel to China and his actions overseas. On November 22, 2019, Lee was sentenced to 19 years in prison.

United States v. Kevin Patrick Mallory: On May 17, 2019, in the Eastern District of Virginia, Kevin Patrick Mallory was sentenced to 240 months in prison for his role in a conspiracy to deliver national defense information (NDI) to the People's Republic of China (PRC). On June 8, 2018, a jury found Mallory guilty on all four counts of the indictment: 1) conspiracy to deliver NDI to aid a foreign government; 2) delivery of NDI to aid a foreign nation; 3) attempted delivery of NDI to aid a foreign nation; and 4) materially false statements. The trial judge later granted acquittal on Counts 2 and 3 for lack of venue. According to the indictment: Mallory is a U.S. citizen who speaks fluent Chinese. He held numerous positions with various U.S. government agencies and defense contractors, including working as a covert case officer for the Central Intelligence Agency (CIA) and an intelligence officer for the Defense Intelligence Agency (DIA). Mallory held a Top Secret security clearance, which was terminated in October 2012 when he left government service. In March and April 2017, Mallory travelled to Shanghai, China, and met with an individual, Michael Yang, whom he quickly concluded was working for the PRC Intelligence Service. During a voluntary interview with FBI agents in May 2017, Mallory stated that Yang represented himself as working for a PRC think tank, the Shanghai Academy of Social Sciences; however, Mallory stated that he assessed Yang to be a Chinese Intelligence Officer. Mallory told FBI agents that he travelled to Shanghai in March and April to meet with Yang and Yang's boss. After Mallory consented to a review of a device he had been given by Yang in order to communicate covertly, the FBI viewed a message from Mallory to Yang in which Mallory stated that he could visit in the middle of June and he could bring the remainder of the documents with him at that time. Analysis of the device also revealed a handwritten index describing eight different documents, later determined to be classified. Four of the eight documents listed in the index were found stored on the device.

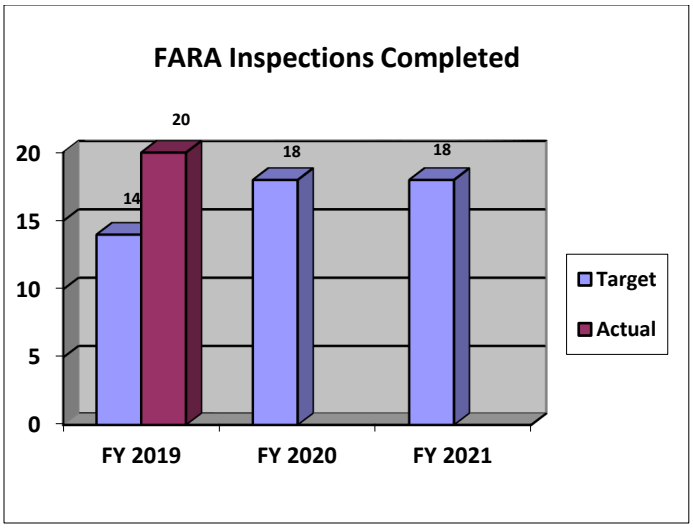
Measure:	**Percentage of CE Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2019 Target:	**99%**
FY 2019 Actual:	**100%**
FY 2020 Target:	**99%**
FY 2021 Target:	**99%**

Discussion: The FY 2021 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.



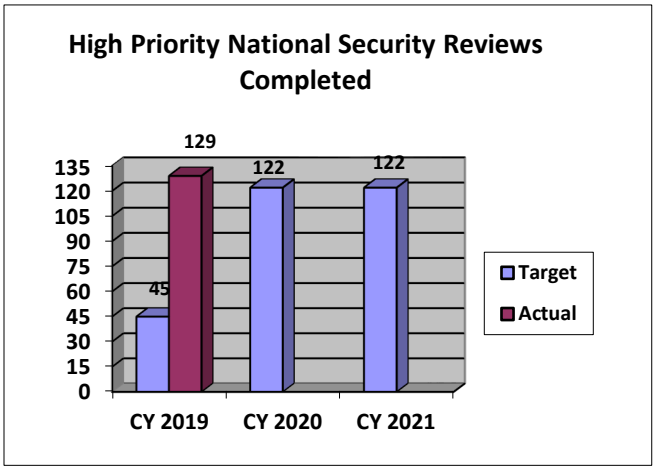
Data Definition: Classified information - information that has been determined by the United State Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data as defined by the 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 2019 Target: **14**
FY 2019 Actual: **20**
FY 2020 Target: **18**
FY 2021 Target: **18**
Discussion: The FY 2021 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 2019 Target: **45**
CY 2019 Actual: **129**
CY 2020 Target: **122**
CY 2021 Target: **122**
Discussion: NSD has increased its CY 2021 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.

Note telecommunications supply chain reviews is a new element of the performance measures, and reflects anticipated work as a result of new supply chain regulations being promulgated pursuant to an Executive Order signed by the President in May 2019. While the number of reviews is not yet knowable, NSD estimates conservatively that there will be at least one review per year led by DOJ and/or FBI. Civil enforcement actions is also a new category and only appears in "high priority" because if it occurs, it is expected to be a unique DOJ responsibility.

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 DOJ'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 DOJ 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, domestic terrorists, 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 DOJ's Hezbollah Task Force. NSD will continue to co-chair the Attorney General's Domestic Terrorism Executive Committee.

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 DOJ 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 DOJ 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 2019 – FY 2023 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 2019, NSD exceeded its 90 percent target with a 100 percent actual performance. NSD opened one cyber case and closed one cyber case, which was favorably resolved.

VI. Program Increases by Item

1. Counterintelligence and Export Control

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: Counterintelligence and Export Control Section

Program Increase: Positions 2 Atty 2 FTE 1 Dollars $550,000

Description of Item

NSD's Counterintelligence and Export Control Section (CES) requests two (2) Attorneys and an increase of $200,000 for software upgrades to, and further development of, the FARA.gov website for a total of $550,000.

Justification

One trial attorney will be a dedicated civil enforcement litigator, and the other trial attorney will handle the expected increase in criminal investigations growing out of the China Initiative.

Attorney Position: Civil Enforcement Litigator
This attorney will be assigned to CES's Foreign Agent Registration Act Unit (FARA Unit). NSD has seen increased efforts by foreign powers to carry out influence campaigns through representatives in the United States who engage in political activities or lobbying. These activities give rise to an obligation to register under the Foreign Agents Registration Act (FARA). When the FARA Unit learns of persons or businesses that might have a registration obligation, it sends out letters of inquiry seeking further information from the potential registrant. Based on the information it receives and other research, the FARA Unit frequently finds a registration obligation and sends a letter of determination. The preparation of these letters is very time-consuming and require the work of a skilled attorney because the possibility of litigation if a party refuses to register is high. Enforcing compliance with FARA is a top priority for NSD. One of the primary mechanisms for achieving that compliance is civil lawsuits. Accordingly, NSD intends to pursue civil lawsuits when persons or entities fail to comply with FARA. Additionally, registrations under FARA have increased dramatically over the last three years, which means the FARA Unit has received hundreds of new filings that may contain deficiencies. Under the statute, the most effective means to compel registrants to fix those deficiencies are civil lawsuits. During FY 2019, CES successfully litigated its first civil suit to compel registration in almost 30 years, and NSD anticipates a growing number of such lawsuits going forward and into FY 2021.

The requested civil enforcement litigator will handle these matters as well as other FARA-related enforcement efforts. In addition, the litigator will work with NSD's Foreign Investment Review Section (FIRS) to bring civil actions when necessary to enforce the mitigation agreements FIRS enters into with parties to transactions that present national security concerns, when other remedies are not available or desirable. For example, if a party to a Team Telecom mitigation agreement with FIRS breaches that agreement, and if the normal remedy of pursuing revocation of the party's telecommunications license would have negative collateral effects on the U.S. Government and other customers that rely on services provided by the breaching party, civil litigation to enjoin compliance with the terms of the mitigation agreement could be a more favorable enforcement vehicle. The civil enforcement litigator would handle these matters on behalf of FIRS.

Attorney Position: Criminal Investigations for China Initiative
NSD also is requesting an additional trial attorney for CES in FY 2021 to handle the expected increase in criminal investigations growing out of the China Initiative. NSD has seen increasingly aggressive efforts by foreign powers, particularly China, to steal U.S. national defense information and trade secrets. These cases are very labor intensive, requiring close coordination with the intelligence community 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. As previously noted, in November 2018, DOJ established a "China Initiative" to improve and increase our enforcement efforts targeted the range of national security threats posed by China, and since then, DOJ has charged five trade secret or economic espionage matters.

Software upgrades to FARA.gov website
The FARA.gov website is the means by which persons and businesses with obligations to register under the Foreign Agents Registration Act (FARA) submit the required forms. The FARA.gov website is also the electronic portal through which members of the public, Congress, and law enforcement can obtain access to DOJ's FARA records. During FY 2019 and FY 2020, DOJ will be rolling out eFile 4.0. These changes to the FARA.gov website will enable registrants to complete their filings in html format. The changes will also enhance the ability to search DOJ's records. However, a substantial portion of DOJ's FARA records are not in html format or, in the case of older records, have not been uploaded to the current website. The additional funding NSD is seeking will enable DOJ to archive all records and maintain the records in an easily searchable format. This will enhance transparency with the public and give law enforcement, primarily the FBI, and other government entities such as the Department of State, better access to FARA materials.

<u>Impact on Performance</u>

The above requests will allow NSD to keep up with the tracking demands required for registration obligations under FARA, handle the expected increase in criminal investigations growing out of the China Initiative, and to modernize its Fara.gov website, thereby increasing transparency for the public. These resources directly relate to Strategic Objective 1.3 Combat unauthorized disclosures, insider threats, and hostile intelligence activities.

Funding

Base Funding

FY 2019 Enacted				FY 2020 Enacted				FY 2021 Current Services			
Pos	Agt/ Atty	FTE	$(000)	Pos	Agt/ Atty	FTE	$(000)	Pos	Agt/ Atty	FTE	$(000)
39	28	34	$ 10,921	47	34	41	12,606	47	34	45	$ 13,549

Personnel Increase Cost Summary

Type of Position/Series	Full-year Modular Cost per Position ($000)	1st Year Adjustments	Number of Positions Requested	FY 2021 Request ($000)	2nd Year Annual-ization	FY 2022 Net Annualization (change from 2021) ($000)	FY 2023 Net Annualization (change from 2022) ($000)
Attorneys (0905)	$ 292	$ 175	2	$ 350	$ 517	$ 166	$ -
Total Personnel	**$ 292**	**$ 175**	**2**	**$ 350**	**$ 517**	**$ 166**	**$ -**

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2021 Request ($000)	FY 2022 Net Annualization (change from 2021) ($000)	FY 2023 Net Annualization (change from 2022) ($000)
Software upgrades for FARA.gov website	$ 200	1	$ 200	$ -	0
Total Non-Personnel	**$ 200**	**1**	**$ 200**	**$ -**	**0**

Total Request for this Item

	Pos	Agt/Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2022 Net Annualization (change from 2021) ($000)	FY 2023 Net Annualization (change from 2022) ($000)
Current Services	47	34	45	$ 13,549	$ -	$ 13,549	$ -	
Increases	2	2	1	$ 350	$ 200	$ 550	$ 166	$ -
Grand Total	**49**	**36**	**46**	**$ 13,899**	**$ 200**	**$ 14,099**	**$ 166**	**$ -**

2. 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 Section

Program Increase: Positions 1 Atty 1 FTE 1 Dollars $175,000

Description of Item

NSD requests $175,000 for one (1) new attorney position for its Foreign Investment Review Section (FIRS). The position would be an Attorney-Advisor, and as discussed in more detail below would handle an emerging workstream involving supply chain risk mitigation. This request directly enhances DOJ's cyber security goals as they relate to national security, the top priority of the Attorney General in preparing the FY21 budget. Further, this addition would support the efforts that form DOJ's China Initiative.

Justification

NSD works to prevent and disrupt national security threats, and 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 United States for national security risks, mitigates those risks through contractual agreements with the parties to transactions, and monitors compliance with those mitigation agreements going forward. NSD prioritizes those transactions that pose a risk to the security of the telecommunications sector, law enforcement or intelligence community equities (e.g., tools, techniques, facilities, and jurisdiction), or personal information or privacy (e.g., PII and PHI); or that may otherwise give a foreign intelligence service access to a collection platform in the United States. Our increasing reliance on computer and telecommunications networks means that cybersecurity is an increasing component of FIRS's reviews.

One main function of the new attorney position would be to fulfill new responsibilities NSD will need to undertake to support pending regulations under Executive Order 13873 relating to the supply chain threat to telecommunications. That Executive Order was signed by the President in May 2019, and NSD has been assisting the Department of Commerce in drafting regulations to implement the Executive Order. The regulations will establish an interagency process for the U.S. Government to review certain transactions that present telecommunications supply chain risks, and NSD will have a major role, on an ongoing basis, in participating in these interagency

reviews. The Attorney Advisor would participate in these reviews on behalf of NSD, and perform other work related to the Executive Order and the regulations.

The other main function of the new attorney position would be to serve as FIRS's expert on mitigating supply chain risks presented by the transactions FIRS currently reviews in two primary capacities, as DOJ'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 Federal Communications Commission (FCC) on whether to grant certain telecommunications license applications). The number of transactions reviewed by NSD has increased significantly in recent years, and is anticipated to continue increasing in the coming years. Where transactions present national security concerns, they may be either prohibited or mitigated, as noted above, through contractual agreements with the parties to transactions. Because the vast majority of transactions that present national security concerns are mitigated rather than prohibited, as time goes on, the volume of mitigation agreements that NSD must monitor steadily increases. Indeed, priority agreements have increased by 36 percent from 2018 to 2019. In both CFIUS and Team Telecom cases reviewed by FIRS, priority national security risks are increasingly including supply chain issues, and therefore FIRS increasingly needs to address supply chain risk in mitigation agreements and ongoing compliance monitoring of those agreements.

The new Attorney-Advisor would work with FIRS's compliance team on supply chain risk, which among other things would include providing guidance on 1) crafting mitigation provisions that address supply chain risk; 2) negotiating those mitigation provisions with parties to CFIUS and Team Telecom mitigation agreements; and 3) monitoring parties' compliance with mitigation provisions that involve supply chain risk. The Attorney-Advisor would also be responsible for helping ensure that CFIUS and Team Telecom supply chain risk mitigation is consistent with mitigation strategies and activities that occur pursuant to the regulations promulgated to implement the Executive Order discussed above.

Impact on Performance

An additional personnel resource dedicated to mitigating supply chain risks to the Nation's telecommunications and other infrastructure will enhance NSD's ability to ensure that our Nation's sensitive technologies and critical infrastructure are protected from foreign ownership or control that could pose an unacceptable risk to U.S. national security. This request supports the Strategic Objective 1.3 of combating 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. The request also directly enhances DOJ's cyber security goals as they relate to national security, highlighted in the Attorney General's FY 2021 budget priorities, and it forms part of DOJ's China Initiative.

Funding

Base Funding

FY 2019 Enacted				FY 2020 Enacted				FY 2021 Current Services			
Pos	Agt/ Atty	FTE	$(000)	Pos	Agt/ Atty	FTE	$(000)	Pos	Agt/ Atty	FTE	$(000)
13	9	11	$ 3,640	34	25	23	$ 8,749	34	25	33	$ 10,721

Personnel Increase Cost Summary

Type of Position/Series	Full-year Modular Cost per Position ($000)	1st Year Adjustments	Number of Positions Requested	FY 2021 Request ($000)	2nd Year Annual-ization	FY 2022 Net Annualization (change from 2021) ($000)	FY 2023 Net Annualization (change from 2022) ($000)
Attorneys (0905)	$ 292	$ 175	1	$ 175	$ 258	$ 83	$ -
Total Personnel	**$ 292**	**$ 175**	**1**	**$ 175**	**$ 258**	**$ 83**	**$ -**

Total Request for this Item

	Pos	Agt/Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2022 Net Annualization (change from 2021) ($000)	FY 2023 Net Annualization (change from 2022) ($000)
Current Services	34	25	33	$ 10,721	$ -	$ 10,721	$ -	$ -
Increases	1	1	1	$ 175	$ -	$ 175	$ 83	$ -
Grand Total	**35**	**26**	**34**	**$ 10,896**	**$ -**	**$ 10,896**	**$ 83**	**$ -**

3. Intelligence Collection and Oversight

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

Strategic Objective: 1.1: Disrupt and defeat terrorist operations

Budget Decision Unit(s): National Security Division

Organizational Program: Office of Intelligence

Program Increase: Positions 2 Atty 1 FTE 1 Dollars $1,060,000

Description of Items

NSD's Office of Intelligence (OI) requests two (2) positions, including one (1) attorney and one (1) program specialist, $91,000 for equipment, and $650,000 to support reengineering/rebuilding its critical case tracking system for a total of $1,060,000.

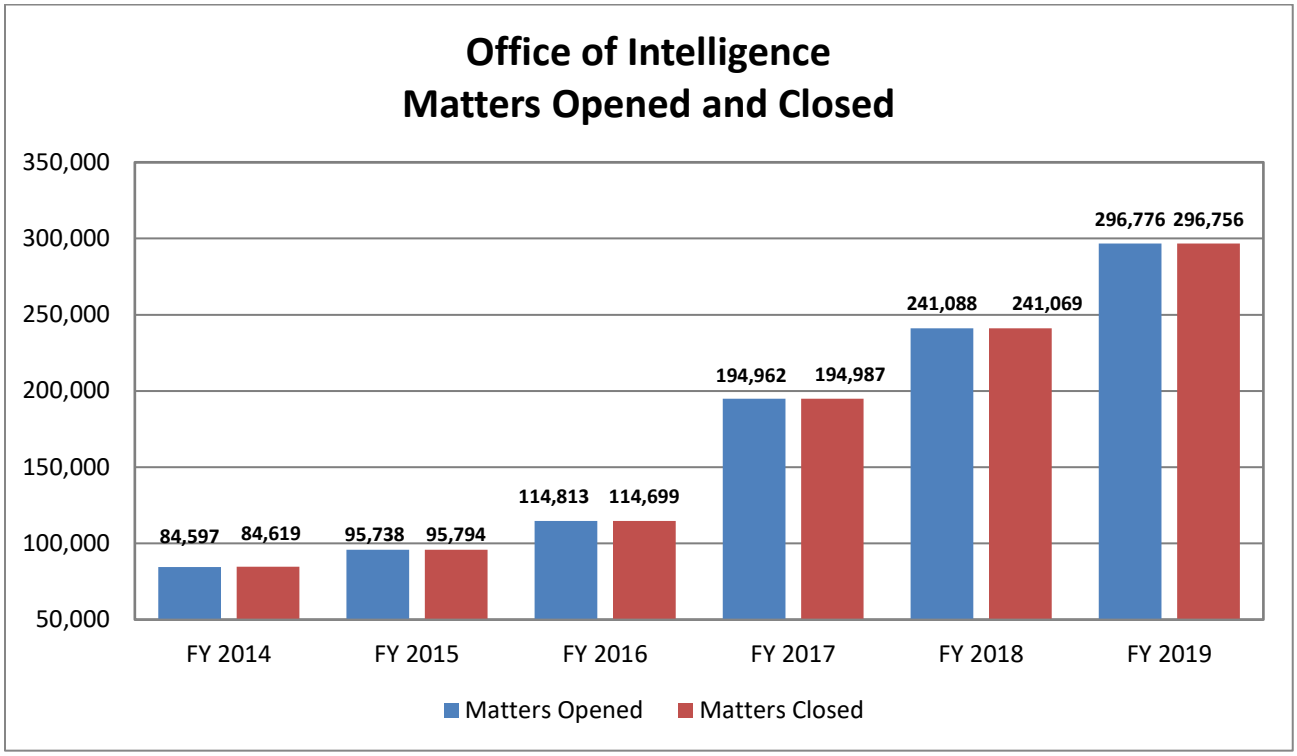
Justification

OI serves a critical role in DOJ's effort to prevent acts of terrorism and cyber attacks and to thwart hostile foreign intelligence activities. OI ensures that: 1) Intelligence Community (IC) agencies have the legal authorities necessary to conduct intelligence operations, particularly operations involving the Foreign Intelligence Surveillance Act (FISA); 2) OI exercises meaningful oversight over various national security activities of IC agencies; and 3) OI plays an effective role in FISA-related litigation. Within NSD, OI has primary responsibility for representing the government before the FISC and obtaining approval for foreign intelligence collection activities under FISA, conducting oversight to ensure that those authorities, and other national security authorities, are used in compliance with the law, and defending the use of FISA collection in criminal cases. OI conducts this work in an entirely classified setting, working on some of the most sensitive and significant cases in the government. OI works on the early stages of investigation of serious matters, often obtaining the initial legal authority to combat threats as diverse as cybercrime, foreign influence operations and terrorist activity. This work all directly supports DOJ's priority initiative of effectively identifying, disrupting, and prosecuting terrorist acts, as well as investigating and prosecuting cybercrimes and foreign intelligence threats to our nation, in compliance with lawful authorities.

Personnel

Over the last several years, OI's work has significantly grown in volume and complexity. As reflected in the below chart, between FY 2014 and FY 2018, OI experienced a roughly 185 percent increase in the number of matters handled each year, and of particular note a 70 percent increase between FY 2016 and FY 2017 alone (and an additional 24 percent increase between FY 2017 and FY 2018). This increase is reflective of OI's work countering the diverse foreign intelligence threats we face, as well as supporting wide-ranging and complex matters

such as declassification reviews, reviews of legislative proposals, document productions to Congressional committees, and responses to FOIA and other types of litigation.



OI plays a primary role in implementing and overseeing Section 702 of FISA. As President Trump stated in January 2018 when he signed the bill re-authorizing this provision of FISA 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." All taskings under the Section 702 program are reviewed by OI to ensure compliance with the law. The number of Section 702 targets has steadily increased over the last several years, and shows no signs of abating. Between CY 2014 and CY 2018, the number of Section 702 targets increased roughly 78 percent from 92,707 to 164,770. The requested increase in OI resources is needed to continue effectively supporting this vital program as it continues to grow.

Equipment

OI is also requesting $91,000 to acquire 130 stand-alone printers. Stand-alone printers are critical to OI's ability to meet the requirements of the IC and the FISC:

- Security requirements: The overwhelming amount of work done by OI personnel is classified in nature, much of it subject to compartmentation and other restrictions on dissemination, even to other OI personnel who have Top Secret clearances. As part of their daily work, OI personnel must print numerous and voluminous documents regarding such sensitive matters as human sources, investigatory techniques, and the identity of the subjects of national security investigations. In addition, OI handles numerous "close hold" cases and other compartmented filings, *i.e.*, matters for which our IC partners have

asked that only a small number of individuals be read into because of particular sensitivities. Ensuring that OI properly applies "need to know" principles requires that additional steps be taken to limit broad access to information. Budgetary limitations requiring communal printing on Multi-Functional Devices (MDFs) do harm to "need to know" and "close hold" principles required by the IC. By requiring attorneys to print to a shared printer, OI loses control over who has access to and can see this compartmented information, thus doing away with safeguards that OI currently has in place.

- Operational requirements: Stand-alone printers are also an operational necessity in OI, where the practice is extremely paper-intensive. In addition to reviewing paper copies of each case, OI is required by FISC rules to file three paper copies of every case. The volume of pages to be printed just for official filings with the FISC is extremely high. By way of example during two representative weeks, the weeks of March 4 and 11, 2019, we calculate that approximately 8,808 pages and 10,482 pages, respectively, were printed just to be filed with the FISC. Timing in addition to sheer volume is also at issue in OI's cases, since often attorneys are printing matters at the same time in order to meet court filing deadlines. Relying on communal MFD printers creates bottlenecks and puts OI attorneys at risk of missing Court-ordered filing deadlines.

In order to meet these requirements, OI has historically provided its staff with stand-alone printers. However, many of these printers are beginning to fail or have broken-down completely. Reliance on communal MDF printers has been shown to be an unsatisfactory substitute, as discussed above.

Case Tracking System

In support of its critical national security mission, OI uses a number of information technology (IT) systems to provide needed case tracking and reporting capabilities. The current OI Case Tracking system was developed in 2002 as a client/server application, built with the Microsoft Visual Basic 6 programming language using a Ricoh eCabinet document repository. In 2011, Ricoh eCabinet was discontinued/reached end-of-life and the repository was replaced with a new vendor/product, OpenText Livelink/Content Server. However, the Case Tracking application itself has remained in its original format since its inception- which is now obsolete, having been superseded by other modern programming languages and frameworks. The technology officially became unsupported by the vendor (Microsoft) as of April 8, 2008. In order to meet ever-changing business needs, numerous single purpose ancillary tools have been developed in-house using modern web-based methods. While this strategy has allowed the technology to meet the immediate business needs, it has also led to an unsustainable model of disparate and complex add-on tools.

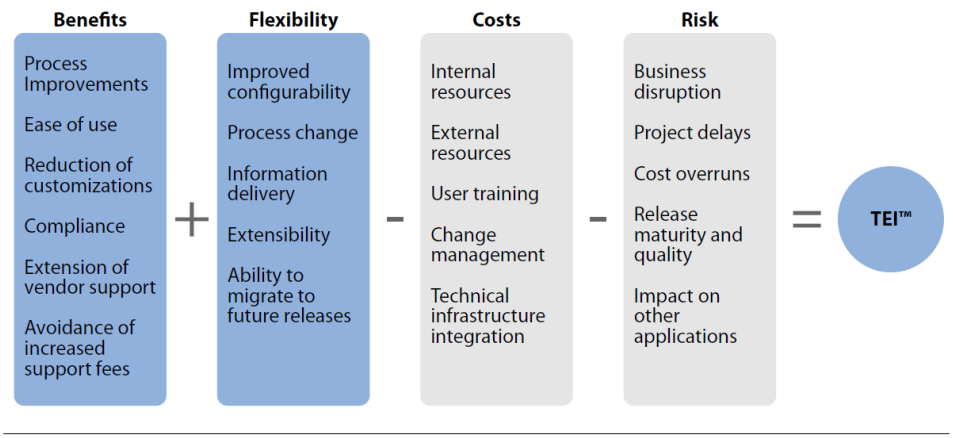
In addition, given the lack of vendor support and significantly diminished use of the underlying technology within the industry the current Case Tracking system now operates in an environment that poses a number of risks and vulnerabilities, both from an IT and business perspective. From possible system failures and data loss, to insider threat and lack of security controls, the continued use of the Case Tracking system poses significant risks in critical areas such as information security, sustainment and quality management. Indeed, NSD was recently advised by the FBI and the National Institute of Standards and Technology (NIST) that, based on its unsupported technology and its antiquated security controls, within the next couple of years the

current Case Tracking system may be found not to comply with federally mandated governance controls. NSD eventually will likely lose the authority to operate this system if not upgraded to a current technology and security base, which would grind NSD's critical national security practice to a halt.

Moreover, in 1998, Congress amended the Rehabilitation Act of 1973 to require Federal agencies to make their electronic and information technology (EIT) accessible to people with disabilities. The law (29 U.S.C. § 794 (d)) applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Under Section 508, agencies must give disabled employees and members of the public access to information that is comparable to the access available to others. The core Case Tracking system does not meet requirements of Section 508 in 3 out of 12 areas and is only partially compliant in 2 out of 12. In order to meet all 508 requirements, significant re-engineering activities would likely be required.

Using industry best-practice methodologies, such as Forrester's Total Economic Impact (TEI), IT would provide recommendations for NSD leadership that best support provided user stories and priorities. Unlike typical cost/benefit analyses for upgrades, which limit the ability of the organization to measure the full economic impact of the investment, this type of methodology would also add the dimensions of risk or uncertainty, as well as future flexibility (see below).

Figure 5 Total Economic Impact Framework For Upgrade Decisions



56624 Source: Forrester Research, Inc.

Based on the above figure (costs column) as well as expected outcomes from the project's current progress, additional budget, estimated at around $650,000, is necessary to accommodate external resources, user training, and technical infrastructure integration activities.

Impact on Performance

These requested positions, stand-alone printers, and rebuild/re-engineer of OI's case tracking system are critical to DOJ's efforts to fully support the nation's security, including its mission to disrupt and defeat terrorist operations and its ever-growing role in preventing cyber attacks. OI plays a critical role supporting IC partners as well. As those partners continue to grow, and technological capabilities continue to evolve, particularly regarding cyber security matters, NSD will need commensurate resources to support IC operations while maintaining the rule of

law. With these additional resources, NSD anticipates it will have sufficient staff and equipment to fully execute the intelligence-related work needed to support its national security mission, including countering terrorist and cyber threats. All of the requested resources are critical to ensure that NSD can keep pace with the changing and growing threat landscape, and to fully support disruption of these threats. OI's success is measured in part by the IC Oversight Reviews performance goal.

Funding

Base Funding

FY 2019 Enacted				FY 2020 Enacted				FY 2021 Current Services			
Pos	Agt/ Atty	FTE	$(000)	Pos	Agt/ Atty	FTE	$(000)	Pos	Agt/ Atty	FTE	$(000)
136	108	119	$ 38,083	136	108	130	$ 38,890	136	108	130	$ 39,551

Personnel Increase Cost Summary

Type of Position/Series	Full-year Modular Cost per Position ($000)	1st Year Adjustments	Number of Positions Requested	FY 2021 Request ($000)	2nd Year Annual-ization	FY 2022 Net Annualization (change from 2021) ($000)	FY 2023 Net Annualization (change from 2022) ($000)
Program Specialist (0300-0399)	$ 229	$ 144	1	$ 144	$ 200	$ 57	$ -
Attorneys (0905)	$ 292	$ 175	1	$ 175	$ 258	$ 83	$ -
Total Personnel	**$ 521**	**$ 319**	**2**	**$ 319**	**$ 459**	**$ 140**	**$ -**

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2021 Request ($000)	FY 2022 Net Annualization (change from 2021) ($000)	FY 2023 Net Annualization (change from 2022) ($000)
130 Stand-alone Printers	$ 0.7	130	$ 91	$ -	$ -
Upgrade of Case Management Tracking System	$ 650	1	$ 650	$ -	$ -
Total Non-Personnel	**$ 651**	**131**	**$ 741**	**$ -**	**$ -**

Total Request for this Item

	Pos	Agt/Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2022 Net Annualization (change from 2021) ($000)	FY 2023 Net Annualization (change from 2022) ($000)
Current Services	136	108	130	$ 39,551	$ -	$ 39,551	$ -	$ -
Increases	2	1	1	$ 319	$ 741	$ 1,060	$ 140	$ -
Grand Total	**138**	**109**	**131**	**$ 39,870**	**$ 741**	**$ 40,611**	**$ 140**	**$ -**

4. Insider Threat Prevention and the Protection of National Security Classified Systems

Strategic Goal:	Goal 1: Enhance National Security and Counter the Threat of Terrorism
Strategic Objective:	1.1: Disrupt and defeat terrorist operations 1.2: Combat cyber-based threats and attacks 1.3: Combat unauthorized disclosures, insider threats, and hostile intelligence activities
Budget Decision Unit(s):	National Security Division
Organizational Program:	Executive Office

Program Increase: Positions 4 Atty 0 FTE 2 Dollars $1,038,000

Description of Item

NSD requests four (4) positions and $400,000 to support deterring, detecting, and mitigating insider threats as well as the protection of national security classified systems for a total of $1,038,000.

Justification

I. Insider Threat Prevention

An insider threat is the threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the U.S. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. Cybersecurity is of particular concern in insider threat cases, in light of the high level of access to government computer networks and classified information that is now available to hundreds of thousands of government employees, defense contractors, and third party vendors and consultants. This widespread access to sensitive information via the government's varied computer networks presents a tremendous challenge for monitoring and national security reviews, and requires investment of dedicated resources. Executive Order (E.O.) 13587 established the National Insider Threat Task Force (NITTF), under joint leadership of the Attorney General and the Director of National Intelligence. The primary mission of the NITTF is to prevent, deter and detect compromises of classified information by malicious insiders. As part of the E.O., Federal agencies with classified networks were directed to establish insider threat detection and prevention programs. The E.O. directs the NITTF to assist agencies in developing and implementing their insider threat programs, while ensuring the program standards do not erode civil liberties, civil rights, or privacy protections for government employees. In November 2012, following an extensive interagency coordination and vetting process, the National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs was issued via a Presidential Memorandum.

The requested positions – one (1) Senior Security Network Engineer, one (1) IT Specialist, and two (2) IT Risk/Forensic Analysts – will ensure NSD's compliance with this program by, among other things, (1) identifying, developing, implementing, and maintaining security-related processes that reduce NSD's operational risks; (2) applying digital forensic, intrusion, and malware analysis and reverse engineering techniques for identifying and characterizing events for signs of insider threat activity; and (3) designing and implementing security projects to include firewalls, network access control, vulnerability management, end-point protection, care, and content of NSD's Secret and Top-Secret networks.

II. Protection of National Security Classified Systems

As part of the standard 4-year technical refresh cycle for its classified network systems, NSD is seeking $400k to support the migration of the NSD-S (Secret) services to a DOJ sanctioned cloud platform. This is the estimated cost for NSD to begin hosting the current infrastructure within a cloud infrastructure. NSD is currently discussing classified cloud offerings with Microsoft, Amazon, and FBI. This enhancement will provide network redundancy, thus allowing NSD to manage disaster recovery using a hybrid premise and cloud provider model, which will include the NSD classified off-site location as well as cloud provider resources. The migration will also reduce overall cost to operate the secret classified network as NSD becomes less dependent upon the on premise server hardware, it also becomes less dependent costly hardware upgrades for replacement infrastructure as well as support on a variety of hardware, Resource scalability upward/outward will becomes less costly and reduce overall operational costs of the secret classified network

Impact on Performance

This request is critical to NSD's ability to guard against the threats posed by insiders who misuse information or improperly disclose it without authorization and to protect its classified systems. These additional resources directly support all strategic objectives under Strategic Goal 1: Enhance national security and counter the threat of terrorism.

Funding

Base Funding

FY 2019 Enacted				FY 2020 Enacted				FY 2021 Current Services			
Pos	Agt/ Atty	FTE	$(000)	Pos	Agt/ Atty	FTE	$(000)	Pos	Agt/ Atty	FTE	$(000)
73	14	64	$ 20,442	73	14	70	$ 20,875	73	14	70	$ 21,229

Personnel Increase Cost Summary

Type of Position/Series	Full-year Modular Cost per Position ($000)	1st Year Adjustments	Number of Positions Requested	FY 2021 Request ($000)	2nd Year Annual-ization	FY 2022 Net Annualization (change from 2021) ($000)	FY 2023 Net Annualization (change from 2022) ($000)
Senior Security Network Engineer and IT Specialist (INFOSEC) (2210)	$ 292	$ 175	2	$ 350	$ 517	$ 166	$ -
IT Risk/Forensic Analysts (2210)	$ 229	$ 144	2	$ 288	$ 401	$ 113	$ -
Total Personnel	**$ 521**	**$ 319**	**4**	**$ 638**	**$ 918**	**$ 280**	**$ -**

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2021 Request ($000)	FY 2022 Net Annualization (change from 2021) ($000)	FY 2023 Net Annualization (change from 2022) ($000)
NSD- S Cloud Transformation	$ 400	1	$ 400	$ -	$ -
Total Non-Personnel	**$ 400**	**1**	**$ 400**	**$ -**	**$ -**

Total Request for this Item

	Pos	Agt/Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2022 Net Annualization (change from 2021) ($000)	FY 2023 Net Annualization (change from 2022) ($000)
Current Services	73	14	70	$ 21,229	$ -	$ 21,229	$ -	$ -
Increases	4	0	2	$ 638	$ 400	$ 1,038	$ 280	$ -
Grand Total	**77**	**14**	**72**	**$ 21,867**	**$ 400**	**$ 22,267**	**$ 280**	**$ -**

5. Item Name: Victims Outreach and Support

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

Strategic Objective: 1.1: Disrupt and defeat terrorist operations

Budget Decision Unit(s): National Security Division

Organizational Program: Office of Justice for Victims of Overseas Terrorism's (OVT)

Program Increase: Positions 2 Atty 0 FTE 1 Dollars $206,000

Description of Item

Office of Justice for Victims of Overseas Terrorism's (OVT) is requesting $206,000 for two (2) positions: a Victim Outreach Specialist, and an Administrative Support Specialist.

Justification

Victim Outreach Specialist: In cases where the FBI's Victim Services Division (VSD) is not providing social support services to the victims (because there is not an open FBI investigation) – approximately 28 percent of OVT's recent cases – OVT may need to provide mental health referrals to victims during our interaction with them as we identify needs. For this reason, OVT is requesting a Victim Outreach Specialist (VOS). This position requires an individual trained in working with individuals who have suffered severe trauma, to support NSD's increasing direct contact with terrorism victims and ensure that NSD can provide support and resources to victims who are experiencing emotional and mental health issues when interacting with the U.S. government or participating in a foreign criminal justice proceeding. Moreover, even in cases where an FBI/VSD staff person is assigned, those staff are frequently not available over the long term as cases go to trial in foreign countries because the FBI staff are responding to the significant influx of new cases. As attorneys, OVT's current staff does not have the level of expertise in social services to provide the best possible trauma-informed victim assistance. A degree and licensure in social work would be an excellent background for this expertise.

Administrative Support Specialist*:* The primary functions the administrative person performs for OVT are travel support (including reservations, travel authorizations and vouchers in E2 for both staff travel and victim travel under the CJPAF program), Time and Attendance, employee on-boarding (including detailees and interns), conference call coordination, weekly staff meeting organization, and acting as OVT's administrative liaison. OVT does not currently have dedicated administrative resource, and as OVT's work volume continues to increase, so does its need for this dedicated resource. Travel support in particular is complex and requires significant training and lead-time.

Impact on Performance

OVT provides direct services to members of the public, specifically U.S. citizen victims of overseas terrorism. To meet the increased volume of cases OVT is handling in a comprehensive and competent manner, OVT needs the expertise of a social work-trained trauma specialist. This staff person is needed to develop a communication strategy that will allow us to make outreach to US citizens who have been victimized in overseas attacks and provide professionally competent services and referrals to a population that has been severely traumatized. Finally, OVT needs adequate clerical support so that attorneys are not spending large amounts of time performing clerical tasks, particularly complex travel arrangements for victims, as is now the case.

Funding

Base Funding

FY 2019 Enacted				FY 2020 Enacted				FY 2021 Current Services			
Pos	Agt/ Atty	FTE	$(000)	Pos	Agt/ Atty	FTE	$(000)	Pos	Agt/ Atty	FTE	$(000)
5	4	4	$ 1,400	5	4	5	$ 1,430	5	4	5	$ 1,454

Personnel Increase Cost Summary

Type of Position/Series	Full-year Modular Cost per Position ($000)	1st Year Adjustments	Number of Positions Requested	FY 2021 Request ($000)	2nd Year Annual-ization	FY 2022 Net Annualization (change from 2021) ($000)	FY 2023 Net Annualization (change from 2022) ($000)
Victim Outreach Specialist	$ 229	$ 144	1	$ 144	$ 200	$ 57	$ -
Clerical and Office Services (0300-0399)	$ 124	$ 62	1	$ 62	$ 101	$ 39	$ -
Total Personnel	**$ 645**	**$ 381**	**2**	**$ 206**	**$ 403**	**$ 197**	**$ -**

Total Request for this Item

	Pos	Agt/Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2022 Net Annualization (change from 2021) ($000)	FY 2023 Net Annualization (change from 2022) ($000)
Current Services	5	4	5	$ 1,454	$ -	$ 1,454	$ -	$ -
Increases	2	0	1	$ 206	$ -	$ 206	$ 197	$ -
Grand Total	**7**	**4**	**6**	**$ 1,660**	**$ -**	**$ 1,660**	**$ 197**	**$ -**

VIII. Exhibits