FY 2022
Performance Budget
Congressional Submission

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, which is among the Department of Justice's (DOJ) top priorities. NSD requests for Fiscal Year (FY) 2022 a total of 415 positions (including 279 attorneys), 349 FTE, and $123,093,000.[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 domestic terrorism 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 is responsible for and carries out DOJ's core national security functions and provides strategic national security policy coordination and development. NSD combines counterterrorism, counterintelligence, export control, and cyber prosecutors with attorneys who oversee 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 DOJ's national security efforts by ensuring greater coordination and unity of purpose between prosecutors, law enforcement agencies, intelligence attorneys, and the IC.

NSD is comprised of the following sections:

- Counterintelligence and Export Control Section (CES);
- Counterterrorism Section (CTS);
- Foreign Investment Review Section (FIRS);

[1] Within the totals outlined above, NSD has included a total of 26 positions, 26 FTE, and $17,788,000 for Information Technology (IT).

- Office of Intelligence (OI);
- Office of Justice for Victims of Overseas Terrorism (OVT);
- Office of Law and Policy (L&P); and
- Executive Office (EO).

C. NSD Major Responsibilities.

1. 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 Federal Bureau of Investigation (FBI), the IC, and the 93 United States Attorneys' Offices (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 and violations of sanctions;

- Coordinating, developing, and supervising investigations and prosecutions involving the unauthorized disclosure of classified information;

- Providing advice and assistance to prosecutors nationwide regarding the application of the Classified Information Procedures Act (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, export control and sanctions, and foreign influence.

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 93 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 and protection of classified information through the application of 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 United States (U.S.) Government efforts on the Financial Action Task Force.

3. Foreign Investment.

- Performing DOJ's staff-level work on the Committee on Foreign Investment in the United States (CFIUS), which reviews foreign acquisitions of domestic entities and certain other transactions that might affect national security, and makes recommendations to the President on whether such transactions pose risk to national security requiring prohibition or divestment;

- Identifying unreported transactions that might merit CFIUS review;

- Fulfilling the Attorney General's role as Chair of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (also known as Team Telecom) pursuant to Executive Order 13913 (Apr. 4, 2020), which is the interagency group through which the Executive Branch responds to Federal Communication Commission (FCC) requests for views relating to the national security and law enforcement implications of certain transactions relating to FCC authorizations and licenses issued under the Communications Act of 1934, as amended, the Cable Landing License Act of 1921, and Executive Order 10530 (May 10, 1954), that involve foreign ownership, control, or investment;

- Monitoring transactions approved pursuant to both the CFIUS and Team Telecom processes for compliance with any mitigation agreements;

- Making referrals, in consultation with the Department of Commerce and pursuant to Executive Order 13873 (May 15, 2019), for matters involving foreign equipment or service providers that pose undue and unacceptable national security risks to the information and communications technology and services supply chain of the U.S.; and

- 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.

4. Intelligence Operations, Oversight, and Litigation.

- Ensuring that IC agencies have the legal tools necessary to conduct intelligence operations;

- Representing the U.S. before the Foreign Intelligence Surveillance Court (FISC) to obtain authorization under the Foreign Intelligence Surveillance Act (FISA) for government agencies to conduct intelligence collection activities;

- Overseeing certain foreign intelligence, counterintelligence, and other national security activities of IC components to ensure compliance with the Constitution, statutes, and Executive Branch policies to protect individual privacy and civil liberties;

- Monitoring certain intelligence and counterintelligence activities of the FBI to ensure conformity with applicable laws and regulations, FISC orders, and 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 (DNI) and the IC.

4. Victims of Overseas 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 DOJ's participation in the National Security Council (NSC).

D. Recent Accomplishments (UNCLASSIFIED only).

- **Evolving Threat of Terrorism.** In 2019 and 2020, DOJ charged publicly more than 60 individuals for foreign fighter, homegrown violent extremist, and international terrorism-related conduct. These cases include, among others, individuals inspired by ISIS to plot violent acts in the U.S., but were arrested before leaving the U.S. or disrupted before they could take action, as well as individuals who were captured in Syria and returned to the United States to face justice. In addition, NSD prosecutors have provided technical assistance and case mentoring to foreign counterparts for cases involving returned foreign fighters.

- **Terrorism-Related Convictions.** Over the past year, NSD, in partnership with USAOs, secured numerous convictions and sentences, including:
  - Conviction and 25-year sentence for an individual with anti-government extremist views who attempted to carry out a bomb plot in Oklahoma City, Oklahoma;
  - Conviction and 30-year sentence for Bureau of Prison inmate for attempting to provide material support to a Foreign Terrorist Organization (FTO) and false statements (conduct occurred while the inmate was serving a sentence for a 2012 conviction for conspiring to provide material support to another FTO);
  - Conviction and 15-year sentence for an individual who plotted to carry out a suicide bomb attack in Washington, D.C.;
  - Six-year sentence and 15 years of supervised release for an individual who attempted to send cell phone equipment to be used by ISIS;
  - Conviction of an individual who traveled to Syria to join ISIS and was eventually captured and repatriated to the U.S. to face justice;
  - Multiple convictions of individuals who attempted to purchase chemical or biological weapons through the Dark Web;
  - Conviction for an individual who published bomb making instructions and advocated for violence against Americans; and
  - Conviction for cyberstalking and online harassment of an individual associated with a white supremacist group.

- **China Initiative.** In November 2018, DOJ announced the China Initiative, which is led by 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. NSD has pursued a number of high-priority economic espionage and trade secret theft cases involving China. Recent case examples include:
  - Xiaorong You (U.S. citizen born in China) was convicted in April 2021, in the Eastern District of Tennessee, after trial for economic espionage and theft of trade secrets related to BPA-free coatings, as part of a plan to set up a competing business in China;
  - Yu Zhou was sentenced in April 2021, in the Southern District of Ohio; and his wife, Li Chen, was sentenced in February 2021. Zhou and Chen pled guilty to conspiring to steal scientific trade secrets in the U.S. for financial gain in China.
  - Hao Zhang was sentenced in August 2020, in the Northern District of California, after trial conviction for economic espionage and theft of trade secrets related to the performance of wireless devices; and
  - Shan Shi was sentenced in February 2020, in the District of Columbia, after trial conviction 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 include:

- Charges against Fujian Jinhua Integrated Circuit Co, a state-owned Chinese company, and guilty plea of United Microelectronics Corp., a Taiwanese company, in the Northern District of California, for economic espionage related to their theft of dynamic random access technology from a major U.S. corporation; and
- DOJ worked with the Department of Commerce to add these Chinese companies to the 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 U.S.

- **Espionage Act Enforcement.** NSD continued its enforcement of the Espionage Act by successfully prosecuting defendants for espionage offenses. Recent case examples include:
  - In 2020, Mariam Taha Thompson was charged in the District of Columbia with espionage and retention of national defense information and pled guilty to committing espionage in March 2021;
  - In 2020, Alexander Yuk Ching Ma was charged in the District of Hawaii for conspiring to commit espionage; and
  - In 2020, Peter Debbins pled guilty in the Eastern District of Virginia for conspiring to commit espionage.

- **Combatting Malign Foreign Influence.** NSD significantly increased its efforts to combat malign foreign influence, primarily through rigorous FARA enforcement and improved transparency. The number of new registrants and new foreign principals under FARA more than doubled from 2016 through 2019.
  - In January 2021, NSD obtained criminal charges against Kaveh Lotfolah Afrasiabi for acting and conspiring to act as an unregistered agent of the Government of the Islamic Republic of Iran, in violation of FARA. Afrasiabi has identified or portrayed himself as a political scientist, a former political science professor or as an expert on foreign affairs, but since at least 2007 Afrasiabi allegedly had also been secretly employed by the Iranian government and paid by Iranian diplomats assigned to the Permanent Mission of the Islamic Republic of Iran to the United Nations in New York City;
  - In October 2019, NSD obtained criminal charges against Imaad Zuberi, a campaign fundraiser who pled guilty to violating FARA, tax evasion, and making almost $1 million in illegal campaign contributions. In 2021, Zuberi was sentenced to 12 years in prison;
  - 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; however, in March 2020, the Fourth Circuit reversed the district court and reinstated the guilty verdicts;
  - NSD has improved compliance by publishing more information and guidance on its website, FARA.gov. The website now includes Letters of Determination, redacted Advisory Opinions, a brochure entitled *Protecting the United States from Covert Foreign Influence*, and a robust section on Frequently Asked Questions. These improvements build on NSD's expansion of the website's search features, which enable full-text searches and downloads of results in bulk format of more than 80,000 online FARA filings; and

- NSD recent enforcement efforts have resulted in the registrations of multiple foreign-media entities that had not fulfilled their FARA obligations, including the U.S. agents of Russian state-funded media networks RT and Sputnik and of China's state-controlled television network, CGTN. These foreign media entities had been operating for many years in the U.S. without complying with FARA, preventing the public from knowing the full extent of their activity and which foreign governments are behind that activity.

- **Export Controls and Sanctions Enforcement.** NSD continued its rigorous enforcement of export controls and sanctions, including sanctions against Iran and North Korea. Recent case examples include:
  - In February 2020, NSD and the USAO in the Eastern District of New York filed a superseding indictment charging Chinese telecommunication company Huawei with conspiracy to violate RICO and conspiracy to steal trade secrets. Those charges were added to the existing charges, which included violating Iran sanctions;
  - In June 2020, Seyed Sajjad Shahidian pled guilty in the District of Minnesota for conspiring to conduct financial transactions in violation of U.S. sanctions against Iran. In October 2020, Shahidian was sentenced to 23 months in prison;
  - In July 2020, NSD and the USAO for the District of Columbia filed a complaint to forfeit $2,372,793. The complaint alleged that four companies laundered U.S. dollars on behalf of sanctioned North Korean banks;
  - In August 2020, NSD and the USAO for the District of Columbia disrupted a multimillion dollar fuel shipment by Iran's Islamic Revolutionary Guard Corps. The offices seized and confiscated the cargo from four vessels carrying the fuel, totaling approximately 1.116 million barrels of petroleum;
  - In December 2020, NSD and the USAO for the Western District of Texas charged a Russian citizen and two Bulgarian citizens for a scheme to ship sensitive radiation-hardened circuits from the U.S. to Russia without required licenses; and
  - In February 2021, NSD and the USAO for the District of Columbia filed a complaint alleging that all Iranian petroleum aboard the vessel M/T Achilleas was subject to forfeiture based on U.S. terrorism forfeiture laws.

- **National Security Cyber Cases.** NSD continues 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 case examples include:
  - In February 2020, NSD and the USAO for the Northern District of Georgia charged four members of the Chinese People's Liberation Army with hacking into the computer systems of the credit reporting agency Equifax and stealing nearly 150 million Americans' personal data and Equifax's valuable trade secrets;
  - In March 2020, NSD and the USAO for the District of Columbia charged two Chinese nationals with laundering over $100 million worth of cryptocurrency that had been stolen from a cryptocurrency exchange by North Korean actors in 2018. The charges were accompanied by a civil forfeiture complaint that detailed over $250 million stolen by the North Korean hackers and the seizure of some of those funds;

- In July 2020, NSD and the USAO for the Eastern District of Washington charged two Chinese hackers working with the PRC Ministry of State Security with a global computer intrusion campaign targeting intellectual property and confidential business information, including COVID-19 research; and
- In February 2021, NSD and the USAO for the Central District of California charged three North Korean computer programmers with a criminal conspiracy to conduct a series of destructive cyberattacks, to steal and extort more than $1.3 billion of money and cryptocurrency from companies, to create and deploy multiple malicious cryptocurrency applications, and to develop and fraudulently market a blockchain platform.

- **Combatting Russian Hacking and Disinformation.** NSD is actively prioritizing efforts to combat Russian attempts 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). A recent example includes:
  - In October 2020, NSD and the USAO for the Western District of Pennsylvania charged six Russian intelligence officers in Unit 74455 of the Russian Main Intelligence Directorate (GRU) for computer intrusions and attacks intended to support Russian government efforts to undermine, retaliate against, or otherwise destabilize: (i) Ukraine; (ii) Georgia; (iii) elections in France; (iv) efforts to hold Russia accountable for use of the Novichok nerve agent; and (v) the 2018 PyeongChang Winter Olympic Games. Their computer attacks used some of the world's most destructive malware to date, including NotPetya, which caused immense financial losses worldwide, including nearly $1 billion in losses to the three victims identified in the indictment.

- **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 U.S. 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 also has continued to prioritize cases involving unauthorized disclosures of classified information to the media.
  - In 2020, Henry Kyle Frese was sentenced in the Eastern District of Virginia to 30 months in prison for unauthorized disclosures to journalists; and
  - In April 2021, Daniel Everett Hale pled guilty in the Eastern District of Virginia to making unauthorized disclosures to a member of the media.

- **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.
  - Despite a decrease in transactions subject to CFIUS review during the global COVID-19 pandemic, NSD reviewed only approximately 7% fewer submissions in 2020 than the previous year regarding mergers, acquisitions, and investments;

- NSD led (on behalf of DOJ) approximately 24% of the cases in which a Joint Voluntary Notice was filed with CFIUS in 2020, which was approximately 6% higher than the previous year. In approximately 10% 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 15% of the cases in which a declaration was filed with CFIUS pursuant to the broader jurisdiction created by the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which was approximately 5% higher than the DOJ-led cases in which a declaration was filed with CFIUS pursuant to a similar FIRRMA pilot program for critical technologies in 2019;
- In early 2020, NSD played a significant role in the CFIUS review of the acquisition of StayNTouch, Inc. by Beijing Shiji Information Technology Company, Ltd., a public company organized under the laws of China, and its wholly owned subsidiary Shiji (Hong Kong) Ltd., a Hong Kong limited company. The President determined the transaction threatened to impair the national security of the U.S., and accordingly ordered in March 2020 that the purchaser divest all interests in StayNTouch;
- Also in 2020, NSD co-led (on behalf of DOJ) the CFIUS review of Chinese company ByteDance's 2017 acquisition of the U.S. business Musical.ly. This transaction resulted in Musical.ly's users and data being merged into ByteDance's TikTok mobile application. Based on the CFIUS review, the President ordered ByteDance to divest any tangible assets or property used to enable or support ByteDance's operation of the TikTok application in the U.S., as well as any data obtained or derived from relevant U.S. users of the application. Follow-up work to the presidential order continued into 2021;
- NSD now carries out the Attorney General's formal role as the chair of Team Telecom, an interagency group that reviews telecommunications, submarine cable landing, wireless, satellite earth station, and broadcast license applications involving foreign ownership, control, or investment for national security and law enforcement risks;
    - During the 90-days implementation period after Executive Order 13913 was signed in 2020, in its formal role as Chair of the formalized and strengthened Team Telecom, NSD resolved approximately half of the pending cases to-date, clearing the way to address more complex matters within the timeframes established by the Executive Order;
    - Team Telecom received 13% more applications to review in 2020 than in the previous year. NSD led or co-led 100% of the reviews for FCC referrals to Team Telecom for applications for licenses in 2020; and
    - Team Telecom recommended to the FCC that 6 of the applications it received in 2020 (stemming from 35 applications the FCC referred that involved a total of 78 telecommunications authorizations, cable landing licenses, and petitions for declaratory ruling) be granted contingent on mitigation measures. NSD led or co-led all of the cases that led to those dispositions.
- In another 2020 matter, NSD led the Executive Branch's review of a submarine cable landing license application filed with the FCC by applicants seeking to connect the Pacific Light Cable Network cable system, and in June 2020 recommended to the FCC, based on national security concerns, that the FCC partially deny based on the original makeup of the applicants' consortium and the application's desire to seek a direct connection between the U.S. and Hong Kong. The applicants subsequently withdrew the application

and filed a new application that involved a different combination of applicants and did not seek a direct connection between the U.S. and Hong Kong;

- NSD also led the Executive Branch's review of an FCC international telecommunications license held by China Telecom (Americas) Corp., the U.S. subsidiary of a People's Republic of China (PRC) state-owned telecommunications company, and in April 2020 recommended to the FCC, based on insurmountable national security and law enforcement concerns, that the FCC revoke and terminate the license; and
- NSD provided significant assistance to the Department of Commerce in crafting regulations pursuant to Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," which were published in 2020 and implement the Secretary of Commerce's new authority to prohibit transactions involving information and communications technology equipment and services that are produced or provided by a foreign adversary and pose an unacceptable or undue national security risk. In addition, in 2020 NSD submitted the first two referrals to the Secretary of Commerce pursuant to this new authority.

- **Regulations Implementing FIRRMA.** NSD also worked closely with the Department of the Treasury to draft proposed regulations implementing FIRRMA. These regulations were promulgated in early 2020.

- **FCC Rulemaking Related to Executive Branch Review of Certain Applications and Petitions Involving Foreign Ownership.** The FCC underwent a proceeding for a notice of proposed rulemaking (NPRM) titled "Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership" following Executive Order 13913's issuance. NSD led interagency efforts to draft and submit the Executive Branch's comments to the FCC in connection with its NPRM proceeding and helped shape new FCC regulations that aim to synchronize the FCC's processes with Team Telecom's operation under E.O. 13913.

- **Efforts in CFIUS and Team Telecom Cases.** NSD led two CFIUS cases and six Team Telecom cases in 2020 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 currently approximately 131, which reflects an approximate 25% decrease in mitigation agreements from the previous year, due to an initiative by NSD to reassess all lower-risk mitigation agreements and terminate ones that were no longer necessary. NSD also conducted approximately 13 in-person or virtual mitigation compliance site visits in 2020 to monitor companies' compliance.

- **FISA Section 702 Compliance.** As part of its oversight responsibilities, NSD reviews all taskings under the Section 702 program to ensure compliance with FISA. 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. For example, between CY 2014 and CY 2019, the number of Section 702 targets increased roughly 121%. In the last three calendar years, NSD has also experienced steady increases in the number of potential Section 702 incidents reported by the IC as the number of

taskings has increased. NSD dedicates substantial resources to investigating each such potential incident and remediating compliance incidents with the FISC. Additionally, in CY 2019, 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. If not for the COVID-19 pandemic, CY 2020 was on pace to exceed the workload completed in CY 2019.

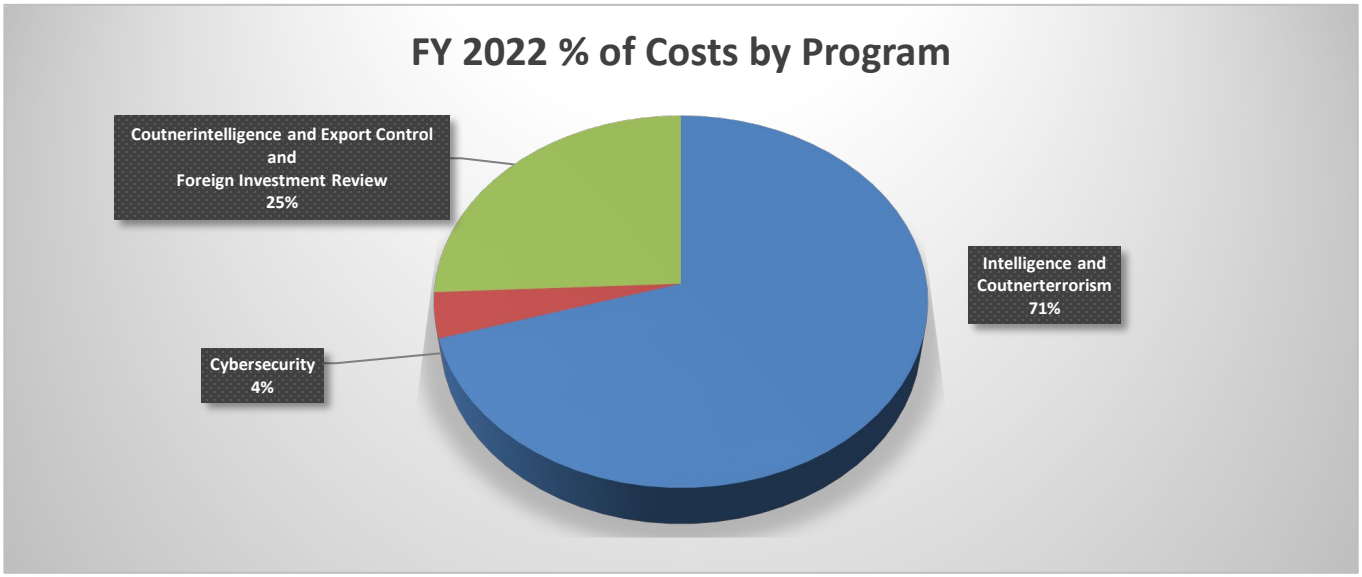
- **Expansion of NSD FISA Oversight.** The FBI and NSD have undertaken multiple corrective measures to ensure the accuracy and completeness of applications submitted to the FISC following the findings and recommendations of the Office of the Inspector General's (OIG) December 2019 Report, *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* (OIG Report). One aspect of NSD's oversight of FBI's FISA applications submitted to the FISC includes the conduct of accuracy reviews to ensure that the facts contained in a FISA application are accurate. NSD conducts multiple accuracy reviews each calendar year during oversight reviews at FBI field offices. In light of the findings of the OIG Report, NSD expanded the nature of its accuracy reviews, which have required additional resources to complete. For example, NSD has expanded its oversight of FBI FISA applications to include completeness reviews, which are resource intensive reviews, designed to identify whether material information has been omitted from a FISA application submitted to the FISC. NSD expanded its oversight in this manner during CY 2020 and has completed multiple such reviews.

- **Assisting Victims of Overseas Terrorism.** OVT assists U.S. citizen victims of overseas terrorism to attend foreign proceedings and participate in foreign criminal justice systems. Since the beginning of FY 2017, 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. In FY 2020 - 2021, OVT continued to support U.S. victims of international terrorism by providing them with foreign legal system information and communicating with foreign counterparts around the world, such as the United Kingdom, Belgium, Kenya, France, Israel, Germany, New Zealand, Bangladesh, and Pakistan.

- **Supporting International Cooperation on Victims of Terrorism.** OVT has cooperated with the U.S. Department of State's Bureau of Counterterrorism on membership and participation in the Council of Europe's 24/7 Network of Contact Points on Victims of Terrorism, and with the U.S. Mission to the United Nations regarding the development of model legislative provisions for victims of terrorism.

E. Full Program Costs.

NSD has a single decision unit. The costs by program depicted below include each program'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 programs.



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 U.S. national and economic security.

Foreign governments and other non-state adversaries of the U.S. are engaged in aggressive campaigns to acquire superior technologies and commodities developed in the U.S., in contravention of export control and sanctions laws. The U.S. 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 U.S. adversaries employ multi-faceted campaigns to acquire valuable proprietary technologies and information through a combination of traditional and asymmetric approaches. For example, the U.S. 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 Team Telecom)—has also expanded to address the asymmetric threat. For CFIUS in particular, the volume of filings before CFIUS has increased significantly over the years. In CY 2019 (and even without the impact yet of new regulations, discussed below), overall NSD reviewed approximately 40% more submissions than in 2018 regarding mergers, acquisitions, and investments. In CY 2020, even during the global COVID-19 pandemic that resulted in decreased transactions, the number of submissions NSD reviewed decreased by only 7%.

In 2020, NSD (on behalf of DOJ) led approximately 24% of CFIUS cases in which a Joint Voluntary Notice was filed, and of those cases led by NSD, approximately 10% 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 15% of the cases in which a declaration was filed with CFIUS pursuant to the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) new process for certain non-control transactions.

With respect to Team Telecom, in addition to the Attorney General serving as the Chair under the new Executive Order, NSD also led or co-led 100% of the group's reviews in 2020. Of the 35 FCC referrals of applications in 2020 (that involved a total of 78 telecommunications authorizations, cable landing licenses, and petitions for declaratory ruling), Team Telecom recommended to the FCC that 6 of the total authorizations, licenses, and petitions for declaratory be granted contingent on mitigation measures.

FIRRMA was enacted in 2018, as part of the John S. McCain National Defense Authorization Act. This legislation reformed 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.

Implementing the law's new provisions, will require additional work from NSD. NSD supports multiple aspects of the CFIUS process. NSD performs reviews and investigations of transactions, serves as DOJ's representative on CFIUS, and currently expects an increase in cases in CY 2022 due to the implementation of FIRRMA and the increase in transactions that may have been deferred because of the global COVID-19 pandemic. As part of the review and investigation process, NSD evaluates threat assessments and modifies them as part of the risk assessment that NSD conducts in each case. NSD also monitors compliance with all mitigation agreements (approximately 131 and growing) to which DOJ is a party, approximately 45 of which represent an agreement associated with a CFIUS transaction.

As time goes on and the volume of CFIUS and Team Telecom cases increases, the volume of mitigation agreements that NSD must monitor will also steadily increase (although in 2020 NSD was successful in terminating approximately 44 mitigation agreements that were no longer necessary). Of the CFIUS and Team Telecom cases discussed above, two CFIUS cases and six Team Telecom cases led or co-led by NSD in 2020 resulted in national security agreements that NSD negotiated and entered into with companies and that NSD will monitor for compliance going forward. 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 4% of the cases that DOJ co-led in 2020 were 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 two-and-a-half years following passage of 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 prompted the Administration's desire to pursue the Executive Order discussed above, which formalized this process with stricter timelines, an administrative chair, and other indicia of a structured interagency process. NSD prepared to meet the challenge required by these increased responsibilities in effecting this change, and developed ways to achieve the goal of institutionalizing the governance of Team Telecom, including by formalizing the Attorney General's role as chair of the group.

Since the President 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 U.S.' telecommunications infrastructure. In 2020, NSD submitted the first two referrals to the Department of Commerce under the new authority.

Also among the most significant challenges that NSD continues to face is the rapid expansion and evolution of cyber threats to the national security. 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. 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 U.S. cybersecurity, espionage, economic espionage, and weapons of mass destruction. NSD's 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) IC agencies have the legal authorities necessary to conduct intelligence operations, particularly operations involving FISA; 2) OI exercises substantial oversight of national

security activities of IC agencies; and 3) OI plays an essential 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 and other national security authorities are used in compliance with the law, and facilitating appropriate use of FISA collection in criminal cases. OI conducts this work in an entirely classified setting,. OI works on the early stages of investigating serious matters of national security, often obtaining the initial legal authority to combat threats as diverse as international terrorism, cyber attacks by hostile foreign actors, and efforts by foreign actors to steal American technology. This work supports 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.

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.

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 19th Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of FISA, covering the period of June – November, 2017: "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 approximately 121% between CY 2014 and CY 2019. The substantial growth of NSD's Section 702 oversight program and the resulting impact on NSD's resources is also apparent from the 250% increase in the number of matters handled by OI, the NSD component that oversees this program, between FY 2014 and FY 2019. In addition, in the last three calendar years, OI also has also experienced steady increases in the number of potential Section 702 incidents reported by the IC as the number of taskings has increased. OI dedicates substantial resources to investigating each such potential incident reported by the IC or otherwise identified by OI. OI also dedicates resources to ensure the IC properly remediates compliance incidents. OI must report the details of each Section 702 compliance incident to the FISC and to Congress. OI expects that there will continue to be increases in such compliance investigations by OI in 2021 and 2022. In addition, as part of its oversight of the IC's use of Section 702, OI dedicates substantial resources to auditing the IC's querying of unminimized information collected pursuant to Section 702. In addition, OI expects that its oversight of the Section 702 program will significantly grow as the program expands to address the foreign intelligence priorities of the IC. By FY2022, OI expects that it will need additional resources to address aspects of the continued expansion of the program.

The FBI and OI have undertaken multiple corrective measures to ensure the accuracy and completeness of applications submitted to the FISC following the findings and recommendations of the Office of the Inspector General's (OIG) December 2019 Report, *Review of Four FISA*

Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation (OIG Report). One aspect of OI's oversight of FBI's FISA applications submitted to the FISC includes the conduct of accuracy reviews to ensure that the facts contained in a FISA application are accurate. OI conducts multiple accuracy reviews each calendar year during oversight reviews at FBI field offices. In light of the findings of the OIG Report, OI has expanded the nature of its accuracy reviews, which have required additional resources to complete. For example, OI has expanded its oversight of FBI FISA applications to include completeness reviews, which are resource intensive reviews. These reviews require additional human resources. In addition, the oversight and compliance mission of OI is accomplished on multiple levels: training, modernization of FISA procedures, new and evolving compliance review programs, reports to Congressional oversight committees and the FISC, and compliance trends analysis. OI develops and presents detailed, effective training programs on the rules governing FISA. Those rules, too, must regularly be updated to keep pace with changes in technology and protocols at the applicable IC agencies. OI leads such efforts to update legal procedures. These efforts are currently underway and will require, with complementary training and the development of additional oversight programs to ensure compliance with these procedures, additional resources.

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 U.S. NSD therefore requires resources to support preventing and disrupting acts of terrorism.

The U.S. faces increased threats of domestic terrorism. 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.

In March 2021, in light of this increased threat, and to promote coordination and consistency in domestic terrorism cases, DOJ issued a new directive to U.S. Attorney's Offices that requires reporting of all domestic terrorism cases to NSD. In addition, the directive grants NSD additional oversight of these cases.

With respect to international terrorism, despite ISIS' loss of territory in Syria and Iraq, ISIS supporters and propaganda continue to assist in the radicalization of others in the U.S. 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 U.S. by these individuals.

NSD is participating in and assisting USAOs with a number of prosecutions of U.S. citizens who have been repatriated from the custody of the Syrian Democratic Forces.

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 U.S. 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 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.

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. Continuing Need for Assistance to U.S. Citizen Victims of Overseas Terrorist Attacks and Support for Foreign 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 around the world, the incidence of foreign attacks harming U.S. victims continues. Moreover, terrorist attacks in Israel and areas under its control continue to harm Americans living in and visiting that region.

OVT assists 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 at 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, 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.

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. The number of cases active in foreign systems at any one time can vary. OVT's monitoring of those cases and its 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.

FYs 2020 and 2021 posed unique challenges to everyone in finding a "new normal," and OVT was no exception. New methods had to be developed and utilized in order to maintain our level of support for U.S. victims of overseas terrorism and their participation in foreign systems in the midst of a global pandemic. We continue to prepare for future international large-scale trials by engaging with our foreign counterparts and communicating with the U.S. victims and survivors.

5. Operational Challenges Related to the COVID-19 Pandemic.

The COVID-19 pandemic brought new and difficult operational challenges for NSD. NSD followed pandemic-related guidelines and restrictions issued by the Department and other government agencies in the National Capital Region. Because the health and safety of employees is paramount, NSD instituted extensive telework and flexible work schedules – with staff accessing office space only as required to carry out essential functions. Limited face-to-face interaction among employees and with partner agencies has affected the efficiency of NSD's operations. Many hearings and trials were postponed and NSD conducted fewer site visits to monitor compliance with CFIUS and Team Telecom mitigation agreements due to the pandemic. In addition, due to travel restrictions resulting from the pandemic, NSD transitioned to conducting its oversight visits of FBI field offices remotely, rather than in person. NSD looks forward to a gradual return to normal operations, as health conditions permit.

II. Summary of Program Changes

Item Name	Description				Page
		Pos.	Estimated FTE	Dollars ($000)	
Intelligence Collection and Oversight	Requesting additional resources for NSD's work related to intelligence oversight.	13	7	$2,690	45
	Grand Total: FY 2020 Enhancement Request	**13**	**7**	**$2,690**	

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, [$117,451,000] *$123,093,000, 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
2020 Enacted	391	317	$110,000,000
2021 Enacted	402	337	$117,451,000
Adjustments to Base and Technical Adjustments	0	5	$2,952,000
2022 Current Services	402	342	$120,403,000
2022 Program Increases	13	7	$2,690,000
2022 Program Offsets	0	0	$0
2022 Request	415	349	$123,093,000
Total Change 2021-2022	**13**	**347**	**$ 5,642,000**

National Security Division -Information Technology Breakout	Direct Pos.	Estimate FTE	Amount
2020 Enacted	22	22	14,603,000
2021 President's Budget	26	24	18,249,000
Adjustments to Base and Technical Adjustments	0	2	-461,000
2022 Current Services	26	26	17,788,000
2022 Program Increases	0	0	0
2022 Program Offsets	0	0	0
2022 Request	26	26	17,788,000
Total Change 2021-2022	**0**	**2**	**(461,000)**

1. Program Description.

NSD is responsible for:

- Overseeing terrorism investigations and prosecutions;
- Protecting critical national assets from national security threats, including through handling counterintelligence, counterproliferation, and national security cyber cases and matters; through reviewing, investigating, and assessing foreign investment in U.S. business assets; by countering malign foreign influence activities and enforcing FARA; and through investigations and prosecutions relating to the unauthorized disclosure and improper handling of classified information;
- 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;

- 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 U.S., including counterintelligence threats and cyber threats to the national security;
- 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 U.S., and develops strategies for emerging national security threats – including cyber threats to the national security;
- NSD administers the U.S. Government's national security program for conducting electronic surveillance and physical search of foreign powers and agents of foreign powers pursuant to FISA, and conducts oversight of certain activities of the IC components and the FBI's foreign intelligence and counterintelligence investigations pursuant to the Attorney General's guidelines for such investigations. NSD prepares and files all applications for electronic surveillance and physical search under FISA, represents the Government before the FISC, and – when evidence obtained or derived under FISA is proposed to be used in a criminal proceeding –obtains the necessary authorization for the Attorney General to take appropriate actions to safeguard national security;
- NSD also works closely with the congressional Intelligence and Judiciary Committees to ensure they are apprised of departmental views on national security and intelligence policy and are appropriately informed regarding operational intelligence and counterintelligence issues;
- NSD also advises a range of government agencies on matters of national security law and policy, participates in the development of national security and intelligence policy through NSC-led policy committees and the Deputies' Committee processes. NSD also represents 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, 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. To help fulfill the Attorney General's new role as Chair of Team Telecom, NSD also leads the interagency process to respond 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; and
- 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 Division											
RESOURCES		**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)**	
		FY 2020		**FY 2020**		**FY 2021**		**Current Services Adjustments and FY 2022 Program Changes**		**FY 2022 Request**	
Workload[1]											
Defendants Charged		**136**		**199**		**136**		**0**		**136**	
Defendants Closed		**131**		**77**		**131**		**0**		**131**	
Matters Opened		**175,730**		**255,036**		**350,740**		**200,000**		**550,740**	
Matters Closed		**175,592**		**254,849**		**350,602**		**200,000**		**550,602**	
FISA Applications Filed[2]		**CY 2020:** 1,800		**CY 2020:** 567		**CY 2021:** 1,500		**0**		**CY 2022:** 1,500	
National Security Reviews of Foreign Acquisitions		**CY 2020:** 500 [3]		**CY 2020:** 541		**CY 2021:** 500		**0**		**CY 2022:** 500	
Total Costs and FTE		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		317	110,000	333	110,000	337	117,451	12	5,642	349	123,093
TYPE	**PERFORMANCE**	**FY 2020**		**FY 2020**		**FY 2021 Request**		**Current Services Adjustments and FY 2022 Program Changes**		**FY 2022 Request**	
Activity	**Intelligence and Couterterrorism**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		227	79,755	227	79,755	229	82,396	11	4,936	240	87,332
Output Measure	Intelligence Community Oversight Reviews	**CY 2020:** 102		**CY 2020:** 70		**CY 2021:** 105		**25**		**CY 2022:** 130	
1Workload measures are not performance targets, rather they are estimates to be used for resource planning.											
2FISA applications filed data remains classified until the public report is submitted to the Administrative Office of the U.S. Courts and the Congress in April for the preceding calen											
3The target was incorrectly reported as 702 in previous submissions. The correct target is 500.											

PERFORMANCE AND RESOURCES TABLE											
Decision Unit: National Security Division											
RESOURCES		**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)**	
TYPE	**PERFORMANCE**	**FY 2020**		**FY 2020**		**FY 2021 Request**		**Current Services Adjustments and FY 2022 Program Changes**		**FY 2022 Request**	
Outcome Measure	Percentage of CT defendants whose cases were favborably resolved	90%		91%		90%		0%		90%	
Outcome Measure	Percentage of CT defendants whose cases were favborably resolved	99%		100%		99%		0%		99%	
Activity	**Cybersecurity**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		22	4,800	22	4,800	24	5,236	0	128	24	5,364
Outcome Measure	Percentage of Cyber defendants whose cases were favorably resolved	90%		0% [4]		90%		0%		90%	
Activity	**Counterintelligence and Export Control and Foreign Investment Review**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		68	25,445	68	25,445	84	29,819	1	578	85	30,397
Outcome Measure	Percentage of CE defendants whose cases were favorably resolved	90%		95%		90%		0%		90%	
Outcome Measure	Percentage of CE cases where classified information is safeguarded (according to CIPA	99%		100%		99%		0%		99%	
Output Measure	FARA inspections completed	18		9		9		9		18	
Output Measure	High priority national security reviews completed	CY 2020:	100	CY 2020:	90	CY 2021:	100	0		CY 2022:	100
4 No Cyber defendants' cases were closed in FY 2020.											

Performance Report and Performance Plan Targets		FY 2014	FY 2015	FY 2016	FY 2017	FY 2018	FY 2019	FY 2020		FY2021	FY2022
		Actual	Actual	Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Output Measure	Intelligence Community Oversight Reviews	CY 2014: 124	CY 2015: 100	CY 2016: 110	CY 2017: 102	CY 2018: 110	CY2019: 97	CY2020: 102	CY 2020: 70	CY2021: 105	CY2022: 130
Outcome Measure	Percentage of CT defendants whose cases were favorably resolved	92%	98%	99%	91%	91%	96%	90%	91%	90%	90%
Outcome Measure	Percentage of CT cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	100%	100%	100%	100%	100%	100%	99%	100%	99%	99%
Outcome Measure	Percentage of CE defendants whose cases were favorably resolved	98%	100%	100%	100%	100%	99%	90%	95%	90%	90%
Outcome Measure	Percentage of CE cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	100%	100%	100%	100%	100%	100%	99%	100%	99%	99%
Output Measure	FARA inspections completed	14	14	14	15	15	20	18	9	9	18
Output Measure	High priority national security reviews completed	CY 2014: 35	CY 2015: 38	CY 2016: 43	CY 2017: 65	CY 2018: 100	CY2019: 129	CY 2020: 100	CY 2020: 90	CY 2021: 100	CY 2022: 100
Outcome Measure	Percentage of Cyber defendants whose cases were favorably resolved	N/A	100%	100%	100%	100%	100%	90%	0% - No Cyber defendants' cases were closed in FY 2020	90%	90%

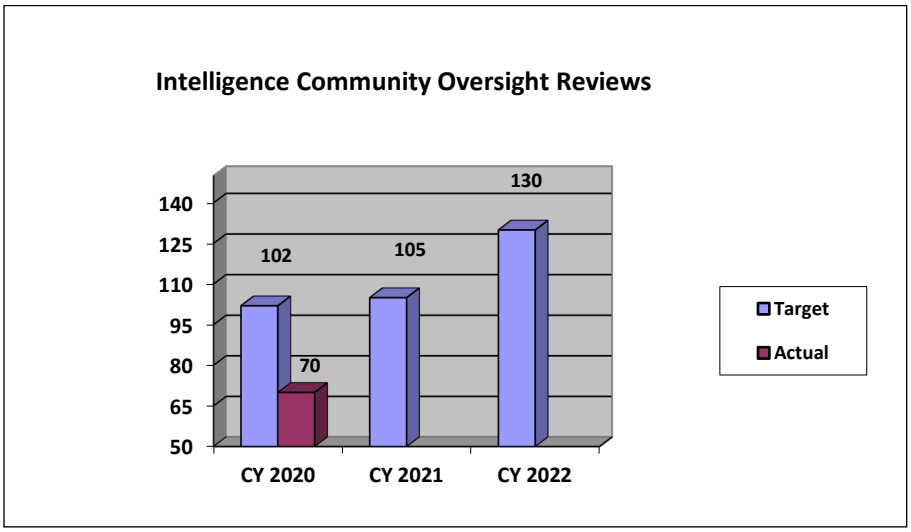
3. Performance, Resources, and Strategies.

For performance reporting purposes, resources for NSD are allocated among three program activities: Intelligence and Counterterrorism, Counterintelligence and Export Control and Foreign Investment Review, and Cybersecurity.

A. Performance Plan and Report for Outcomes

Intelligence and Counterterrorism Performance Report

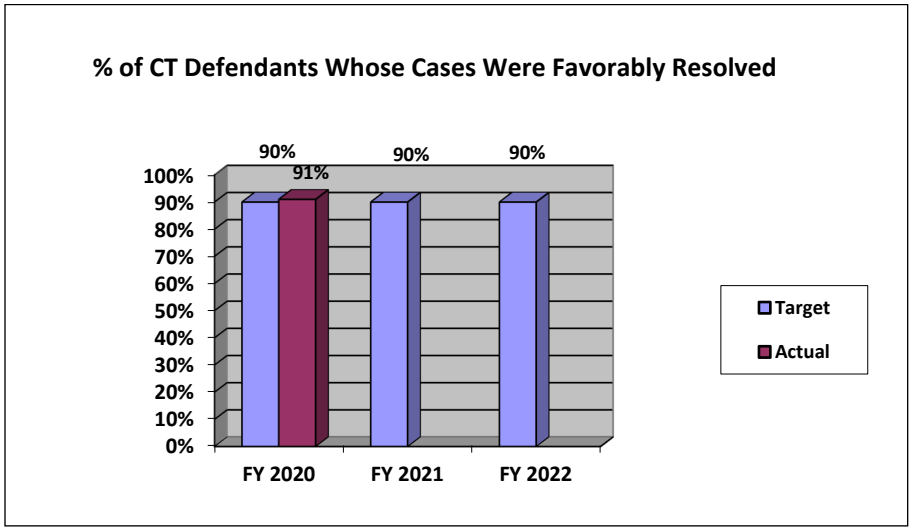
Measure: **Intelligence Community Oversight Reviews**
CY 2020 Target: **102**
CY 2020 Actual: **70**
CY 2021 Target: **105**
CY 2022 Target: **130**
Discussion: CY 2022- The CY 2022 target is consistent with previous targets. CY 2020 - Due to the suspension of travel to FBI field offices following March 2020 in response to the pandemic, OI was unable to meet its CY 2020 Intelligence Oversight Reviews target. Additionally, oversight resources during CY 2020 were used to develop, staff and implement categories of oversight reviews, known as completeness reviews, which were conducted for the first time in CY 2020, all of which were conducted remotely. Most of the reported oversight reviews were conducted remotely, and the Office of Intelligence will be conducting additional remote reviews in CY2021.



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 2020 Target: **90%**
FY 2020 Actual: **91%**
FY 2021Target: **90%**
FY 2022 Target: **90%**
Discussion: FY 2022 – The FY 2022 target is consistent with previous fiscal years. The strategies NSD will pursue in this area include consulting, advising, and collaborating with prosecutors nationwide on international and domestic terrorism prosecutions.



Data Definition: Defendants whose cases were favorably resolved include those defendants whose cases were closed during the fiscal year that resulted in court judgments favorable to the Government.
Data Collection and Storage: Data is stored and tracked in NSD's Case Management System (CMS).
Data Validation and Verification: Data validation and verification is accomplished via quarterly review by CTS management.
Data Limitations: None identified at this time.

Highlights from Recent Counterterrorism Cases

The following are highlights from recent counterterrorism cases.

U.S. v Taheb: In July 2020, in the Northern District of Georgia, Hasher Jallal Taheb ("Taheb") was sentenced to 180 months in prison, followed by three years of supervised release. On April 1, 2020, Taheb pled guilty to a one-count indictment charging him with attempting to damage or destroy, by means of an explosive, a building owned or possessed by the U.S., in violation of 18 U.S.C. § 844(f)(1).

In December of 2018, Taheb arranged a meeting with two individuals who, unbeknownst to him, were an undercover FBI agent ("UCE") and a confidential human source ("CHS"). During that meeting, Taheb stated that he wanted to carry out an attack in the U.S. During subsequent meetings, Taheb showed the UCE a hand-drawn diagram of the White House and described a plan for attacking the West Wing. Taheb also recorded a video and authored a 40-page document in which he extolled the importance of jihad and discussed his justification for creating and leading his group to conduct violent attacks in the U.S. In January of 2019, Taheb sent the UCE a list of weapons and explosives needed for the attack on the White House and detailed his plan to pick up the explosives and drive straight to Washington, D.C. to carry out the attack. Taheb provided the UCE with two backpacks to transport the explosives and continued to discuss his plan to attack the White House and achieve martyrdom.

On January 16, 2019, Taheb, the UCE, and the CHS drove to a parking lot to pick up the weapons and explosives that Taheb had ordered. Taheb discussed how to operate the weapons and explosives with the purported seller (who was actually a UCE) and also handled some of the explosives (all of which had been rendered inert prior to the meeting). Ultimately, Taheb took possession of two backpacks containing the inert explosives and was arrested.

U. S. v. Varnell: In March 2020, in the Western District of Oklahoma, Jerry Drake Varnell ("Varnell") was sentenced to 25 years in prison and a lifetime of supervised release for attempting to use a weapon of mass destruction at BancFirst in downtown Oklahoma City. In April 2018, a federal grand jury charged Varnell in a superseding indictment with attempting to use a weapon of mass destruction, in violation of 18 U.S.C. § 2332a, and attempting to destroy by fire or explosive a property used in interstate commerce, in violation of 18 U.S.C. § 844(i). He had been previously indicted only on the arson charge. In February 2019, a jury found Varnell guilty of the charged offenses.

In August 2017, Varnell, of Sayre Oklahoma, was arrested and charged by criminal complaint after trying to detonate an inoperable Vehicle Borne Explosive Device at the BancFirst building in downtown Oklahoma City. His arrest was the culmination of a long-term FBI undercover investigation. Varnell initially stated he wanted to blow up the Federal Reserve Building in Washington, D.C. with a truck bomb similar to the one used in the 1995 Oklahoma City attack because he was upset with the Government. Subsequently, he identified BancFirst as his target. As his plan developed, he prepared a statement to be posted after the explosion, helped assemble the device, and loaded it into a van that he believed was stolen. Varnell then drove the van from El Reno and parked it next to BancFirst. From a distance, he dialed a number on a cellular telephone believing it would trigger the explosion.

U.S. v. Shahnaz: In March 2020, in the Eastern District of New York, Zoobia Shahnaz ("Shahnaz") was sentenced to 13 years in prison. On November 26, 2018, Shahnaz pled guilty to one count of attempting to provide material support to the Islamic State of Iraq and al-Sham ("ISIS"), a designated foreign terrorist organization, in violation of 18 U.S.C. § 2339B.

The plea stemmed from Shahnaz's July 2017, attempt to board a flight from John F. Kennedy International Airport in Queens, New York to Turkey, seeking to join ISIS in Syria. Shahnaz had purchased a ticket and attempted to board the plane, but was stopped at the gate by law enforcement officials. In February 2018, a grand jury returned a six-count superseding indictment against Shahnaz, charging her with bank fraud, in violation of 18 U.S.C. § 1344, conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h), and three substantive counts of money laundering, in violation of 18 U.S.C. § 1956. As part of her plea agreement, Shahnaz admitted to defrauding numerous financial institutions and laundering the stolen proceeds out of the country with the intent to support a specified unlawful activity, namely the provision of material support to ISIS. After effectuating the scheme, Shahnaz attempted to leave the U.S. and travel to Syria.

U.S. 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, that 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 U.S. in 2003. By 2008, IJO recruited Kourani to its ranks. In August 2008, Kourani submitted an application for naturalization in the U.S. 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 U.S. 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 U.S. 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.

Multiple Forfeiture Complaints and a Criminal Complaint Targeting Terrorist Financing: In August 2020, in the District of Columbia, the U.S. unsealed three forfeiture complaints and a

criminal complaint representing the Government's largest-ever seizure of cryptocurrency in the terrorism context.

Hamas's al-Qassam Brigades Social Media Cryptocurrency Campaign

Starting in January 2019, Hamas's military wing, the al-Qassam Brigades, began a public fundraising campaign, soliciting Bitcoin ("BTC") donations on Twitter. The post called upon supporters to "Donate for Palestinian Resistance via Bitcoin" and provided a link to a BTC wallet where individuals could send donations to the al-Qassam Brigades. The al-Qassam Brigades subsequently began seeking BTC donations on its two websites, alqassam.net and alqassam.ps, and advised donors on how to obscure and layer their donations in an effort to avoid detection. In total, the al-Qassam Brigades' fundraising efforts on Twitter and through these two websites, raised more than $15,000 from supporters around the world. The investigation revealed that the al-Qassam Brigades intended to use the funds for "buying weapons and training mujahideen."

The Government secured search and seizure warrants that enabled the Government to seize and covertly operate the al-Qassam Brigades' website. The Government filed a civil forfeiture complaint seeking forfeiture of 53 virtual currency accounts, 127 virtual currency wallets, 5 financial accounts, and the two al-Qassam website domains. In addition, the Government has filed a criminal complaint against two Turkish individuals, identified during the course of the investigation, who were engaged in widespread money laundering and acting as unlicensed money transmitters.

AQ Cryptocurrency Fundraising

Al-Qaeda and affiliated terrorist groups have utilized a BTC money-laundering network, soliciting donations on Telegram channels and other social media platforms. Specifically, in April 2019, the administrator of the now-defunct Telegram group "Tawheed & Jihad Media" provided a BTC address as a repository for pro-al-Qaeda donations. Posts on the Tawheed & Jihad Media Telegram group during that same time solicited donations for fighters, including direct calls to finance "bullets and rockets for the mujahideen."

On or about May 5, 2019, the affiliated BTC address for Taweed & Jihad Media's fundraising effort sent its entire BTC balance to a BTC address cluster assessed to be a central hub used to collect and redistribute funds within a broader money-laundering network. Several other entities, some of which purport to be charities, have contributed to, or received funds from, this BTC cluster. The complaint details five such entities: Leave an Impact Before Departure, Al Ikhwa, Malhama Tactical, Reminders From Syria, and Al Sadaqah.

In total, the Government seeks to forfeit 155 BTC accounts associated with this terrorist-fundraising scheme.

Murat Cakar: ISIS Financier and COVID-19

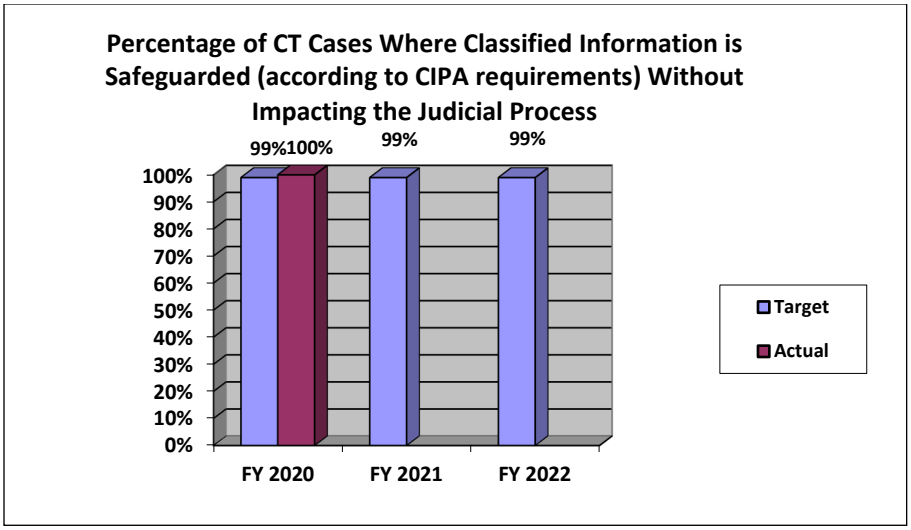
In spring of 2020, Murat Cakar, a Turkish-based financier, attempted to exploit the COVID-19 pandemic by selling fake personal protective equipment on a website and Facebook page—both of which contained materially fraudulent statements. Cakar, who received $100,000 from convicted terrorist Zoobia Shahnaz, is a known ISIS facilitator responsible for managing select ISIS hacking operations. Cakar used the fraudulent PPE website and other Facebook

accounts and businesses to defraud individuals and launder funds. The forfeiture complaint seeks forfeiture of the Facebook accounts and website used by Cakar to facilitate his criminal activity. On February 5, 2021, the Government filed a motion for default judgment.

Measure: **Percentage of CT Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**

FY 2020 Target: **99%**
FY 2020 Actual: **100%**
FY 2021 Target: **99%**
FY 2022 Target: **99%**

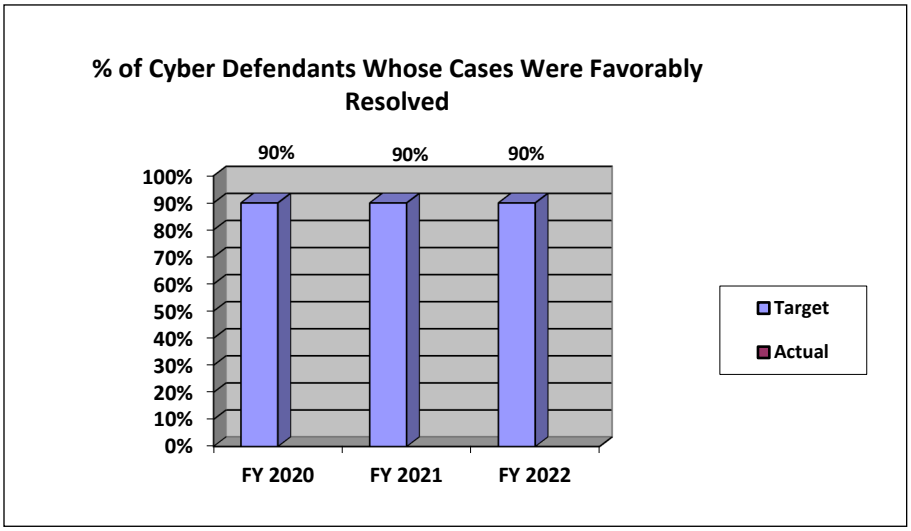
Discussion: The FY 2022 target is consistent with previous fiscal years. NSD will support successful prosecutions by providing advice and assistance on the use of classified evidence through the application of the Classified Information Procedures Act (CIPA).



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.

Cybersecurity Performance Report

Measure: **Percentage of Cyber Defendants Whose Cases Were Favorably Resolved**
FY 2020 Target: **90%**
FY 2020 Actual: **0%. Due to the complexity of these cases, they can take several years to resolve. Though 14 cyber defendants were charged in FY 2020, no defendants' cases were closed.**
FY 2021 Target: **90%**
FY 2022 Target: **90%**
Discussion: The FY 2022 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

U.S. v. Wu et al.: In February 2020, in the Northern District of Georgia, an indictment was unsealed charging four members of China's People's Liberation Army (PLA) with hacking into the computer systems of the credit reporting agency Equifax Inc. and stealing approximately 145 million Americans' personal data and Equifax's valuable trade secrets. The nine-count indictment alleges that Wu Zhiyong, Wang Qian, Xu Ke, and Liu Lei – members of the PLA's 54th Research

Institute, a component of the Chinese military – executed a conspiracy to commit computer fraud and abuse, economic espionage, and wire fraud. According to the indictment, in 2017 the defendants conspired with each other to exploit a vulnerability in the software used by Equifax's online dispute portal, gain unauthorized access to Equifax's systems, and spend several weeks running queries to identify Equifax's database structure and searching for sensitive, personally identifiable information, including names, dates of birth, and Social Security numbers. The defendants also are alleged to have stolen trade secret information, namely Equifax's data compilations and database designs. The defendants took steps to evade detection throughout the intrusion. They routed traffic through approximately 34 servers located in nearly 20 countries to obfuscate their true location, used encrypted communication channels within Equifax's network to blend in with normal network activity, and deleted compressed files and wiped log files on a daily basis in an effort to eliminate records of their activity.

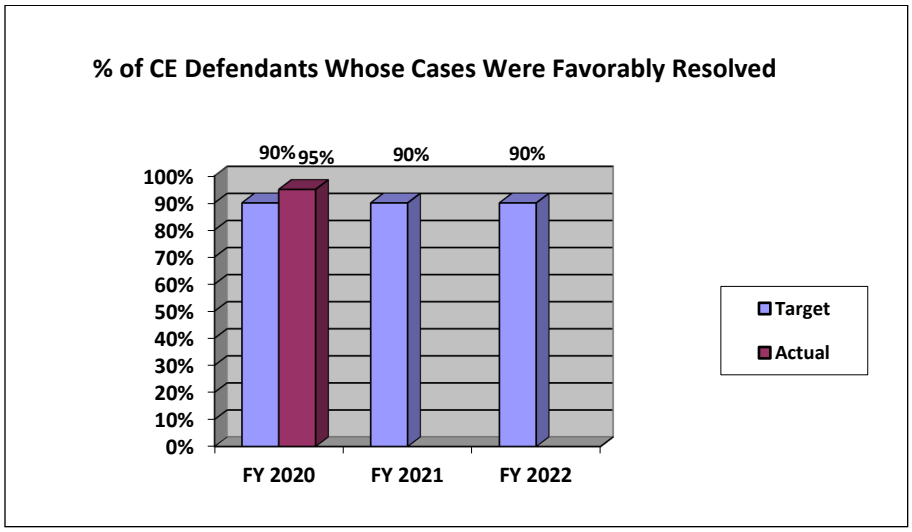
U.S. v. Andrienko et al.: In October 2020, in the Western District of Pennsylvania, a federal grand jury returned a seven-count indictment charging six computer hackers – all nationals of the Russian Federation and officers in Unit 74455 of the Russian Main Intelligence Directorate (GRU) – in connection with worldwide deployment of destructive malware and other disruptive actions in cyberspace. The defendants – Yuriy Andrienko, Sergey Detistov, Pavel Frolov, Anatoliy Kovalev, Artem Ochichenko, and Petr Pliskin – were charged with conspiracy to conduct computer fraud and abuse, conspiracy to commit wire fraud, wire fraud, damaging protected computers, and aggravated identity theft. These computer attacks used some of the world's most destructive malware to date, including: KillDisk and Industroyer, which each caused blackouts in Ukraine; NotPetya, which caused nearly $1 billion in losses to the three victims identified in the indictment alone; and Olympic Destroyer, which disrupted thousands of computers used to support the 2018 Winter Olympics. The GRU hackers engaged in computer intrusions and attacks intended to support Russian government efforts to undermine, retaliate against, or otherwise destabilize: (1) Ukraine; (2) Georgia; (3) elections in France; (4) efforts to hold Russia accountable for its use of a weapons-grade nerve agent, Novichok, on foreign soil; and (5) the 2018 PyeongChang Winter Olympic Games, after Russian athletes were banned from participating under their nation's flag, as a consequence of a Russian government-sponsored doping effort. The defendants and their co-conspirators caused damage and disruption to computer networks worldwide, including in France, Georgia, the Netherlands, the Republic of Korea, Ukraine, the United Kingdom, and the U.S.

U.S. v. Hyok et al.: In February 2021, in the Central District of California, an indictment was unsealed charging three North Korean computer hackers with participating in a wide-ranging criminal conspiracy to conduct a series of destructive cyber attacks, to steal and extort more than $1.3 billion of money and cryptocurrency from financial institutions and companies, to create and deploy multiple malicious cryptocurrency applications, and to develop and fraudulently market a blockchain platform. Jon Chang Hyok, Kim Il, and Park Jin Hyok were charged with conspiracy to commit computer fraud and abuse and conspiracy to commit wire fraud and bank fraud. The defendants were members of units of the Reconnaissance General Bureau, a military intelligence agency of the Democratic People's Republic of Korea, which engaged in criminal hacking. These military hacking units are known by multiple names in the cybersecurity community, including Lazarus Group and Advanced Persistent Threat 38 (APT38). The indictment alleges a conspiracy to cause damage, steal data and money, and otherwise further the strategic and financial interests of the DPRK Government and its leader, Kim Jong Un. The indictment lists a broad array of criminal cyber activities undertaken by the conspiracy, in the U.S. and abroad, for revenge or financial gain. The alleged schemes include: cyber attacks on the

entertainment industry; cyber-enabled heists from banks; cyber-enabled ATM cash-out thefts; ransomware and cyber-enabled extortion; creation and deployment of malicious cryptocurrency applications; targeting of cryptocurrency companies and theft of cryptocurrency; and spear-phishing campaigns targeting U.S. companies and government agencies.

Counterintelligence and Export Control and Foreign Investment Review Performance Report

Measure: **Percentage of CE Defendants Whose Cases Were Favorably Resolved**
FY 2020 Target: **90%**
FY 2020 Actual: **95%**
FY 2021 Target: **90%**
FY 2022 Target: **90%**
Discussion: The 2022 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.

U.S. v. 92 IRGC Domains: In October 2020, in the Northern District of California, the U.S. seized 92 domain names that were unlawfully used by Iran's Islamic Revolutionary Guard Corps (IRGC) to engage in a global disinformation campaign. According to the seizure documents, four of the domains purported to be genuine news outlets but actually were controlled by the IRGC and targeted the U.S. for the spread of Iranian propaganda to influence U.S. domestic and foreign policy in violation of FARA, and the remainder spread Iranian propaganda to other parts of the world. The seizure documents also describe how all 92 domains were being used in violation of U.S. sanctions targeting both the Government of Iran and the IRGC. Pursuant to the International Emergency Economic Powers Act (IEEPA), unauthorized exports of goods, technology, or services to Iran from the U.S. are prohibited; however, the Treasury Department may issue a license through its Office of Foreign Assets Control (OFAC). All 92 domains were owned and operated by U.S. companies. Neither the IRGC nor the Government of Iran obtained a license from OFAC prior to utilizing the domain names. The U.S. seized the 92 domain names pursuant to a seizure warrant.

U.S. v. All Petroleum et al.: In October 2020, in the District of Columbia, DOJ announced the filing of a civil complaint to forfeit two shipments of Iranian missiles that the U.S. Navy seized in transit from Iran's Islamic Revolutionary Guard Corps (IRGC) to militant groups in Yemen, and the sale of approximately 1.1 million barrels of Iranian petroleum that the U.S. previously obtained from four foreign-flagged oil tankers bound for Venezuela. The weapons and fuel were subject to seizure and forfeiture pursuant to 18 U.S.C. § 981, as assets of the IRGC – an organization engaged in terrorism. These actions represent the U.S. Government's largest-ever forfeiture actions for weapons and fuel shipments from Iran. U.S. Navy Central Command seized the weapons from two flagless vessels in the Arabian Sea in November 2019 and February 2020. The weapons included 171 guided anti-tank missiles, 8 surface-to-air missiles, land attack cruise missile components, anti-ship cruise missile components, thermal weapons optics, and other components for missiles and unmanned aerial vehicles. In August 2020, in D.C. District Court, DOJ filed a complaint seeking to forfeit the seized weapons. In July 2020, DOJ also filed a civil complaint seeking to forfeit all petroleum cargo aboard the four foreign-flagged oil tankers. D.C. District Court later issued a warrant for arrest in rem, and the U.S. subsequently transferred approximately 1.1 million barrels of refined petroleum from the four vessels. The U.S. now has sold that petroleum.

U.S. v. Man et al.: In May 2020, in the District of Columbia, a 14-count indictment was unsealed charging 28 North Korean nationals and 5 Chinese nationals in the largest-ever North Korean sanctions criminal enforcement action. The indictment alleges that the North Korean government operated a shadow banking system outside the purview of U.S. and U.N. sanctions. The defendants are charged with conspiring to defraud the U.S. by interfering with the lawful enforcement of U.S. sanctions and oversight of U.S. banks, to defraud U.S. banks that process international U.S. dollar wire transactions, to violate the International Emergency Economic Powers Act (IEEPA) and the Weapons of Mass Destruction Proliferators Sanctions Regulations, and to launder monetary instruments. The two lead defendants also are charged with conducting a continuing financial crimes enterprise. The indictment contains a forfeiture allegation noting that the U.S. government has seized approximately $63.5 million as part of this investigation. This represents the largest seizure of North Korean funds by DOJ and is one of the first-ever indictments of North Korean nationals. According to the indictment: North Korea's Foreign Trade Bank (FTB) is North Korea's primary foreign exchange bank and acts as a wholly state-owned institution that represents the government of North Korea in international banking. FTB

sent agents overseas to establish covert branches from which they would form front companies to circumvent U.S. sanctions, bank fraud laws, and money laundering laws. These agents set up covert offices in China, Russia, Thailand, Austria, Libya, and Kuwait, among others. From these covert branches, North Korea laundered over $2.5 billion in payments to procure various items. The covert branch agents engaged in coded communications with FTB Headquarters in North Korea about these illicit payments. Over 250 FTB front companies served to conceal FTB's presence from correspondent banks in the U.S. that processed these transactions.

U.S. v. Airbus SE: In January 2020, in the District of Columbia, Airbus SE (Airbus or the Company), a global provider of civilian and military aircraft based in France, agreed to pay combined penalties of more than $3.9 billion to resolve foreign bribery charges with authorities in the U.S., France, and the United Kingdom arising out of the Company's scheme to use third-party business partners to bribe government officials and non-governmental airline executives around the world, and to resolve the Company's violation of the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR) in the U.S. Airbus entered into a deferred prosecution agreement with DOJ in connection with a criminal information filed on January 28, 2020, in the District of Columbia charging the Company with conspiracy to violate the anti-bribery provision of the Foreign Corrupt Practices Act (FCPA) and conspiracy to violate the AECA and its implementing regulations, the ITAR. The FCPA charge arose out of Airbus's scheme to offer and pay bribes to foreign officials, including Chinese officials, in order to obtain and retain business, including contracts to sell aircraft. The AECA charge stems from Airbus's willful failure to disclose political contributions, commissions or fees to the U.S. Government, as required under the ITAR, in connection with the sale or export of defense articles and defense services to the Armed Forces of a foreign country or international organization.

The following are highlights from recent Counterintelligence Cases.

U.S. v. Imaad Shah Zuberi: In February 2021, in the Central District of California, campaign fundraiser Imaad Shah Zuberi was sentenced to 12 years in prison. In October 2019, Zuberi pled guilty to a three-count Information charging him with working as a foreign agent while lobbying high-level U.S. government officials – work that earned him millions of dollars. In addition to violating FARA, Zuberi was charged with tax evasion and making illegal campaign contributions that included funneling money from foreign entities and individuals to influence U.S. elections. In relation to the FARA charge, Zuberi agreed to plead guilty to submitting false registration statements in which he concealed his direction of a Sri Lanka lobbying effort, as well as the millions of dollars he received. In relation to the tax charge, Zuberi agreed to plead guilty to one count of tax evasion for failing to report on his 2014 tax return millions of dollars in income he received from Sri Lanka. In relation to the campaign finance charge, Zuberi agreed to plead guilty to violating the Federal Election Campaign Act in 2015 by making "conduit contributions" in the names of other people, reimbursing contributions made by others, and being reimbursed for contributions he made. In his plea agreement, Zuberi admitted that over a five-year period – 2012 through 2016 – he made or solicited more than $250,000 in illegal campaign contributions. Zuberi, who operated a venture capital firm called Avenue Ventures, solicited foreign nationals and representatives of foreign governments with claims he could use his influence in Washington, DC, to change U.S. foreign policy and create business opportunities for his clients and himself. According to court documents, clients gave Zuberi money for consulting fees, to make investments, or to fund campaign contributions. As part of his efforts to influence

public policy, Zuberi hired lobbyists, retained public relations professionals, and made campaign contributions, which gave him access to U.S. officials.

U.S. v. Kaveh Afrasiabi: In January 2021, in the Eastern District of New York, Kaveh Lotfolah Afrasiabi was charged with acting and conspiring to act as an unregistered agent of the Government of the Islamic Republic of Iran, in violation of FARA. It is alleged that, since at least 2007 to the present, Afrasiabi has been secretly employed by the Iranian government and paid by Iranian diplomats assigned to the Permanent Mission of the Islamic Republic of Iran to the United Nations (IMUN) in New York City. Afrasiabi was paid approximately $265,000 in checks drawn on the IMUN's official bank accounts since 2007 and had received health insurance through the IMUN's employee health benefit plans since at least 2011. Over the course of his employment by the Iranian government, Afrasiabi lobbied a U.S. Congressman and the U.S. Department of State to advocate for policies favorable to Iran, counseled Iranian diplomats concerning U.S. foreign policy, made television appearances to advocate for the Iranian government's views on world events, and authored articles and opinion pieces espousing the Iranian government's position on various matters of foreign policy. Afrasiabi had long known that FARA requires agents of foreign principals to register with DOJ and had discussed information obtained from FARA disclosures with others.

U.S. v. Alexander Ma: In August 2020, in the District of Hawaii, a criminal complaint was unsealed charging Alexander Yuk Ching Ma with conspiracy to communicate classified national defense information to intelligence officials of the People's Republic of China (PRC). According to court documents: Ma, a naturalized U.S. citizen born in Hong Kong, was a CIA intelligence officer from 1982 to 1989, maintained a Top Secret clearance, and signed numerous non-disclosure agreements. After Ma left the CIA, he lived and worked in Shanghai, PRC, before arriving in Hawaii in 2001. Ma and one of his relatives – who also is a former CIA officer – conspired with each other and with multiple PRC intelligence officials to communicate classified national defense information over the course of a decade. The scheme began in Hong Kong in March 2001, when the two former CIA officers provided information to the PRC intelligence service about the CIA's personnel, operations, and methods of concealing communications. Part of the meeting was captured on videotape, including a portion where Ma can be seen receiving and counting $50,000 in cash for the information they provided. Court documents further allege that after Ma moved to Hawaii, he sought employment with the FBI in order to once again gain access to classified U.S. government information, which he could in turn provide to his PRC handlers. In 2004, the FBI's Honolulu Field Office hired Ma as a contract linguist tasked with reviewing and translating Chinese-language documents. Over the following six years, Ma regularly copied, photographed, and stole documents that displayed U.S. classification markings. Ma took some of the stolen documents and images with him on his frequent trips to China with the intent to provide them to his handlers. Ma often returned from China with thousands of dollars in cash and expensive gifts. In spring 2019, over the course of two in-person meetings, Ma confirmed his espionage activities to an FBI undercover employee Ma believed was a representative of the PRC intelligence service. Ma also offered to once again work for the PRC intelligence service. In August 2020, during a meeting with an FBI undercover employee, Ma accepted money for his past espionage activities, expressed his willingness to continue to help the Chinese government, and stated that he wanted the Chinese "motherland" to succeed.

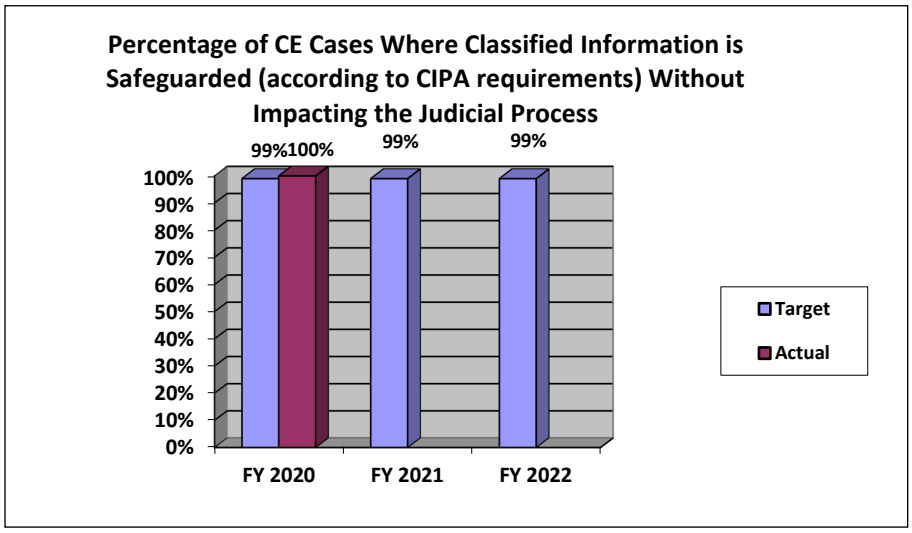
U.S. v. Mariam Thompson: In March 2020, in the District of Columbia, DOD linguist Mariam Taha Thompson was charged with transmitting highly sensitive national defense information

(NDI) to a foreign national with apparent connections to Hizballah, a designated foreign terrorist organization. In March 2021, Thompson pled guilty to committing espionage. According to court documents, the information Thompson gathered and transmitted included classified NDI regarding active human assets, including their true names. Thompson was arrested by FBI Special Agents on February 27, 2020, at an overseas U.S. military facility, where she worked as a contract linguist and held a Top Secret security clearance. The investigation leading to Thompson's arrest revealed that starting on or about December 30, 2019, a day after U.S. airstrikes against Iranian-backed forces in Iraq, and the same day protesters stormed the U.S. Embassy in Iraq to protest those strikes, audit logs showed a notable shift in Thompson's network activity on DOD classified systems, including repeated access to classified information she had no need to access. Specifically, between December 30, 2019, and February 10, 2020, Thompson accessed dozens of files concerning human intelligence sources, including true names, personal identification data, background information, and photographs of the human assets, as well as operational cables detailing information the assets provided to the U.S. Government. A court-authorized search of Thompson's living quarters on February 19, 2020, led to the discovery of a handwritten note in Arabic concealed under Thompson's mattress. The note contained classified information from DOD computer systems, identifying human assets by name, and warning a DOD target affiliated with a designated foreign terrorist organization with ties to Hizballah. The note also instructed that the human assets' phones should be monitored. The investigation revealed Thompson transmitted the classified information in the handwritten note to a co-conspirator, in whom she had a romantic interest, and that Thompson knew the co-conspirator was a foreign national whose relative worked for the Lebanese Government. The investigation also revealed that the co-conspirator has apparent connections to Hizballah. In a separate communication, Thompson also provided information to her co-conspirator identifying another human asset and the information the asset had provided to the U.S., as well as providing information regarding the techniques the human assets were using to gather information.

U.S. v. Henry Kyle Frese: In June 2020, in the Eastern District of Virginia, Henry Kyle Frese, a former employee of the Defense Intelligence Agency (DIA), was sentenced to 30 months in prison for leaking classified information. In February 2020, Frese pled guilty to willful transmission of classified U.S. national defense information (NDI) to two journalists. In October 2019, Frese was indicted on two counts related to his disclosure of classified NDI to two journalists in 2018 and 2019. Frese, of Alexandria, Virginia, was a DIA counterterrorism analyst holding a Top Secret security clearance. According to court documents, between mid-April and early May 2018, Frese accessed classified intelligence reports, some of which were unrelated to his job duties, and provided Top Secret information regarding a foreign country's weapons systems to a journalist ("Journalist 1"). Based on Frese's and Journalist 1's public social media pages, it appears they were involved in a romantic relationship for some or all of that time period. A week after Frese accessed an intelligence report ("Intelligence Report 1") in April 2018, Journalist 1 wrote to Frese and asked whether he would be willing to speak with another journalist ("Journalist 2"). Frese stated that he was "down" to help Journalist 2 if it helped Journalist 1 because he wanted to see Journalist 1 "progress." In the hours after searching for terms related to the topic of Intelligence Report 1, Frese spoke by telephone with both Journalist 1 and Journalist 2, and within approximately a half-hour after Frese's conversations with the two journalists, Journalist 1 published an article that contained NDI from Intelligence Report 1, classified at the Top Secret level.

Measure: **Percentage of CE Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2020 Target: 99%
FY 2020 Actual: 100%
FY 2021 Target: 99%
FY 2022 Target 99%

Discussion: The FY 2022 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.

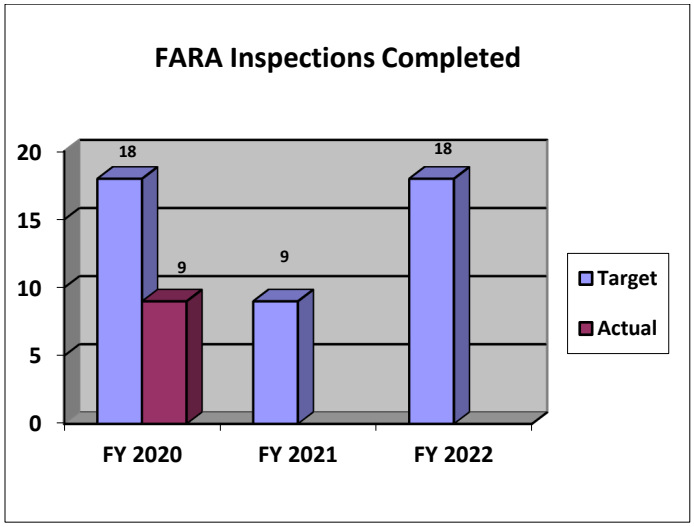


Data Definition: Classified Information - information that has been determined by the United State Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data as defined by the 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 2020 Target: 18
FY 2020 Actual: 9
FY 2021 Target: 9
FY 2022 Target: 18

Discussion: FY 2022 – The FY 2022 target is consistent with fiscal years 2020 and prior. FY 2021 – The FY 2021 target has been decreased because FARA inspections involve sending a team of DOJ employees to an outside office to meet with and talk to countless employees. It is anticipated that the COVID-19 pandemic-related restrictions will inhibit NSD's ability to restart inspections until FY 2022. FY 2020 – The target was missed due to the COVID-19 pandemic.

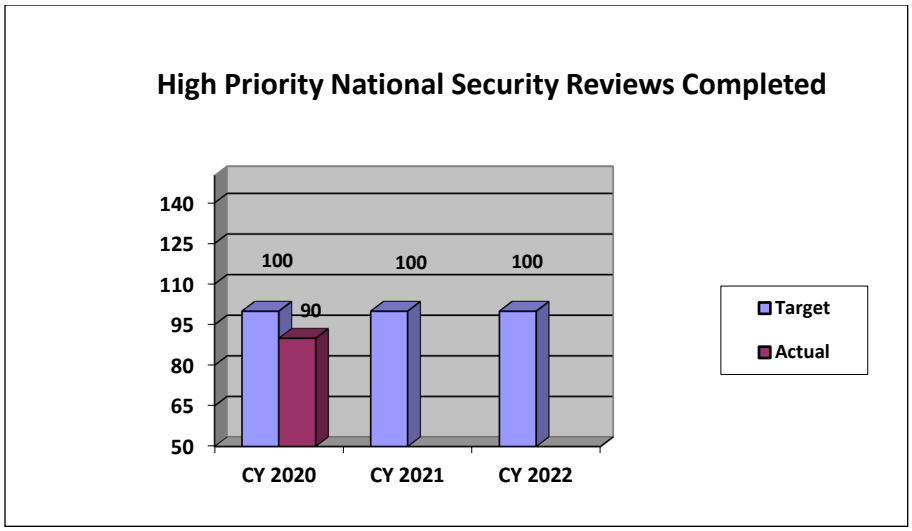
Performing targeted inspections allows the FARA Unit to more effectively enforce compliance among registrants under FARA.



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 2020 Target: **100**
CY 2020 Actual: **90**
CY 2021 Target: **100**
CY 2022 Target: **100**

Discussion: CY 2022 - The CY target is consistent with previous fiscal years. To address potential national security concerns with foreign investment, NSD will continue to work with its partners to perform these high priority reviews. CY 2020 – The CY 2020 target was incorrectly reported as 122 previously; the correct target is 100. In addition, the target was missed due to the COVID-19 pandemic.



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 that result in a mitigation agreement to which DOJ is a signatory;
4. Mitigation monitoring site visits;
5. 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; and
6. 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.

VI. Program Increases by Item

I. Intelligence Collection and Oversight

Budget Decision Unit(s): National Security Division

Organizational Program: Office of Intelligence (OI)

Program Increase: Positions 13 Atty 10 FTE 7 Dollars $2,690,000

Description of Items

NSD's OI requests 13 positions, including 10 attorneys, 1 program specialist, and 2 legal administrative assistant positions for a total of $2,690,000. These positions are required to enable OI's Oversight Section to accomplish the extensive oversight and compliance work being handled by the Section and anticipated increases in the volume of oversight-related work that OI expects to be handling during FY 2022. The increase in oversight-related work that necessitates additional positions is described below.

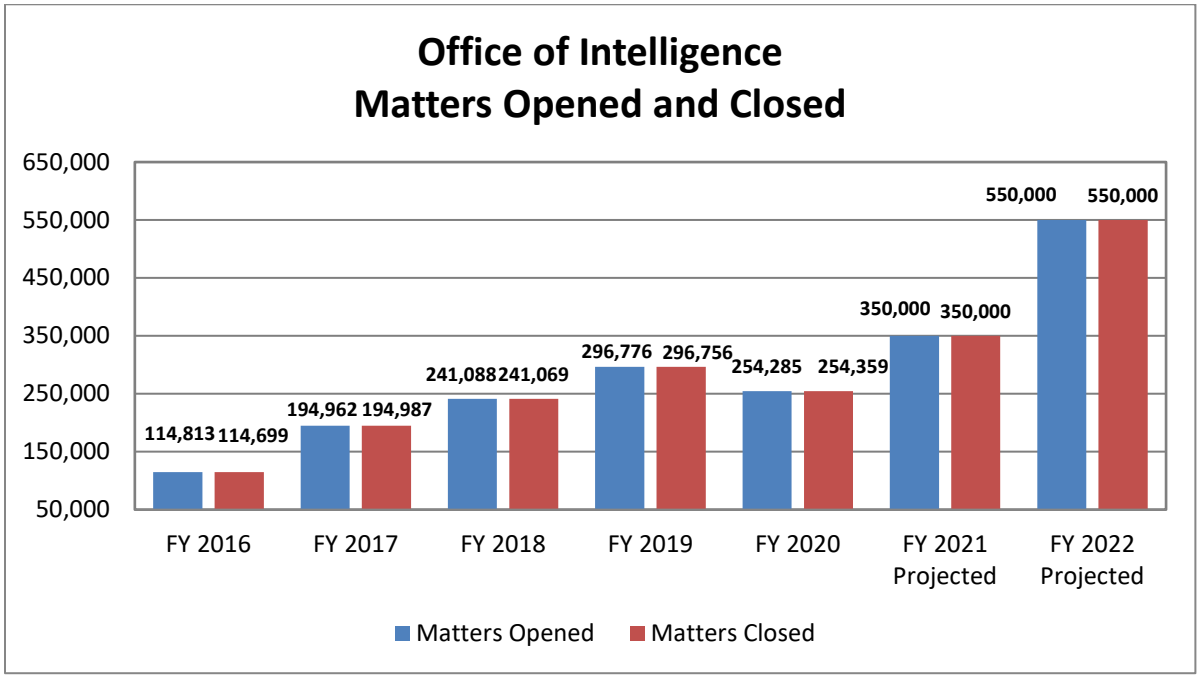
Justification

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) IC agencies have the legal authorities necessary to conduct intelligence operations, particularly operations involving FISA; 2) OI exercises substantial oversight of national security activities of IC agencies; and 3) OI plays an essential 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 and other national security authorities are used in compliance with the law, and facilitating appropriate use of FISA collection in criminal cases. OI conducts this work in an entirely classified setting, working on some of the most sensitive cases to the U.S. Government. OI works on the early stages of investigating serious matters of national security, often obtaining the initial legal authority to combat threats as diverse as international terrorism, cyber attacks by hostile foreign actors, and efforts by foreign actors to steal American technology. This work all directly supports 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.

Matters Handled

Over the last several years, OI's work has significantly grown in volume and complexity. Although there has been a decrease in the number of FISA applications handled by OI over the last several years, the number of oversight-related matters handled by OI has significantly increased during that same time period. As reflected in the below chart, between FY 2014 and FY 2019, OI experienced a roughly 250% increase in the number of matters handled, and, of particular note, a 70% increase between FY 2016 and FY 2017 alone. OI also saw an additional 24% increase between FY 2017 and FY 2018 and a 23% increase between FY 2018 and FY

2019. The vast majority of the matters opened and closed that are represented in the below chart reflect the resources dedicated to OI's oversight responsibilities. The number of FISA applications handled by OI is not included in the number of matters opened and closed and are separately measured by OI.[2] In addition to the work reflected in these numbers, which is quantifiable, OI also supports wide-ranging and complex matters that are not as quantifiable, such as development of IC agency FISA procedures, drafting complex analyses pertaining to questions of law, declassification reviews, reviews and comment on legislative proposals, document review and production to Congressional committees, responses to FOIA and other types of litigation, and regular reporting to Congress on the utilization of FISA authorities by the IC. Implementing and sustaining effective oversight of, and compliance with, FISA authorities requires IC agencies and DOJ to commit sufficient resources to accomplish the goal so that Congress, the courts, and the American people maintain faith that those authorities are used properly.



FISA Section 702

OI plays a primary role in implementing and overseeing Section 702 of FISA. Section 702 has been an important tool used to enhance U.S. national security and counter the threat of terrorism and cyberattacks. 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 five years and shows no signs of abating. Between CY 2014 and CY 2019, the number of Section 702 targets increased roughly 121% from 92,707 to 204,968. In the last three calendar years, OI also has also experienced steady increases in the number of potential Section 702 incidents reported by the IC. OI dedicates substantial resources to investigating each such

2 In addition to oversight-related responsibilities that are covered by the matters opened and closed in the chart above, some of the quantifiable work handled by OI's Litigation Section is included.

potential incident reported by the IC or otherwise identified by OI. OI also dedicates resources to ensure the IC properly remediates compliance incidents. OI must report the details of each Section 702 compliance incident to the FISC and to Congress. Between CY 2016 and CY 2019, the number of potential Section 702 incidents reported to OI increased 123%. All of these reported potential incidents required dedicated OI resources to investigate the potential incidents. OI expects that there will continue to be increases in such compliance investigations in 2021 and 2022. In addition, as part of its oversight of the IC's use of Section 702, OI dedicates substantial resources to auditing the IC's querying of unminimized information collected pursuant to Section 702. While OI has consistently dedicated a portion of its resources toward auditing such queries, the requested increase in attorney positions would allow a broader and more robust query oversight program.

In addition, OI expects that its oversight of the Section 702 program will significantly grow as the program expands to address the foreign intelligence priorities of the IC. By FY 2022, OI expects that it will need additional resources to address one of the aspects of the continued expansion of the program.

In short, to keep pace with the increasing oversight demands that the IC's utilization of Section 702 is placing on OI, this request includes an additional seven attorneys, one program specialist, and one administrative legal assistant.

FISA Application Accuracy and Other Oversight Initiatives

The FBI and OI have undertaken multiple corrective measures to ensure the accuracy and completeness of applications submitted to the FISC following the findings and recommendations of the Office of the Inspector General's (OIG) December 2019 Report, *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* (OIG Report). One aspect of OI's oversight of FBI's FISA applications submitted to the FISC includes the conduct of accuracy reviews to ensure that the facts contained in a FISA application are accurate. OI conducts multiple accuracy reviews each calendar year during oversight reviews at FBI field offices. In light of the findings of the OIG Report, OI has expanded the nature of its accuracy reviews, which will require additional resources to complete. For example, OI has expanded its oversight of FBI FISA applications to include completeness reviews, which are resource intensive reviews. These reviews will require additional human resources. In addition, reports will need to be generated following these reviews, including trends analyses. OI will also be required to compile additional reports to the FISC pursuant to related FISC Orders regarding OI's accuracy and completeness reviews, which will require additional resources to complete.

The oversight and compliance mission of OI is accomplished on multiple levels: training, modernization of FISA procedures, new and evolving compliance review programs, reports to Congressional oversight committees and the FISC, and compliance trends analysis. OI develops and presents detailed, effective training programs on the rules governing FISA. Those rules, too, must be updated regularly to keep pace with changes in technology and protocols at the applicable IC agencies. OI leads such efforts to update legal procedures. These efforts are currently underway and will require, with complementary training and the development of additional oversight programs to ensure compliance with these procedures, additional attorney and non-attorney resources.

Finally, OI's Oversight Section has been working with the Criminal Division to implement the Clarifying Lawful Overseas Use of Data (CLOUD) Act. The U.S. enacted the CLOUD Act to improve procedures for both foreign and U.S. investigators in obtaining access to electronic information held by service providers. Such information is critical to investigations of serious crime by authorities around the world, ranging from terrorism and violent crime to sexual exploitation of children and cybercrime. The CLOUD Act authorizes the U.S. Government to enter into executive agreements with foreign nations under which each country would remove any legal barriers that may otherwise prohibit compliance with qualifying court orders issued by the other country. As DOJ enters into international agreements with other foreign governments under the CLOUD Act, the Act and the agreements will require oversight of the implementation of the agreements. OI's Oversight Section has been designated to assist in conducting oversight under the agreement. Thus far, DOJ has negotiated an international agreement under the CLOUD Act with one foreign government. There will be additional future agreements. By FY 2022, OI will need additional resources to assist in oversight activities under this program.

For the above additional oversight programs, OI will need three additional attorneys and one additional administrative.

Impact on Performance

These requested positions 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. Without these additional resources, NSD will not have sufficient staff to address the increase in workload outlined above and 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

1. Base Funding

FY 2020 Enacted				FY 2021 Enacted				FY 2022 Current Services			
Pos	Atty	FTE	Amount ($000)	Pos	Atty	FTE	Amount ($000)	Pos	Atty	FTE	Amount ($000)
136	108	120	$38,890	138	109	121	$40,579	138	109	122	$41,384

2. Personnel Increase Cost Summary

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2022 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Program Specialist (0300-0399)	1	$143	$55	$232	$143	$55	$1
Attorneys (0905)	10	$228	$43	$348	$2,248	$425	($1)
Legal Admin. Assistant (0300-0399)	2	$131	$62	$208	$263	$124	$9
Total Personnel	**13**	**$503**	**$160**	**$789**	**$2,690**	**$605**	**$12**

3. Non-Personnel Increase Cost Summary

Non-Personnel Item	FY 2022 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Not Applicable	$0	$0	0	$0	$0
Total Non-Personnel	**$0**	**$0**	**0**	**$0**	**$0**

4. Justification for Non-Personnel Annualizations: N/A

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Atty	FTE	Personnel	Non-Personnel	Total	FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Current Services	138	109	122	$41,384		$41,384		
Increases	13	10	7	$2,690		$2,690	605	12
Grand Total	**151**	**119**	**129**	**$44,074**		**$44,074**	**$605**	**12**

6. Affected Crosscuts

National Security Division

VI. Program Offsets by Item (Not Applicable)

VII. EXHIBITS