FY 2023
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 and directly supports the Department of Justice's (DOJ) top funding priority, Keeping our Country Safe. NSD requests for Fiscal Year (FY) 2023 a total of 434 positions (including 292 attorneys), 364 FTE, and $133,512,000.[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.

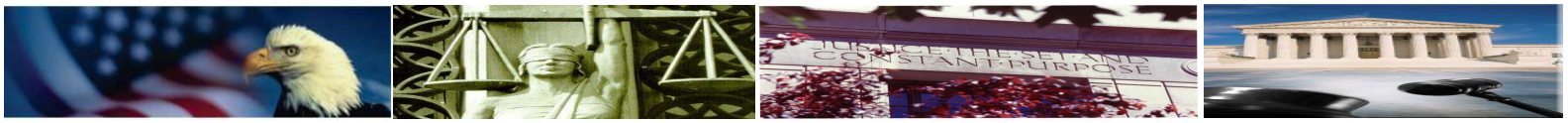
2. Division Structure.

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 offices and sections:

- Counterintelligence and Export Control Section (CES);
- Counterterrorism Section (CTS);

[1] Within the totals outlined above, NSD has included a total of 26 positions, 26 FTE, and $19,302,000 for Information Technology (IT).



- Foreign Investment Review Section (FIRS);
- 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;

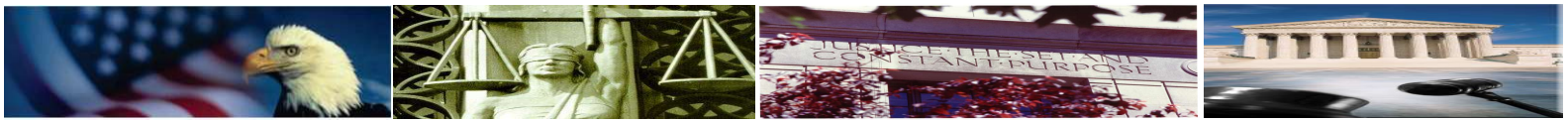
- Coordinating with interagency partners the use of all tools to protect our national assets, including use of law enforcement tools, economic sanctions, and diplomatic solutions; and

- 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.

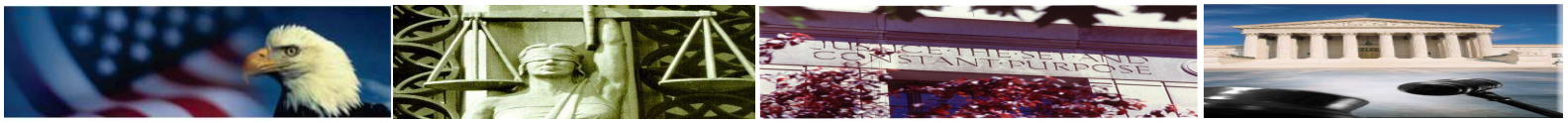
3. Foreign Investment.

- 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 National Security Council (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;

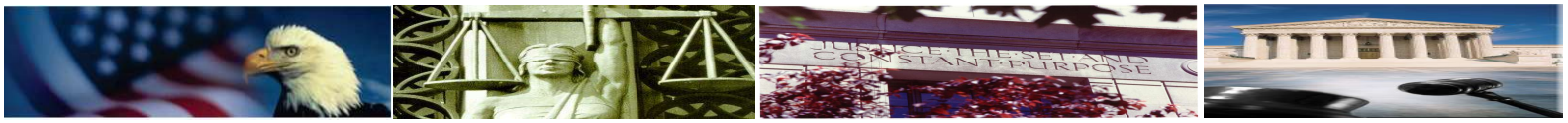
- Coordinating and supervising intelligence-related litigation matters, including the evaluation and review of requests to use information collected under FISA in criminal and non-criminal proceedings; and

- 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;

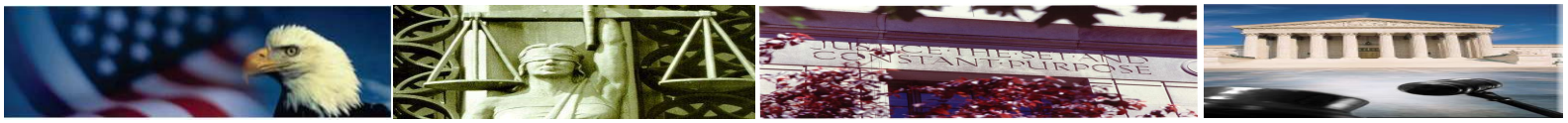
- Providing legal assistance and advice on matters arising under national security laws and policies, and overseeing the development, coordination, and implementation of DOJ-wide policies with regard to intelligence, counterintelligence, counterterrorism, and other national security matters;

- 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 NSC.

D. Recent Accomplishments (UNCLASSIFIED only).

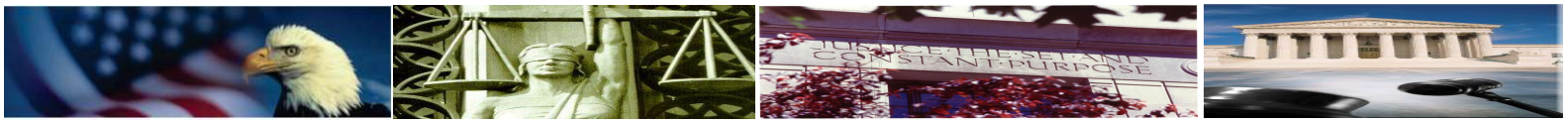
- **Evolving Threat of Terrorism.** In 2020 and 2021, DOJ charged more than 300 individuals for foreign fighter, domestic terrorism and domestic violent extremism-related, and international terrorism-related conduct. These cases include, among others, individuals inspired by ISIS to plot violent acts in the U.S., but who 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 of an individual for the hostage taking of four Americans in Syria;
  - Conviction and 25-year sentence for an individual who plotted to carry out a bomb attack at a political rally in California;
  - Conviction for an ISIS supporter who created a computer program designed to make sharing ISIS propaganda easier online;
  - Conviction for an individual who attempted to travel to Afghanistan to join the Taliban and fight against American service members;
  - Conviction of an individual who attempted to purchase a chemical weapon through the Dark Web;
  - Conviction of an ISIS leader wo controlled the terror group's English propaganda efforts;
  - Conviction for an individual who purposely wrecked a train at a rail yard in California;
  - Conviction and 15-year sentence for an individual who published bomb making instructions and advocated for violence against Americans; and
  - Conviction and 20-year sentence for an individual who attempted to sell ghost guns to a terrorist group.
- **January 6 – Capitol Riot Investigation.** In connection to the breach of the U.S. Capitol on January 6, 2021, about 165 individuals have pleaded guilty to a variety of federal charges, from misdemeanors to felony obstruction, many of whom will face incarceration at sentencing (as of January 6, 2022).

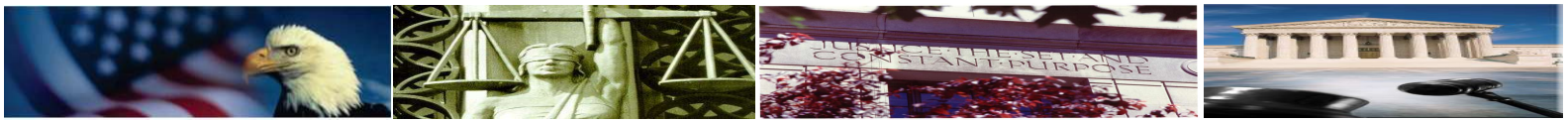
- **Espionage Enforcement.** NSD continued its enforcement of the Espionage Act and Economic Espionage Act by successfully prosecuting defendants for espionage offenses. Recent case examples include:
  - In April 2021, Xiaorong You was convicted in the Eastern District of Tennessee after trial for economic espionage related to "BPA-free" coatings, as part of a plan to set up a competing business in China;
  - In May 2021, Peter Debbins, who earlier pled guilty in the Eastern District of Virginia for conspiring to commit espionage, was sentenced to a prison term of 188 months;
  - In June 2021, Mariam Taha Thompson was sentenced in the District of Columbia to 23 years in prison for delivering classified national defense information to aid a foreign government;
  - In February 2022, Jonathan Toebbe and Diana Toebbe pleaded guilty in the Northern District of West Virginia to violating the Atomic Energy Act by selling Restricted Data concerning the design of nuclear-powered warships.
- **Combatting Malign Foreign Influence.** NSD significantly increased its efforts to combat malign foreign influence, primarily through FARA enforcement and improved transparency. The number of new registrants and new foreign principals under FARA more than doubled from 2016 through 2019. 2021 saw the second highest level of new registrants since 2016 and



the highest overall number of active registrants since 2016, with a 67% increase in active registrants from the 2016 figure. The FARA Unit also conducted 23 inspections of current registrants, surpassing its pre-pandemic record of 20 inspections in a calendar year. Recent case examples include:

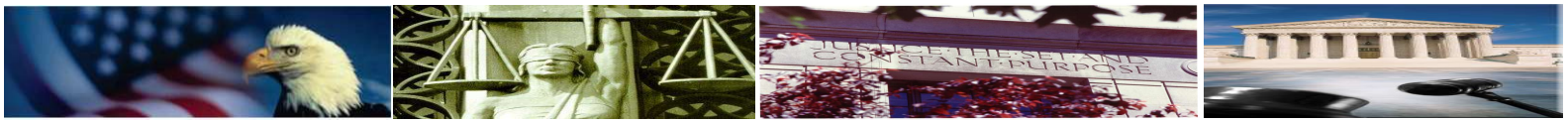
- In December 2021, Maffick LLC registered as an agent of Russian state-owned media entity ANO TV-Novosti. The registration was an example of the FARA Unit's use of its civil tools to enforce compliance with the Act. Another example was the May 2021, Xinhua News Agency North America has registered as the U.S. agent of PRC-based Xinhua News Agency. Recent NSD enforcement efforts have also resulted in the registrations of multiple other 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.
- In July 2021, NSD obtained criminal charges, including violations of 18 U.S.C. § 951, against Thomas Barrack, Matthew Grimes, and Rashid Sultan Rashid Al Malik Alshahhi for their alleged efforts to advance the interests of the United Arab Emirates (UAE) in the United States at the direction of senior UAE officials by influencing the foreign policy positions of a 2016 presidential campaign and, subsequently, the foreign policy positions of the U.S. government in the incoming administration, as well as seeking to influence public opinion in favor of UAE interests.
- 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;
- 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.

- **Export Controls and Sanctions Enforcement.** NSD continued its rigorous enforcement of export controls and sanctions, including sanctions against Iran, China, and North Korea. Recent case examples include:
  - 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;
  - In April 2021, in the District of Massachusetts, Shuren Qin pled guilty to illegally procuring and exporting U.S.-origin goods to Northwestern Polytechnical University in the People's Republic of China, which is heavily involved in military research;

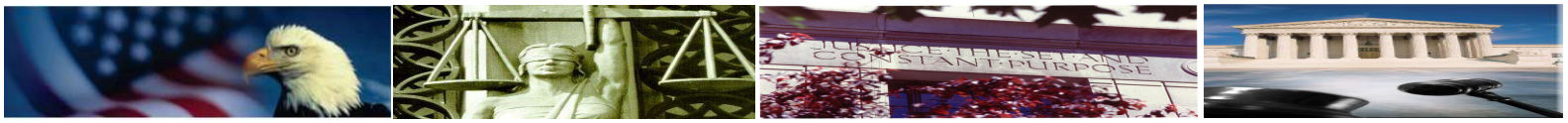


- In April 2021, NSD and the USAO for the District of Massachusetts entered into a Non-Prosecution Agreement (NPA) with SAP SE. SAP voluntarily disclosed its illegal downloads and services to Iran pursuant to NSD's voluntary disclosure policy. SAP paid $5.14 million as part of the NPA;
- In September 2021, in the District of Columbia, Marc Baier, Ryan Adams, and Daniel Gericke entered into a deferred prosecution agreement restricting their future employment and requiring the payment of $1,685,000 in penalties to resolve an investigation regarding violations of U.S. export control, computer fraud, and access device fraud 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 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. The Department also seized several million dollars of stolen cryptocurrency.
  - On March 2, 2021, multiple U.S. technology and cybersecurity companies, including Microsoft, publicly disclosed multiple previously unknown vulnerabilities targeting computers using Microsoft Exchange Server software. Microsoft publicly advised that the vulnerabilities were being exploited by Chinese state actors, which Microsoft referred to as "HAFNIUM." On April 12, 2021, NSD and the USAO for the Southern District of Texas utilized a search warrant to copy and remove hundreds of malicious web shells that these actors had deployed on U.S. victim networks through the compromise Exchange Server software.
  - In May 2021, Colonial Pipeline was the victim of a highly publicized ransomware attack resulting in the company taking portions of its fuel pipelines (*i.e.*, critical infrastructure) out of operation, thereby causing gasoline shortages along the Eastern United States. Colonial Pipeline reported that its business-side computer network had been accessed by a group named "DarkSide," and that the company had received and paid a $4.4 million ransom demand in bitcoin. On June 7, 2021, NSD, the USAO for the Northern District of California, and the Criminal Division announced the seizure of the vast majority of the ransom bitcoin from at least one actor affiliated with DarkSide.
- **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 April 2021, Daniel Everett Hale pled guilty in the Eastern District of Virginia to making unauthorized disclosures to a member of the media; he later was sentenced to 45 months in prison.



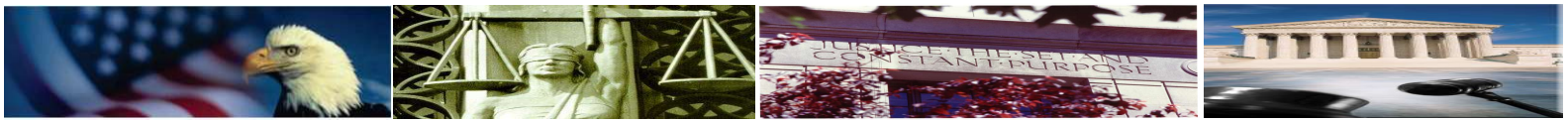
- **Foreign Investment Review.** NSD's robust engagement in foreign-investment review supports DOJ's Strategy for Countering Nation-State Threats as well as NSD's general responsibilities to enhance national security and counter foreign adversaries trying to steal, spy on, and sabotage key U.S. assets and technology.
    - Despite an expected decrease in transactions subject to CFIUS review during the global COVID-19 pandemic, NSD instead reviewed approximately 28% more submissions overall in 2021 than the previous year regarding mergers, acquisitions, and investments;
    - NSD led (on behalf of DOJ) approximately 25% of the cases in which a Joint Voluntary Notice was filed with CFIUS in 2021, which was approximately 42% higher overall number of cases than the previous year. In approximately 50% of those cases, the transaction was prohibited, abandoned, or mitigated (or anticipated to require prohibition or mitigation, for pending cases), based on national security risks identified by NSD;
    - NSD also led (on behalf of DOJ) approximately 24% (up from 15% the prior year) 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 119% 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 2019–2020;
    - NSD represents the Attorney General in his 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-day implementation period after Executive Order 13913 was signed in 2020, in its 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 reviewed 4% more applications in 2021 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 2021; and
        - Team Telecom recommended in 2021 to the FCC that 11 of the reviewed applications (stemming from 41 applications the FCC referred that involved a total of 84 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.
    - Following the June 2020 recommendation to partially deny a submarine cable landing license application filed with the FCC by applicants seeking to connect the Pacific Light Cable Network cable system, the applicants subsequently withdrew the application and filed a new application that sought to address the Executive Branch's national security and law enforcement concerns., Months of dialogue and negotiations culminated in November 2021 when Team Telecom recommended to the FCC that the application be granted contingent on the applicants' agreeing to certain standard and non-standard mitigation measures.
    - NSD also led the Executive Branch's participation in the FCC's Show Cause proceedings against China Telecom (Americas) Corp., the U.S. subsidiary of a People's Republic of China (PRC) state-owned telecommunications company, and in January 2021 filed Team



Telecom's Response to the FCC's Order Instituting Proceedings on Revocation and Termination, recommending to the FCC, based on insurmountable national security and law enforcement concerns, that the FCC revoke and terminate the license.

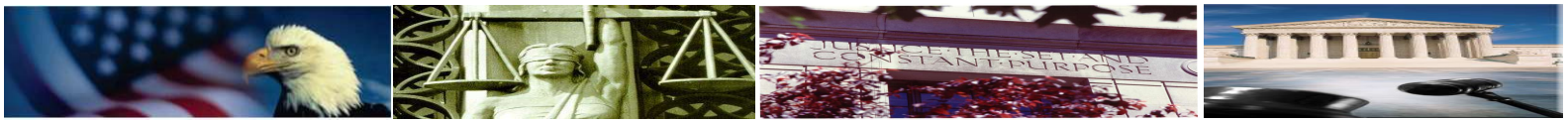
- NSD provided significant assistance to the Department of Commerce in administering its regulations pursuant to Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," which were published in 2020 and implement the Secretary of Commerce's new authority 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 2021 NSD submitted one referral to the Secretary of Commerce, and thus far remains the only U.S. government entity to make a referral pursuant to this new authority.

- **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. The FCC followed this rulemaking with another NPRM which led to the FCC adopting a Second Report & Order on Process Reform for Executive Branch Reviews – Adopting Standard Questions. NSD was instrumental in shaping the resulting FCC rules.
- **Efforts in CFIUS and Team Telecom Cases.** NSD led eight CFIUS cases and 59 Team Telecom cases in 2021 that resulted in 38 new national security agreements that NSD negotiated and entered with companies, and that NSD will monitor for compliance going forward. The total number of such agreements monitored by NSD is currently approximately 185, which reflects an approximate 63% increase in mitigation agreements from the previous year. This significant increase in the total number of active agreements occurred despite terminating 10 agreements in 2021 as part of NSD's ongoing initiative to reassess all lower-risk mitigation agreements and end ones that were no longer necessary. NSD also conducted approximately 12 in-person or virtual mitigation compliance site visits in 2021 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 calendar year (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 IC components. NSD plays a critical role ensuring that the FISC and Congress remain apprised of NSD's oversight findings and fully understands the steps being taken to remedy and prevent such instances of noncompliance. 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



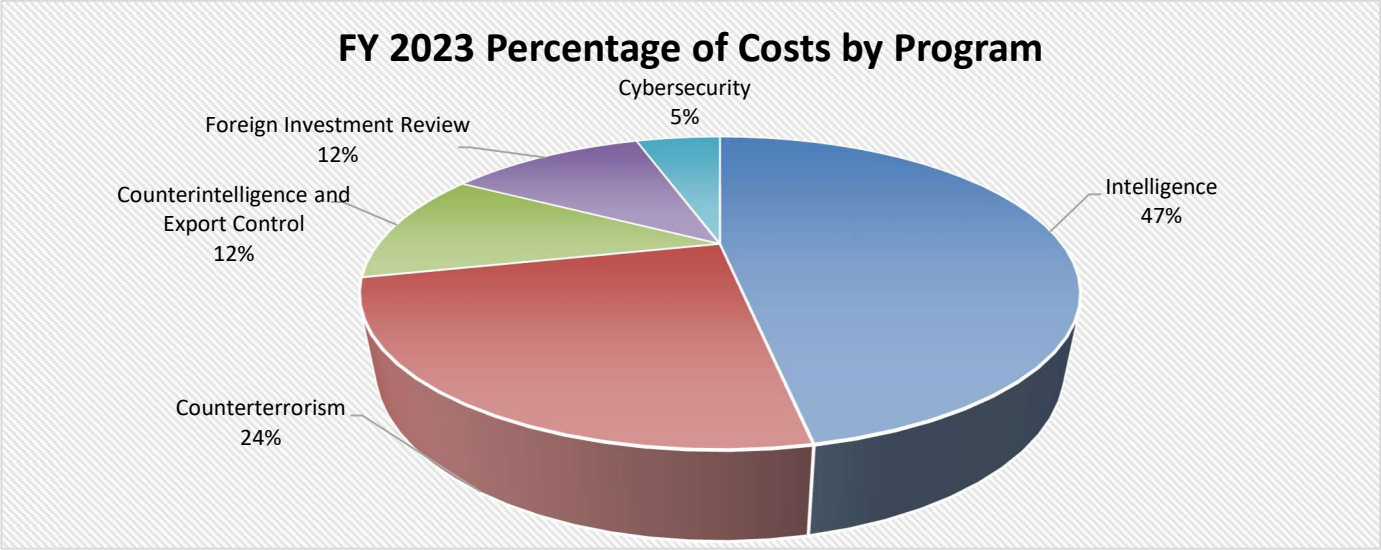
compliance with acquisition, retention and/or dissemination requirements of Section 702 authorities. If not for the COVID-19 pandemic, CY 2020 was on pace to exceed the workload completed in CY 2019. CY 2021 saw an overall return to pre-COVID levels of workload, and NSD anticipates the historic workload increase to continue through CY 2022.

- **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 its oversight reviews of FBI FISA applications, which have required additional resources to complete. For example, NSD has expanded its oversight of FBI FISA applications to include completeness reviews in addition to the existing accuracy reviews. The completeness reviews 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. The reviews have continued in CY 2022.
- **Enhanced Focus on Query Reviews.** NSD's oversight of the use of FISA-acquired information includes ensuring that query restrictions found in standard minimization and query procedures are followed. In CY 2018, CY 2019, CY 2020, and CY 2021, NSD identified a number of query-related compliance issues at a particular agency. As a part of its response to addressing these compliance issues, NSD has broadened the scope of its query reviews and worked closely with the applicable IC agency to address the issues implicated. These efforts have, and will continue to, consume significant resources.
- **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 - 2022, 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 Bangladesh, Belgium, France, Germany, Indonesia, Israel, Kenya, New Zealand, Pakistan and the United Kingdom.
- **Providing Training to International Partners.** In FY 2020 - 2022, OVT provided virtual training about its mission and terrorism victims' rights and access to justice to partners in Cameroon, Burkina Faso, and the European Commission's Network of EU single contact points for victims of terrorism.
- **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.



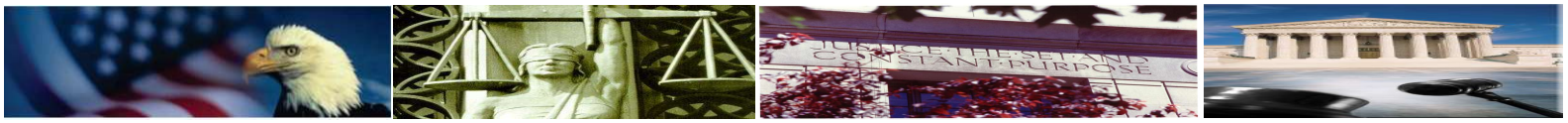
F. Performance Challenges.

1. Increasing and Changing Threats to U.S. National Assets, Including Significant Cyber Threat Growth.

Protection of national assets through counterintelligence investigations and prosecutions, enforcement of export controls and sanctions, and cyber-related investigations and prosecutions

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.

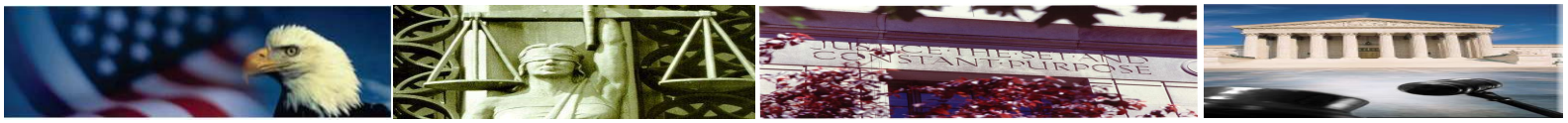
Also, among the most significant challenges that NSD continues to face is the rapid expansion, evolution, and sophistication of cyber threats to the national security. NSD must be prepared to continue to take lessons learned over the past decade and adapt them to this new threat. Highly technical cyber 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.

Recently, ransomware attacks, including the May 2021 attack on Colonial Pipeline, underscore the growing threat that ransomware and digital extortion pose to the Nation, and the destructive and devastating consequences ransomware attacks can have on national and economic security. NSD plays a critical role, along with other Department components, in identifying those who engage in these schemes and in developing lawful options to disrupt and dismantle the infrastructure, networks, and foreign safe havens used to carry out these attacks. Accordingly, NSD will be expected to adequately resource the Department's counter ransomware efforts, and to bring its unique authorities and expertise to bear, through the recently launched Ransomware and Digital Extortion Task Force.

Foreign Investment Review

NSD's foreign-investment review work has also expanded to address the asymmetric threat. This work, handled through NSD's Foreign Investment Review Section (FIRS), includes the following primary lines of effort:

(1) reviewing and resolving national-security risks posed by foreign transactions and investments in matters before the Committee on Foreign Investment in the United States (CFIUS);
(2) reviewing and resolving, through the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector (known informally as Team Telecom), national-security and law-enforcement risks posed by foreign entities' licenses and applications to provide telecommunications services in matters before the Federal Communications Commission;
(3) monitoring national security agreements for compliance (including conducting physical and virtual site visits) and initiating enforcement actions when necessary and appropriate; and
(4) reviewing transactions of information and communications technology and services (ICTS) that are designed, developed, manufactured, or supplied by entities connected to foreign adversaries and referring those that pose undue or unacceptable risks to U.S. national security to the Department of Commerce for action under Executive Order 13873.



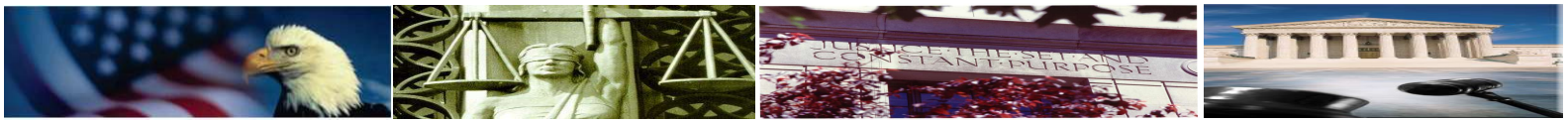
Each of these lines of effort has continued to significantly expand in volume and complexity. First, with respect to NSD's CFIUS work, the volume of filings before CFIUS has continued to increase dramatically over the years. In CY2021, overall NSD reviewed approximately 28% more submissions than in 2020 regarding mergers, acquisitions, and investments. In 2021, NSD (on behalf of DOJ) led approximately 25% of CFIUS cases in which a Joint Voluntary Notice was filed, and of those cases led by NSD, approximately 50% 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 24% (up from 16% in 2020) 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.

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 continue to 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 to which DOJ is a party, approximately 25% of which represent an agreement associated with a CFIUS transaction.

Second, with respect to NSD's Team Telecom work, in addition to exercising the Attorney General's role as the Chair under Executive Order 13913, NSD also led or co-led all of the group's reviews in 2021. Of the 67 FCC referrals of applications in 2021 (that involved a total of 84 completed telecommunications authorizations, cable landing licenses, and petitions for declaratory ruling), Team Telecom recommended to the FCC that 59 of the total authorizations, licenses, and petitions for declaratory be granted contingent on mitigation measures. NSD also monitors compliance with all mitigation agreements (approximately 185 and growing) to which DOJ is a party, approximately 73% of which represent an agreement associated with a Team Telecom application.

Third, 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 2021 NSD was successful in terminating approximately 10 mitigation agreements that were no longer necessary). Of the CFIUS and Team Telecom cases discussed above, 8 new CFIUS cases and 30 new Team Telecom cases led or co-led by NSD in 2021 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; for example, approximately 4% of the cases that DOJ co-led in 2020 were brought before CFIUS by DOJ as non-notified transactions.

Fourth, since the President signed Executive Order 13873 in May 2019 to secure the ICTS supply chain, NSD (FIRS) has been actively involved in helping the Department of Commerce draft regulations to implement this new authority and continues to assist the Department of Commerce



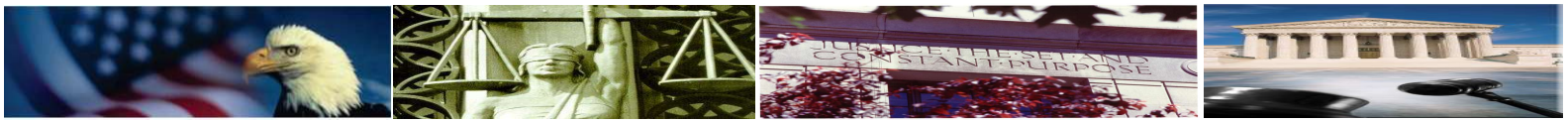
administer its ICTS Supply Chain risk management regulatory process. In 2021, NSD submitted one referral to the Department of Commerce under the new authority—bringing the total number of interagency referrals to three. All three interagency referrals have been investigated, drafted, and submitted by NSD (FIRS).

In addition to these quantitative expansions in its caseload, NSD's foreign-investment work has also continued to grow qualitatively in complexity and breadth. NSD 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 in CFIUS performs this integrated function. In particular, since the passage of FIRRMA, NSD has 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.

Similarly, with respect to Team Telecom, complex transactions and differences in evaluative priorities among agencies prompted the Executive Order 13913, which formalized this process with stricter timelines, an administrative chair, and other indicia of a structured interagency process. NSD represents DOJ in exercising the Attorney General's role as chair of this committee, which is proving crucial to securing the nation against digital communications threats introduced via the U.S. telecommunications infrastructure. NSD has had increased responsibilities in effecting this change and has been responsible for developing legal and operational guidance to govern Team Telecom.

Despite the high-volume, expanding, and complex nature of NSD's foreign-investment work, the critical role that this work plays in protecting U.S. assets from national-security and law-enforcement risks, and the importance of this work in countering foreign adversaries trying to use our supply chains to steal, spy, and sabotage, NSD's personnel and IT resources have not kept pace with the expansion of its mission. NSD (FIRS) currently relies on manually inputting and tracking all cases and data, resulting in significant inefficiencies and diverting resources from its substantive work to protect national security. To meet this challenge, NSD (FIRS) is actively pursuing the acquisition of a modern, dynamic case-management system to track its national-security reviews, analyze trends, and identify strategic priorities and gaps.

Finally, NSD's foreign-investment work also faces external challenges. Changes in the global economic environment could reduce international business activity and telecommunications investments in the United States and thus reduce the number of cases within the federal government's jurisdiction. In particular, a consistent government policy of denying foreign adversaries access to U.S. intellectual property and telecommunications networks, or otherwise restricting foreign investment in the United States, could prompt companies to shift transactions and investments to unregulated forms outside the federal government's jurisdiction or less regulated forms (such as contracting or licensing arrangements) or to less overt channels (such as espionage). In addition, the lack of a federal privacy and data-protection framework has led the private sector to increasingly rely on other jurisdictions for de facto industry standards (such as state privacy laws and foreign laws such as the European Union's General Data Protection Regulation). This disaggregated patchwork makes it more difficult to negotiate appropriate measures to mitigate risks to national security and law enforcement.



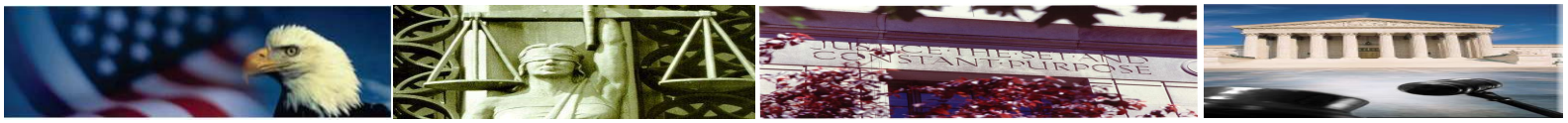
2. Increasing Workload in Intelligence Oversight, Operations, and Litigation.

NSD's intelligence-related work fully supports the U.S. Government's national security mission, including combating the threats posed by terrorists, threats to 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 and performs the following functions: 1) OI ensures that 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. NSD plays a primary role in implementing and overseeing Section 702 of FISA. Over the last several years, NSD has experienced a significant growth in the volume and complexity of the work related to Section 702. 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 growth in the coming years.

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. While the number of targeting decisions remains classified, the Government reported in the 21st Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of FISA, covering the period of June – November 2018: "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 number of targets reported for CY 2020 was just below the number of targets reported for CY 2019; this slight decrease was likely due to the COVID-19 pandemic, and NSD anticipates that the upward trend will resume in CY2022. The substantial growth of NSD's Section 702 oversight program and the resulting impact on NSD's resources is also apparent from the over 400%[2] increase in the number of matters handled by OI, the NSD component that oversees this program, between FY 2014 and FY 2021. In addition, OI also has 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

2 A part of this increase is attributable to OI accounting for certain matters not previously included in workload reporting.



ensure the IC properly remediates compliance incidents. OI must report the details of each Section 702 compliance incident to the FISC and to Congress. While the number of potential incidents reported fell in CY 2020, this number returned to pre-pandemic levels by the end of 2021 and OI expects that the yearly increases in such compliance investigations by OI will continue in 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.

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 expanded its oversight of FBI FISA applications to include completeness reviews and conducted completeness reviews of 130 FISA applications between May 2020 and January 2022. These resource-intensive 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.

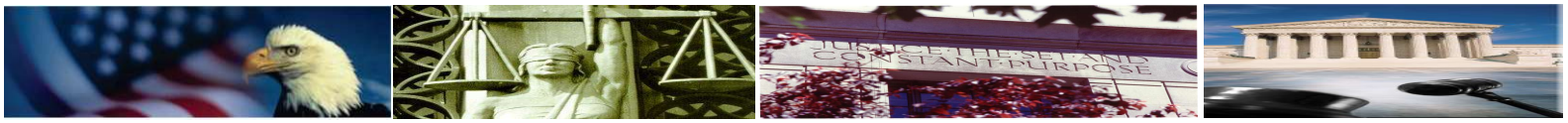
NSD expects to see continued growth in the area of use and litigation relating to traditional FISA and Section 702 information. There have been several high-profile litigation matters during the past year, including some involving individuals indicted for terrorism-related charges. The Government has 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 USAOs that requires reporting of all domestic



terrorism cases to NSD. In addition, the directive grants NSD additional oversight of these cases. Relatedly, in January 2022, NSD announced the formation of a domestic terrorism unit, within the Counterterrorism Section, to further ensure national-level coordination and tracking of all domestic terrorism cases. These additional responsibilities come with increased administrative burdens to effectively track, analyze, and report on data related to the growing domestic terrorism threat.

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. In recent months, ISIS fighters, taking advantage of unstable conditions in the region, particularly in refugee camps, have made some advances and shown signs of resurgence.

NSD is participating in and assisting USAOs with several prosecutions of U.S. citizens and high-level ISIS fighters who have been repatriated from the custody of the Syrian Democratic Forces.

Beyond Syria and Iraq, ongoing conflicts in other parts of the world, including Afghanistan, the Horn of Africa, and Lebanon, have presented opportunities for terrorist groups to find safe havens, attract travelers wishing to join their ranks, and continue to inspire homegrown violent extremists. NSD has seen an uptick in cases involving Americans expressing a desire to travel overseas and join various terrorist groups or to carry out plots in the homeland.

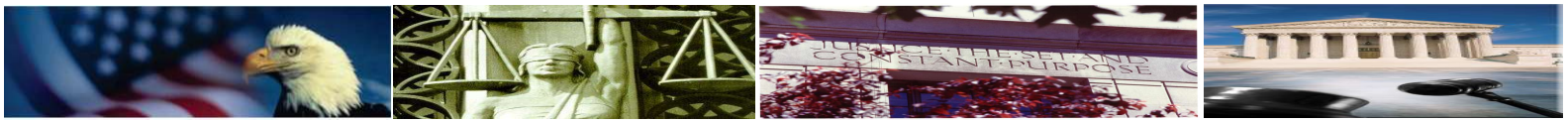
NSD and the IC predict a continued threat of self-radicalized individuals engaging in terrorist attacks on government and civilian targets in the U.S. Online radicalization is a particular problem as terrorists and other criminals increasingly use technology, including encryption, to conceal their crimes 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 to build their capacity to prosecute terrorism offenses, including those committed by repatriated foreign fighters. Over the last year, NSD has detailed multiple attorneys overseas to work with partner countries on these efforts.

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



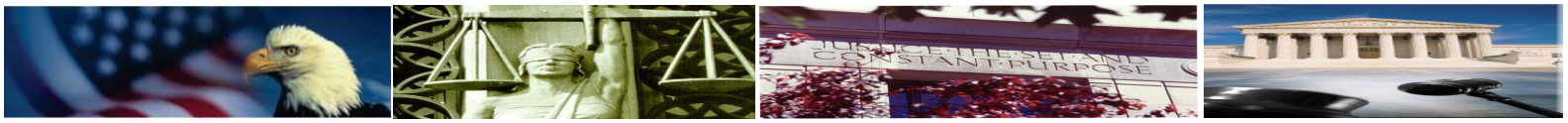
Americans have fallen victim in terror attacks arising from the changing terrorist threats identified earlier in this document both at home and abroad. As the terrorism threat from ISIS and others evolves and inspires attacks around the world, the incidence of foreign attacks harming U.S. victims continues.

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 regularly. 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.

FY 2020 - FY 2022 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 U.S. and foreign counterparts and communicating with the U.S. victims and survivors.



II. Summary of Program Changes

Item Name	Description				Page
		Pos.	Estimated FTE	Dollars ($000)	
Counterintelligence and Export Control, including Countering Cyber Threats	Requesting additional resources for NSD's cyber-related investigations and prosecutions	6	3	$1,362	52
Intelligence Oversight	Requesting additional resources for NSD's intelligence oversight function	8	4	$1,551	56
Counterterrorism, including Domestic Terrorist Threats	Requesting additional resources for NSD's domestic terrorism work	5	2	$1,825	61
Remote Classified Processing	Requesting additional resources to support remote classified (secret) processing	0	0	$2,405	65
Grand Total: FY 2023 Enhancement Request		**19**	**9**	**$7,143**	

III. Appropriations Language and Analysis of Appropriations Language

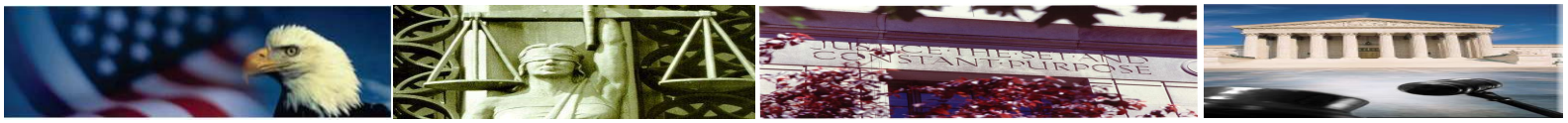
Appropriations Language

SALARIES AND EXPENSES, NATIONAL SECURITY DIVISION

For expenses necessary to carry out the activities of the National Security Division, [$123,093,000] *$133,512,000, 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

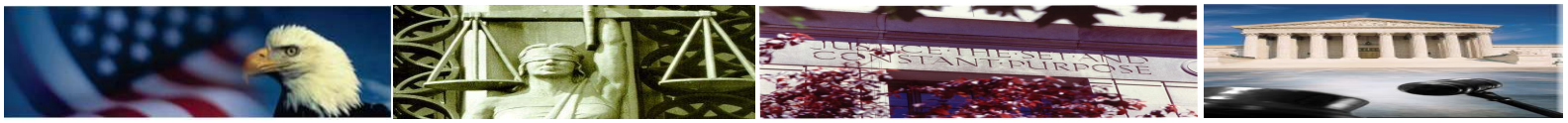
National Security Division	Direct Pos.	Estimate FTE	Amount
2021 Enacted	402	324	$117,451,000
2022 Annualized CR	402	337	$117,451,000
2022 Rebaseline Adjustmnt	13	12	5,642,000
Adjustments to Base and Technical Adjustments	0	6	$3,276,000
2023 Current Services	415	355	126,369,000
2023 Program Increases	19	9	$7,143,000
2023 Program Offsets	0	0	$0
2023 Request	434	364	$133,512,000

National Security Division -Information Technology Breakout	Direct Pos.	Estimate FTE	Amount
2021 Enacted	26	24	13,569,000
2022 Annualized CR	26	26	15,766,000
Adjustments to Base and Technical Adjustments	0	0	56,000
2023 Current Services	26	26	15,822,000
2023 Program Increases	0	0	3,480,000
2023 Program Offsets	0	0	0
2023 Request	26	26	19,302,000
Total Change 2022-2024	**0**	**0**	**3,536,000**

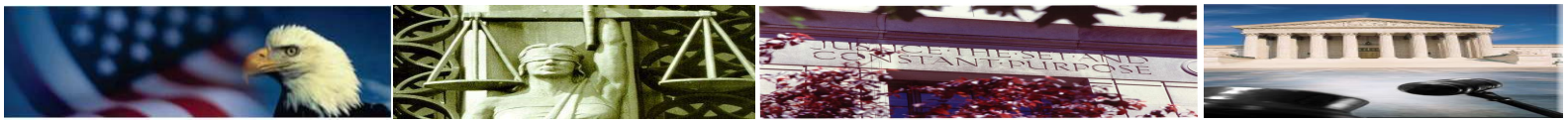
1. Program Description.

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;
- 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 fully informed regarding FISA compliance 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

1. Performance and Resource Tables

PERFORMANCE AND RESOURCES TABLE										
Decision Unit: National Security Division										
RESOURCES ($ in thousands)	Target		Actual		Projected		Changes		Requested (Total)	
	FY 2021		FY 2021		FY 2022		Current Services Adjustments and FY 2023 Program Changes		FY 2023 Request	
Workload*										
Defendants Charged	151		882		136		315		451	
Defendants Closed	131		157		131		250		381	
Matters Opened	350,730		345,130		550,740		-24,670		526,070	
Matters Closed	350,592		343,619		550,602		-24,802		525,800	
FISA Applications Filed**	CY 2021:	1,500	CY 2021:	451	CY 2022:	1,500	-600		CY 2023:	900
National Security Reviews of Foreign Acquisitions	CY 2021:	500	CY 2021:	707	CY 2022:	500	0		CY 2023:	500
Total Costs and FTE	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
(Reimbursable: FTE are included, but costs are bracketed and not included in totals)	337	117,451	337	117,451	349	123,093	15	10,419	364	133,512

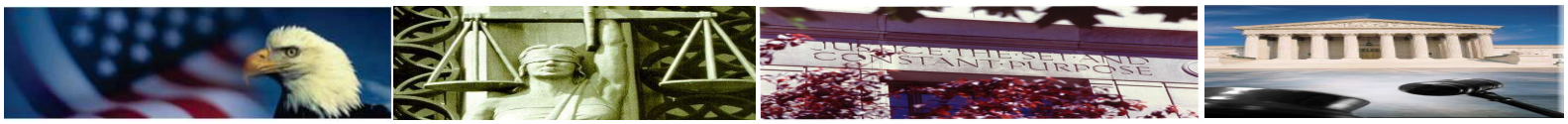
*Workload measures are not performance targets, rather they are estimates to be used for resource planning.

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

PERFORMANCE AND RESOURCES TABLE													
Decision Unit: National Security Division													
RESOURCES ($ in thousands)			**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)**		
TYPE	**STRATEGIC OBJECTIVE**	**PERFORMANCE**	**FY 2021**		**FY 2021**		**FY 2022**		**Current Services Adjustments and FY 2023 Program**		**FY 2023 Request**		
Program Activity	Counterintelligence and Export Control and Foreign Investment Review		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	
			84	29,819	84	29,819	85	30,397	-1	878	84	31,275	
KPI:	2.1 Protect National Security	Percent of prosecutions brought against defendants engaged in a) hostile activities against national assets b) intelligence gathering or c) export violations that are favorably resolved	NA - New measure in FY 2022		NA - New measure in FY 2022		90%		0%		90%		
KPI:	2.1 Protect National Security	Percent of DOJ-led foreign investment cases that were adjudicated favorably	NA - New measure in FY 2022		100%		97%		0%		97%		
Performance Measure:	2.1 Protect National Security	Percentage of CE defendants whose cases were favorably resolved	90%		85%		90%		0%		90%		
Performance Measure:	2.1 Protect National Security	Percentage of CE cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	99%		100%		99%		0%		99%		
Performance Measure:	2.1 Protect National Security	FARA inspections completed	9		20		20		0		20		
Performance Measure:	2.1 Protect National Security	High priority national security reviews completed	CY 2021: 100		CY 2021: 179		CY 2022: 100		10		CY 2023: 110		
Program Activity	Intelligence and Counterterrorism		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	
			229	82,396	229	82,396	240	87,332	13	8,063	253	95,395	

PERFORMANCE AND RESOURCES TABLE													
Decision Unit: National Security Division													
RESOURCES ($ in thousands)			**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)**	
TYPE	**STRATEGIC OBJECTIVE**	**PERFORMANCE**	**FY 2021**		**FY 2021**		**FY 2022**		**Current Services Adjustments and FY 2023 Program**		**FY 2023 Request**	
KPI:	2.2: Counter Foreign and Domestic Terrorism	Percent of counterterrorism defendants whose cases were favorably resolved	90%		93%		90%		0%		90%	
KPI:	2.2: Counter Foreign and Domestic Terrorism	Number of individuals in the Department trained to prosecute domestic terrorism and domestic violent extremism	NA - New measure in FY 2022		1,674		1,000		-500		500	
Performance Measure:	2.2: Counter Foreign and Domestic Terrorism	Percentage of CT cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	99%		100%		99%		0%		99%	
Performance Measure:	2.2: Counter Foreign and Domestic Terrorism	Intelligence Community Oversight Reviews	CY 2021: 105		CY 2021: 117		CY 2022: 130		0		CY 2023: 130	
Program Activity	Cybersecurity		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
			24	5,236	24	5,236	24	5,364	3	1,478	27	6,842
Performance Measure:	2.4 Enhance Cybersecurity and Fight Cybercrime	Percentage of Cyber defendants whose cases were favorably resolved	90%		100%		90%		0		90%	

Strategic Objective	PERFORMANCE MEASURE TABLE										
	Decision Unit: National Security Division										
	Performance Measures		FY 2014	FY 2015	FY 2016	FY 2017	FY 2018	FY 2019	FY 2020	FY 2021	FY 2022	FY 2023
			Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Target	Target
2.1: Protect National Security	**Key Performance Indicator**	Percent of prosecutions brought against defendants engaged in a) hostile activities against national assets b) intelligence gathering or c) export violations that are favorably resolved	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	90%	90%
2.1: Protect National Security	**Key Performance Indicator**	Percent of DOJ-led foreign investment cases that were adjudicated favorably	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	100%	97%	97%
2.1: Protect National Security	**Performance Measure**	Percentage of CE defendants whose cases were favorably resolved	98%	100%	100%	100%	100%	99%	95%	85%	90%	90%
2.1: Protect National Security	**Performance 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%	100%	100%	99%	99%
2.1: Protect National Security	**Performance Measure**	FARA inspections completed	14	14	14	15	15	20	9	20	20	20
2.1: Protect National Security	**Performance Measure**	High priority national security reviews completed	CY 2014: 35	CY 2015: 38	CY 2016: 43	CY 2017: 65	CY 2018: 100	CY 2019: 129	CY 2020: 90	CY 2021: 179	CY 2022: 100	CY 2023: 110
2.2: Counter Foreign and Domestic Terrorism	**Key Performance Indicator**	Percent of counterterrorism defendants whose cases were favorably resolved	92%	98%	99%	91%	91%	96%	91%	93%	90%	90%
2.2: Counter Foreign and Domestic Terrorism	**Key Performance Indicator**	Number of individuals in the Department trained to prosecute domestic terrorism and domestic violent extremism	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	1,674	1,000	500
2.2: Counter Foreign and Domestic Terrorism	**Performance 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%	100%	100%	99%	99%
2.2: Counter Foreign and Domestic Terrorism	**Performance Measure**	Intelligence Community Oversight Reviews	CY 2014: 124	CY 2015: 100	CY 2016: 110	CY 2017: 102	CY 2018: 110	CY 2019: 97	CY 2020: 70	CY 2021: 117	CY 2022: 130	CY 2023: 130
2.4: Enhance Cybersecurity and Fight Cybercrime	**Performance Measure**	Percentage of Cyber defendants whose cases were favorably resolved	NA	100%	100%	100%	100%	100%	0% - No Cyber defedants' cases were closed in FY20	100%	90%	90%



2. Performance, Resources, and Strategies

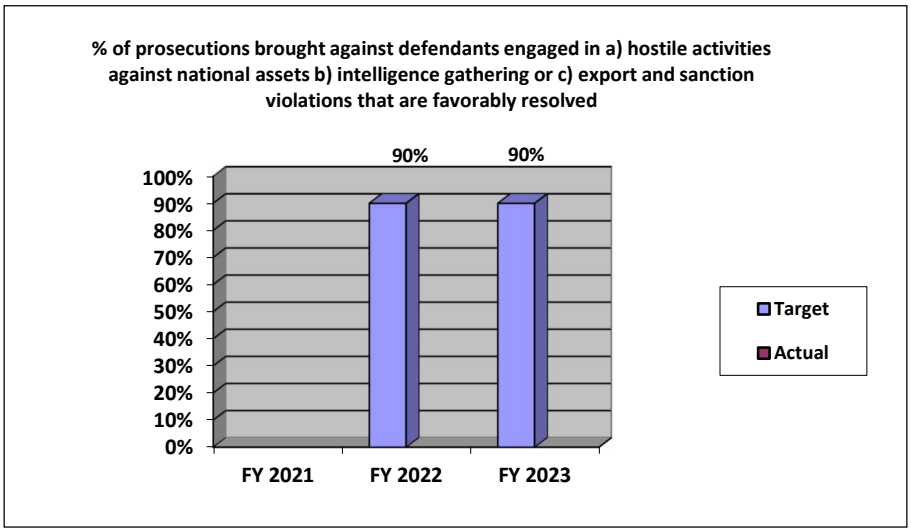
For performance reporting purposes, resources for NSD are included under DOJ Strategic Goal 2: Keep our Country Safe. Within these goals, NSD resources address Strategic Objectives 2.1: Protect National Security, 2.2: Counter Foreign and Domestic Terrorism, and 2.4: Enhance Cybersecurity and Fight Cybercrime.

A. Performance Plan and Report for Outcomes

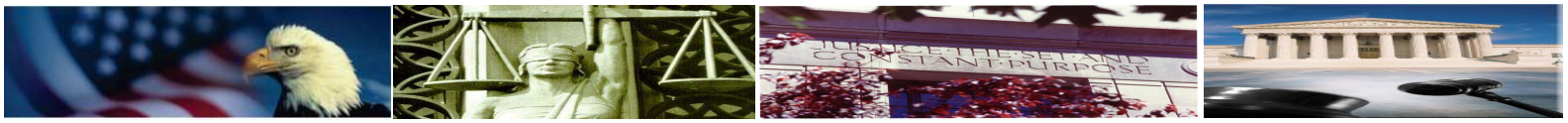
Goal 2: Keep Our Country Safe

Objective 2.1: Protect National Security

Measure: **Percent of prosecutions brought against defendants engaged in a) hostile activities against national assets b) intelligence gathering or c) export and sanction violations that are favorably resolved**
FY 2021 Target: **NA – new measure in FY 2022**
FY 2021 Actual: **NA – new measure in FY 2022**
FY 2022 Target: **90%**
FY 2023 Target: **90%**
Discussion: This is a new measure in FY 2022.



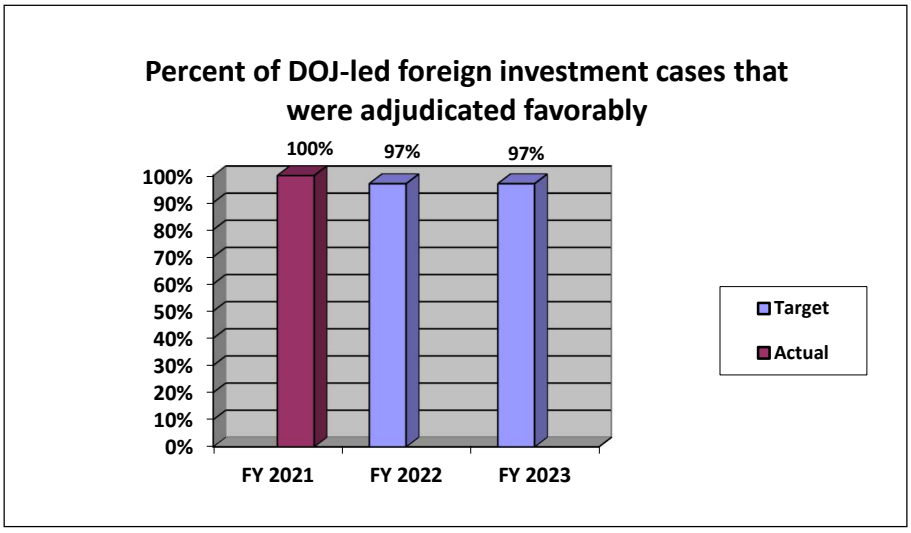
Data Definition: Defendants whose cases were favorably resolved include those defendants whose cases were closed during the fiscal year that resulted in guilty pleas or convictions. Hostile activities against national assets include activities conducted by, at the direction of, or otherwise on behalf of nation-states and international terrorist organizations that negatively impact the national or economic security of the United States and its allies. Intelligence gathering includes defendants who obtained or sought to obtain classified or otherwise sensitive or non-public information at the direction or on behalf of a foreign government or its agents. Export and sanctions violations include criminal violations of the Arms Export Control Act (AECA), the Export Control Reform Act (ECRA), and the International Emergency Economic Powers Act (IEEPA), excluding those violations of the AECA having no relationship to foreign relations.



Data Collection and Storage: Data is stored and tracked in CMS.

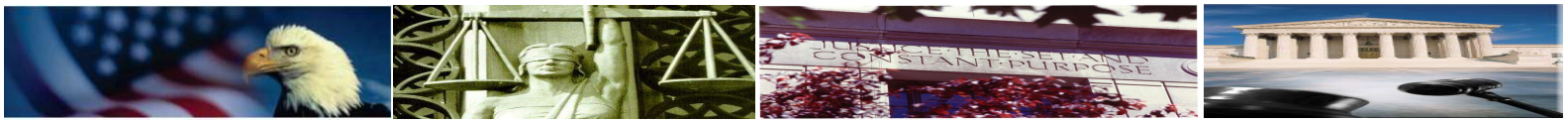
Data Validation and Verification: Data validation and verification is accomplished via quarterly reviews by CES management.
Data Limitations: Reporting lags.

Measure: **Percent of DOJ-led foreign investment cases that were adjudicated favorably**
FY 2021 Target: **NA – new measure in FY 2022**
FY 2021 Target: **100%**
FY 2022 Target: **97%**
FY 2023 Target: **97%**
Discussion: NSD, through FIRS, led and favorably adjudicated a total of 369 foreign-investment cases completed in FY 2021.

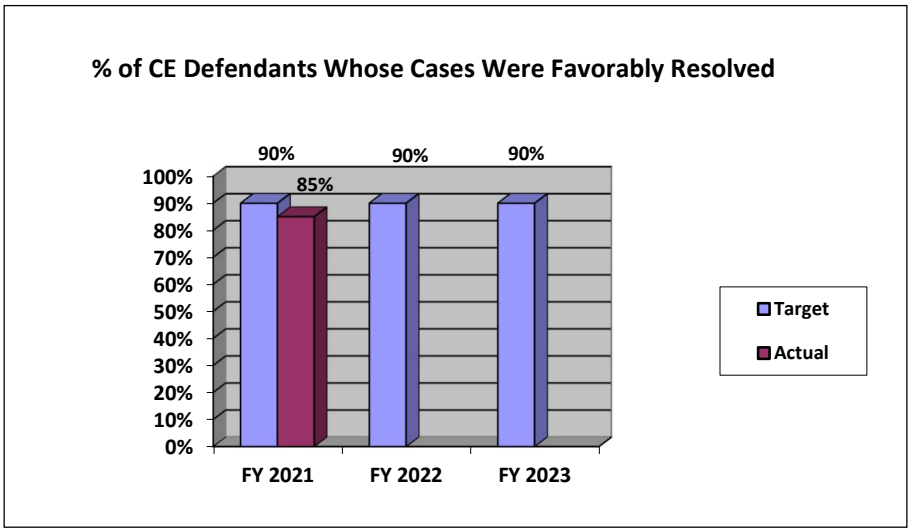


Data Definition: Percentage of cases co-led by the DOJ in the Committee on Foreign Investment in the United States (CFIUS), Team Telecom, and EO 13873 supply chain processes that were completed within defined timelines and within established outcomes and mitigation agreements that were favorably maintained or terminated.
Data Collection and Storage: NSD case records
Data Validation and Verification: Manual validation
Data Limitations: None identified at this time.

Measure: **Percentage of CE Defendants Whose Cases Were Favorably Resolved**
FY 2021 Target: **90%**
FY 2021 Actual: **85%**
FY 2022 Target: **90%**
FY 2023 Target: **90%**
Discussion: FY 2021: The FY 2021 target was not met because several cases were dismissed based on recent case developments, the inability of prosecutors to comply with discovery obligations for a case whose trial was about to start, and the fact that defendants already had received punishments equal to what they would have received upon conviction. FY 2023: 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.



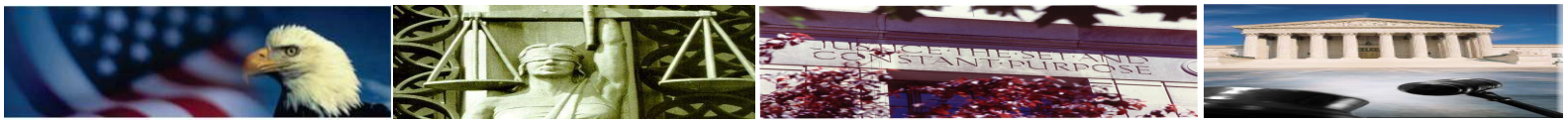
Data Definition: Defendants whose cases were favorably resolved include those defendants whose cases were closed during the fiscal year that resulted in court judgments favorable to the Government.
Data Collection and Storage: Data is stored and tracked in CMS.
Data Validation and Verification: Data validation and verification is accomplished via quarterly reviews by CES management.
Data Limitations: Reporting lags.

Highlights from Recent Counterintelligence Cases

U.S. v. Toebbe: In October 2021, in the Northern District of West Virginia, Jonathan Toebbe and his wife, Diana Toebbe, were indicted for violating the Atomic Energy Act. The Toebbes were charged with selling Restricted Data concerning the design of nuclear-powered warships to a person they believed was a representative of a foreign power. Jonathan was an employee of the Department of the Navy who served as a nuclear engineer and was assigned to the Naval Nuclear Propulsion Program, also known as Naval Reactors. Jonathan worked with information concerning naval nuclear propulsion, including military sensitive design elements, operating parameters, and performance characteristics of the reactors for nuclear-powered warships. In February 2022, both pleaded guilty.

U.S. v. Hale: In July 2021, in the Eastern District of Virginia, Daniel Hale was sentenced to 45 months in prison after pleading guilty to unlawfully disclosing classified information. Hale was charged in May 2019. Hale, held a Top Secret//Sensitive Compartmented Information security clearance both while he was in the U.S. Air Force assigned to the National Security Agency (NSA), and when he worked as a cleared contractor working at the National Geospatial-Intelligence Agency (NGA). Hale took classified documents from his work at NGA and provided them to a reporter. Those documents were later published by the reporter's news outlet.

U.S. v. Thompson: In June 2021, in the District of Columbia, Mariam Taha Thompson was sentenced to 23 years in prison for delivering classified national defense information (NDI) to aid a foreign government. In March 2021, Thompson had pled guilty to one count of delivering NDI, in violation of 18



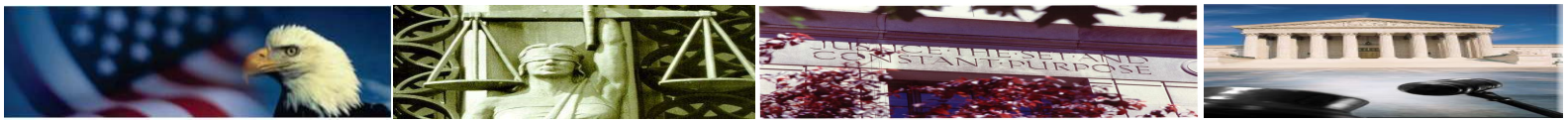
U.S.C. § 794(a). Thompson, a linguist for the Department of Defense (DOD), was charged in March 2020 with transmitting highly sensitive NDI to a foreign national with apparent connections to Hizballah, a designated foreign terrorist organization. According to court documents, the information Thompson gathered and transmitted included classified NDI regarding active human assets, including their true names. Thompson was arrested by FBI Special Agents in February 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. The investigation revealed Thompson transmitted classified information to a co-conspirator, who has apparent connections to Hizballah.

U.S. v. Debbins: In May 2021, in the Eastern District of Virginia, Peter Debbins was sentenced to 188 months in prison for conspiring to gather and deliver national defense information to agents of the Russian Federation. Debbins was charged in August 2020 and pled guilty in January 2021. Debbins conspired with agents of Russian Intelligence Services (RIS) from 1996 through 2011. During that period, from 1998 through 2005, Debbins served as a U.S. Army officer, including in chemical units and the U.S. Army Special Forces. Debbins provided RIS agents with information about his Special Forces deployments and gave them information about his Special Forces team members so the RIS agents could evaluate whether to target those individuals for recruitment.

U.S. v. Zheng: In May 2021, in the Southern District of Ohio, Song Guo Zheng was sentenced to 37 months in prison and was ordered to pay more than $3.4 million in restitution to the National Institutes of Health (NIH) and more than $400,000 to The Ohio State University (OSU). Zheng pled guilty in November 2020 to making false statements in applications for NIH research funding. Zheng concealed from NIH and OSU his foreign support and conflicts of interests, including his participation in People's Republic of China (PRC)-based talent plans. Zheng was arrested in May 2020 in Anchorage, Alaska as he attempted to flee to the PRC.

Highlights from Recent Export Control Cases

U.S. v. All Petroleum et al.: In December 2021, DOJ announced the successful forfeiture of two large caches of Iranian arms, as well as approximately 1.1 million barrels of Iranian petroleum products. 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

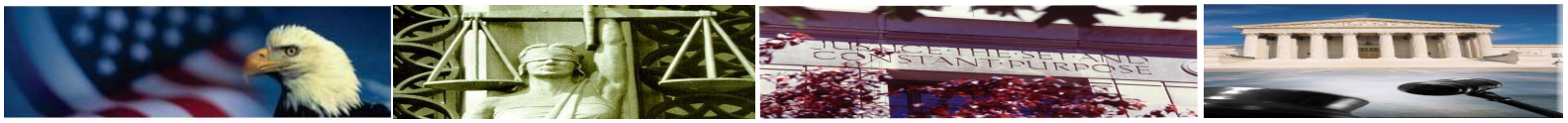


seeking to forfeit the seized weapons. In July 2020, DOJ also filed a civil complaint seeking to forfeit all petroleum cargo aboard the four foreign-flagged oil tankers. D.C. District Court later issued a warrant for arrest in rem, and the U.S. subsequently transferred approximately 1.1 million barrels of refined petroleum from the four vessels. The U.S. now has sold that petroleum.

U.S. v. Qin: In September 2021, in the District of Massachusetts, Chinese national Shuren Qin was sentenced for illegally procuring and exporting U.S.-origin goods to Northwestern Polytechnical University (NWPU), a Chinese military university that is heavily involved in military research and works closely with the People's Liberation Army (PLA) on the advancement of its military capabilities. Qin was sentenced to two years in prison, to be followed by two years of supervised release. Qin also was ordered to pay a fine of $20,000 and will face deportation proceedings upon completion of his sentence. In April 2021, Qin pleaded guilty to conspiracy to unlawfully export items from the United States; making false statements; money laundering; and smuggling.

U.S. v. Farahani et al.: In July 2021, in the Southern District of New York, an indictment was unsealed charging four Iranian nationals with conspiracies related to kidnapping, sanctions violations, bank and wire fraud, and money laundering. A co-conspirator and California resident also faces charges. Alireza Shavaroghi Farahani, Mahmoud Khazein, Kiya Sadeghi, and Omid Noori, all of Iran, allegedly conspired to kidnap a Brooklyn journalist for mobilizing public opinion to bring about changes to the Iranian regime's laws and practices. Niloufar "Nellie" Bahadorifar, originally of Iran and currently residing in California, is alleged to have provided financial services that supported the plot. Farahani, Khazein, Sadeghi, and Noori each are charged with: conspiracy to kidnap; conspiracy to violate the International Emergency Economic Powers Act and sanctions against the government of Iran; conspiracy to commit bank and wire fraud; and conspiracy to launder money. While Bahadorifar is not charged with participating in the kidnapping conspiracy, she is charged with conspiring to violate sanctions against Iran, commit bank and wire fraud, and commit money laundering. Bahadorifar also is charged with structuring cash deposits totaling more than $445,000. According to the indictment: Farahani is an Iranian intelligence official who resides in Iran. Khazein, Sadeghi, and Noori are Iranian intelligence assets who also reside in Iran and work under Farahani. Since at least June 2020, Farahani and his intelligence network conspired to kidnap a U.S. citizen of Iranian origin (Victim-1) from within the United States in furtherance of the government of Iran's efforts to silence Victim-1's criticisms of the regime. Victim-1 is a journalist and author who has publicly criticized the government of Iran for committing human rights abuses. On multiple occasions in 2020 and 2021, as part of the plot to kidnap Victim-1, Farahani and his network procured the services of private investigators to surveil, photograph, and video record Victim-1 and Victim-1's household members in Brooklyn. Network members misrepresented their identities and the purpose of the surveillance to investigators, and laundered money into the United States from Iran to pay for the surveillance. As part of the kidnapping plot, the Farahani-led network also researched methods of transporting Victim-1 out of the United States for rendition to Iran.

U.S. v. SAP SE: In April 2021, in the District of Massachusetts, software company SAP SE, headquartered in Walldorf, Germany, agreed to pay combined penalties of more than $8 million as part of a global resolution with the U.S. Departments of Justice, Commerce, and Treasury. In voluntary disclosures the company made to the three agencies, SAP acknowledged violations of the Export Administration Regulations and the Iranian Transactions and Sanctions Regulations. As a result of its voluntary disclosure, extensive cooperation, and strong remediation costing more than $27 million, DOJ entered into a non-prosecution agreement with SAP. Pursuant to that agreement, SAP will disgorge $5.14 million of ill-gotten gain. Concurrently, SAP entered into administrative agreements with the Commerce Department's Bureau of Industry and Security (BIS) and the Treasury Department's Office of Foreign



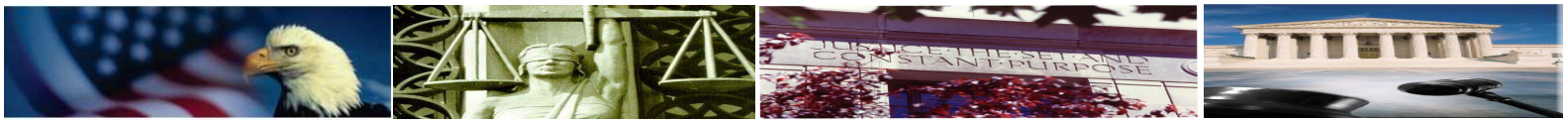
Assets Control (OFAC). Among other things, the BIS settlement agreement requires SAP to conduct internal audits of its compliance with U.S. export control laws and regulations and produce audit reports to BIS for a period of three years. From approximately January 2010 through September 2017, SAP, without a license, willfully exported, or caused the export, of its products to Iranian users. While this conduct constituted serious violations of U.S. law involving the release of U.S.-origin technology and software through cloud servers and online portals, the non-prosecution agreement recognizes the importance of voluntary self-disclosure and cooperation with the government.

U.S. v. Zangakani et al.: In March 2021, in the Central District of California, the Department of Justice announced charges against 10 Iranian nationals for running a nearly 20-year-long scheme to evade U.S. sanctions on the Government of Iran by disguising more than $300 million worth of transactions – including the purchase of two $25 million oil tankers – on Iran's behalf through front companies in California, Canada, Hong Kong, and the United Arab Emirates. In addition, DOJ filed a forfeiture complaint seeking a money laundering penalty in the amount of $157,332,367.

Highlights from Recent Foreign Malign Influence cases

U.S. v. Barrack et al.: In July 2021, in the Eastern District of New York, a seven-count indictment was unsealed relating to unlawful efforts to advance the interests of the United Arab Emirates (UAE) in the United States at the direction of senior UAE officials by influencing the foreign policy positions of a campaign in the 2016 U.S. presidential election and, subsequently, the foreign policy positions of the U.S. government in the incoming administration. Thomas Joseph Barrack of Santa Monica, California; Matthew Grimes of Aspen, Colorado; and Rashid Sultan Rashid Al Malik Alshahhi of the UAE are accused of acting and conspiring to act as agents of the UAE between April 2016 and April 2018, in violation of 18 U.S.C. § 951. The indictment also charges Barrack with obstruction of justice and making multiple false statements during a June 2019 interview with federal law enforcement agents. According to court documents: Barrack served as the executive chairman of a global investment management firm headquartered in Los Angeles, and Grimes was employed at the firm and reported directly to Barrack. Alshahhi worked as an agent of the UAE and was in frequent contact with Barrack and Grimes, including numerous in-person meetings in the United States and the UAE. Between April and November 2016, Barrack served as an informal advisor to the campaign of a candidate in the 2016 U.S. presidential election. Between November 2016 and January 2017, Barrack served as chairman of the Presidential Inaugural Committee. Beginning in January 2017, Barrack informally advised senior U.S. government officials on issues related to U.S. foreign policy in the Middle East. Barrack also sought appointment to a senior role in the U.S. government. As alleged in the indictment, the defendants used Barrack's status as an advisor to the campaign and, subsequently, to senior U.S. government officials, to advance the interests of and provide intelligence to the UAE while simultaneously failing to notify the Attorney General that their actions were taken at the direction of senior UAE officials. Barrack – directly and through Alshahhi and Grimes – was regularly and repeatedly in contact with the senior leadership of the UAE government. On multiple occasions, Barrack referred to Alshahhi as the UAE's "secret weapon" to advance its foreign policy agenda in the United States.

U.S. v. Michel et al.: In June 2021, in the District of Columbia, a federal grand jury returned a superseding indictment charging a U.S. entertainer/businessman and a Malaysian national with orchestrating an unregistered, back-channel campaign beginning in or about 2017 to influence the then-administration of the President of the United States and the Department of Justice both to drop an investigation in connection with the international strategic and development company known as 1Malaysia Development Berhad (1MDB), in violation of the Foreign Agents Registration Act (FARA), 22 U.S.C. § 611, *et seq.*,

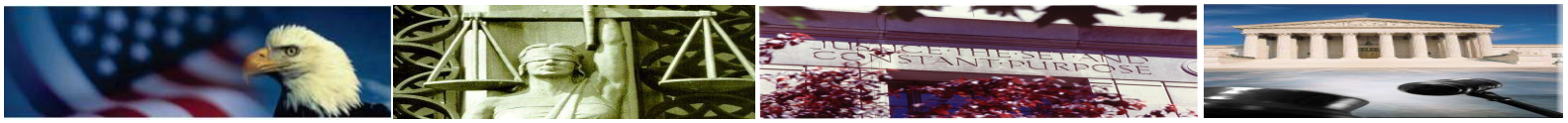


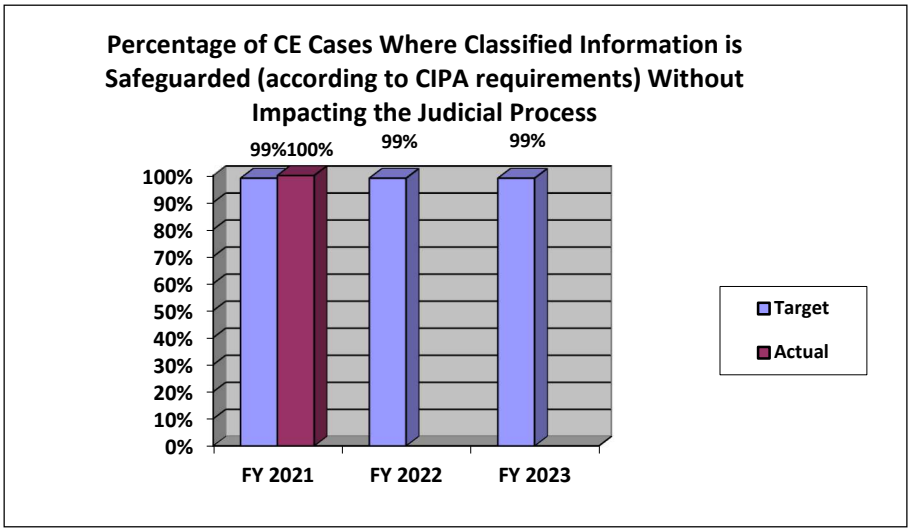
and to send a Chinese dissident back to China, in violation of 18 U.S.C. § 951. According to the indictment, Prakazrel "Pras" Michel and Low Taek Jho a/k/a Jho Low are alleged to have conspired with Elliott Broidy, Nickie Lum Davis, and others to engage in undisclosed lobbying campaigns at the direction of Low and the Vice Minister of Public Security for the People's Republic of China, respectively, both to have the 1MDB embezzlement investigation and forfeiture proceedings involving Low and others dropped and to have a Chinese dissident sent back to China. Michel and Low also are charged with conspiring to commit money laundering related to the foreign influence campaigns. Michel also is charged with witness tampering and conspiracy to make false statements to banks. In May 2019, Michel and Low were charged in the District of Columbia for allegedly orchestrating and concealing a foreign and conduit contribution scheme in which they funneled millions of dollars of Low's money into the U.S. presidential election as purportedly legitimate campaign contributions, all while concealing the true source of the money. To execute the scheme, Michel allegedly received Low's money and contributed it both personally and through approximately 20 straw donors.

U.S. v. Rafiekian: In March 2021, the Court of Appeals for the Fourth Circuit reversed rulings of the district court and reinstated the guilty verdicts. The Fourth Circuit declined the defendant's request for en banc rehearing of the appeal. In July 2019, in the Eastern District of Virginia, a jury convicted Bijan Rafiekian of conspiring to violate 18 U.S.C. § 951, and violations of both FARA and 18 U.S.C. § 951. The charges arose from the lobbying scheme that Rafiekian, General Michael Flynn, and Kamil Alptekin, a Turkish national, carried out to affect public opinion and Congressional views about Turkey's request for the extradition of Turkish dissident Fetullah Gulen. The trial judge later vacated the convictions and conditionally granted a new trial.

U.S. v. Zuberi: In February 2021, in the Central District of California, Imaad Shah Zuberi was sentenced to 12 years in prison – including the statutory maximum five years on a FARA charge – and ordered to pay $15.7 million in restitution and a criminal fine of $1.75 million. Zuberi pled guilty in 2019 to violating FARA, tax evasion, and making almost $1 million in illegal campaign contributions, including money from foreign entities used to influence U.S. elections. Zuberi subsequently pled guilty to obstruction of justice in 2020 in the Southern District of New York. Between 2013 and 2017, Zuberi solicited foreign nationals and representatives of foreign governments with claims he could use his contacts to change U.S. foreign policy to benefit his clients. As part of his efforts to influence public policy, Zuberi hired lobbyists, retained public relations professionals, and made campaign contributions that gave him access to high-level U.S. officials, whom Zuberi then lobbied to act in support of his clients. In relation to the FARA charge, Zuberi admitted to submitting false registration statements that concealed his role in a lobbying effort on behalf of the Government of Sri Lanka, his political contributions, and millions of dollars he received.

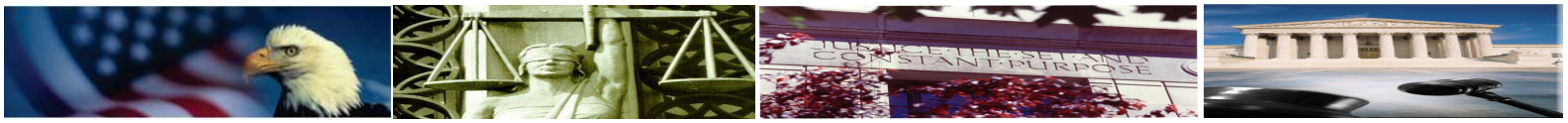
Measure: **Percentage of CE Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2021 Target: **99%**
FY 2021 Actual: **100%**
FY 2022 Target: **99%**
FY 2023 Target **99%**
Discussion: The FY 2023 target is consistent with previous fiscal years. NSD will support successful prosecutions by providing advice and assistance on the use of classified evidence through the application of the CIPA.

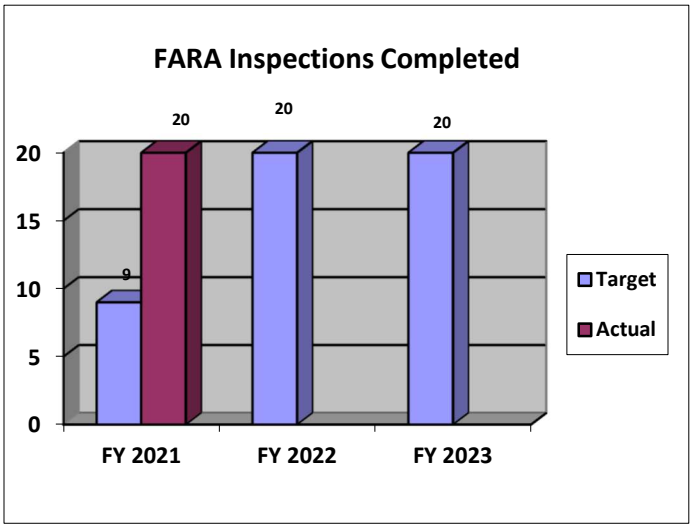




Data Definition: Classified Information - information that has been determined by the United State Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data as defined by the 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 is not 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.

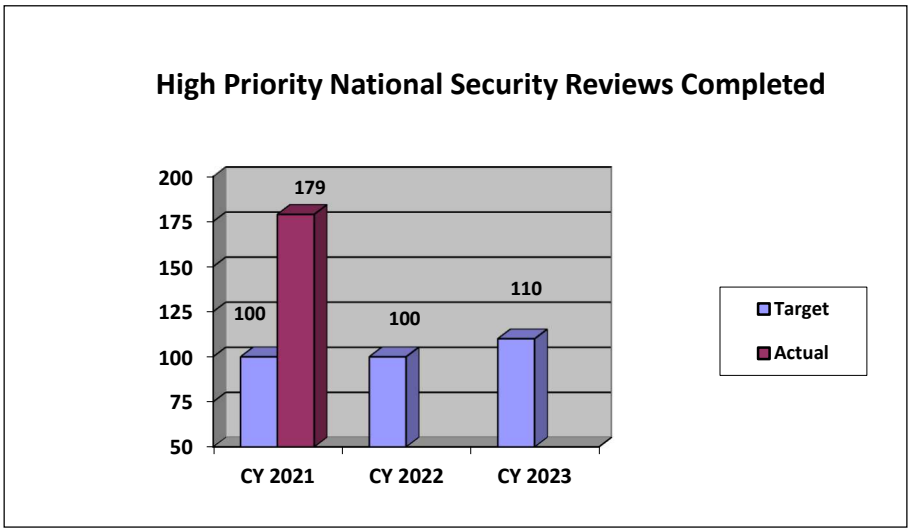
Measure: **FARA Inspections Completed**
FY 2021 Target: **9**
FY 2021 Actual: **20**
FY 2022 Target: **20**
FY 2023 Target: **20**
Discussion: The FY 2023 target is consistent with prior fiscal years. Performing targeted inspections allows the FARA Unit to more effectively enforce compliance among registrants under FARA.



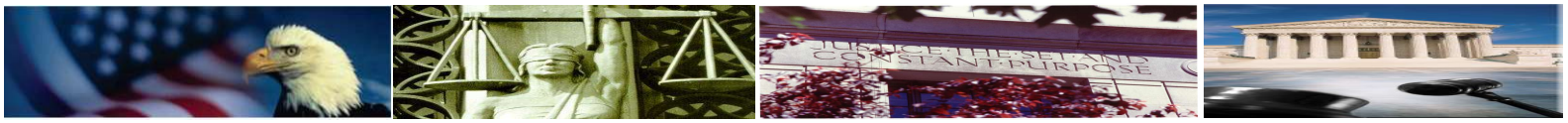


Data Definition: Targeted FARA Inspections are conducted routinely. There can also be additional inspections completed based on potential non-compliance issues. Inspections are just one tool used by the Unit to bring registrants into compliance with FARA.
Data Collection and Storage: Inspection reports 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 2021 Target: **100**
CY 2021 Actual: **179**
CY 2022 Target: **100**
CY 2023 Target: **110**
Discussion: The FY 2023 target is slightly increased from previous fiscal years. NSD will continue to work with its partners to perform these high priority reviews.



Data Definition: High Priority National Security Reviews include:



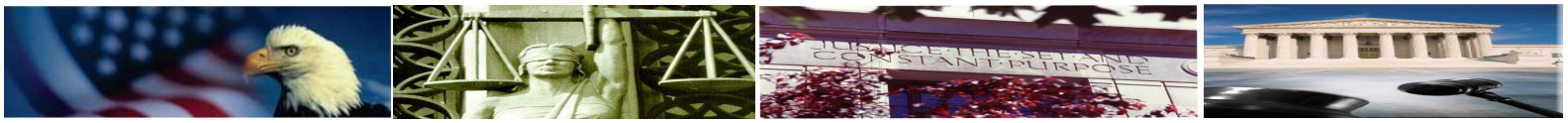
1. CFIUS case reviews of transactions in which DOJ is a co-lead agency in CFIUS due to the potential impact on DOJ equities;
2. CFIUS case reviews which result in a mitigation agreement to which DOJ is a signatory;
3. Team Telecom case reviews which result in a mitigation agreement to which DOJ is a signatory; and
4. Mitigation monitoring site visits.

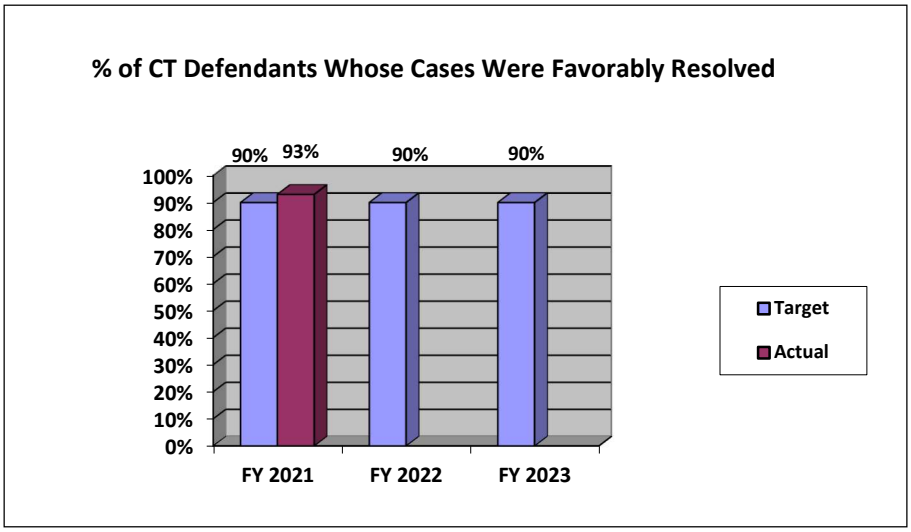
Note telecommunications supply chain reviews is a new element of the performance measures, and reflects anticipated work as a result of new supply chain regulations being promulgated pursuant to an Executive Order signed by the President in May 2019. While the number of reviews is not yet knowable, NSD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

Data Collection and Storage: Data is collected manually and stored in generic files; however, management is reviewing the possibility of utilizing a modified automated tracking system.
Data Validation and Verification: Data is validated and verified by the Foreign Investment Review Section's (FIRS) management.
Data Limitations: Given the expanding nature of the program area – a more centralized data system is desired.

Objective 2.2: Counter Foreign and Domestic Terrorism

Measure: **Percentage of CT Defendants Whose Cases Were Favorably Resolved**
FY 2021 Target: **90%**
FY 2021 Actual: **93%**
FY 2022 Target: **90%**
FY 2023 Target: **90%**
Discussion: The FY 2023 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

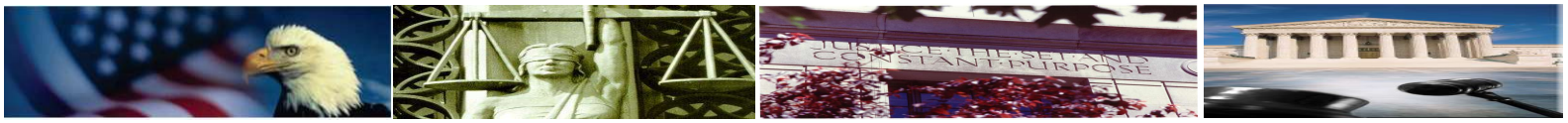
The following are highlights from recent counterterrorism cases.

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.

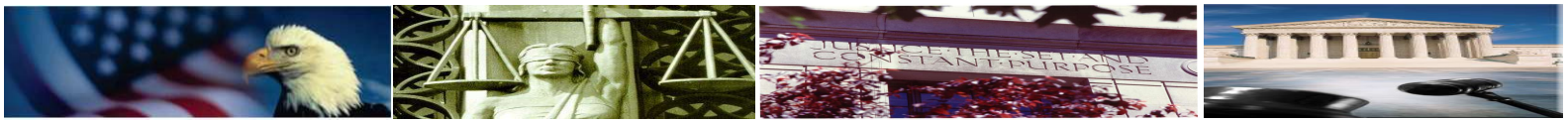
Murat Cakar: ISIS Financier and COVID-19

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.

Alexanda Kotey Pleads Guilty

On September 2, 2021, in the Eastern District of Virginia, Alexanda Amon Kotey ("Kotey") entered a guilty plea to all charges in an eight-count indictment. Kotey is 36 years old and previously had citizenship in the United Kingdom. Kotey is charged with four counts of hostage taking resulting in death, in violation of 18 U.S.C. § 1203, one count of conspiring to take hostages resulting in death, in violation of 18 U.S.C. § 1203, one count of conspiring to murder U.S. nationals outside the United States, in violation of 18 U.S.C. § 2332(b)(2), one count of conspiring to provide material support to terrorists, in violation of 18 U.S.C. § 2339A, and one count of conspiring to provide material support to ISIS, in violation of 18 U.S.C. § 2339B. Sentencing is set for March 4, 2022.

The charges stem from the membership of Kotey and co-defendant El Shafee Elsheikh ("Elsheikh") in ISIS and their roles in an ISIS hostage-taking network. Kotey and Elsheikh left the United Kingdom in 2012 and traveled to Syria, where they joined ISIS. Kotey and Elsheikh were instrumental in detaining, transporting, and subduing hostages, and obtained photos and videos of, and information from, hostages for ransom negotiations. Kotey and Elsheikh specifically participated in the detention of U.S. citizens Kayla Jean Mueller, James Foley, Steven Sotloff, and Peter Kassig. The 2014 executions of Mr. Foley, Mr. Sotloff, and Mr. Kassig by a co-conspirator named Mohamed Emwazi (also known as "Jihadi John") were videotaped and distributed through ISIS media channels as part of ISIS's propaganda



campaign. ISIS informed Ms. Mueller's family of her death in 2015, when she was still being held hostage by that organization.

Sentencing for Michigan Governor Kidnapping Conspirator

On August 25, 2021, in the Western District of Michigan, Ty Garbin ("Garbin") was sentenced to 76 months in prison, 3 years of supervised release, and a $2,500 fine for his role in the conspiracy to kidnap Governor Gretchen Whitmer. On January 27, 2021, Garbin entered a guilty plea for his role in the conspiracy. Garbin's plea agreement requires that he cooperate with the Government.

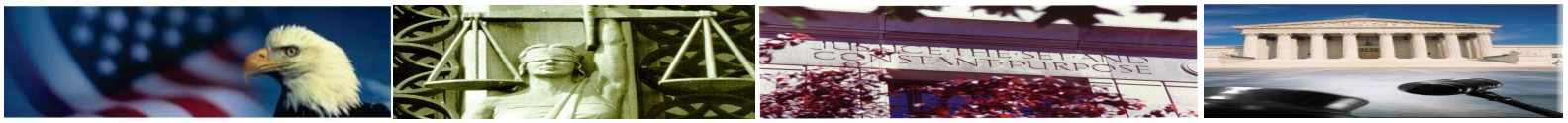
On April 27, 2021, a grand jury returned a superseding indictment charging Barry Gordon Croft ("Croft"), Adam Fox ("Fox"), Daniel Harris ("Harris"), Kaleb Franks ("Franks"), and Brandon Caserta ("Caserta") (collectively, the "Defendants") with conspiring to kidnap Governor Gretchen Whitmer, in violation of 18 U.S.C. § 1201. The superseding indictment also charged: Fox, Croft, and Harris with conspiring to use a weapon of mass destruction, in violation of 18 U.S.C. § 2332a; Croft and Harris with possessing a firearm/destructive device that was not registered to them, in violation of 26 U.S.C. §§ 5861(d), 5841, 5871, and 2; and Harris with possessing a firearm, that is, an Anderson Manufacturing, Model AM-15, .223/5.56 mm caliber semiautomatic assault rifle, which was not registered to him, in violation of 26 U.S.C. §§ 5861(d), 5845(a)(3), 5871, 2.

On June 6, 2020, Croft, Fox, and others gathered in person at a hotel in Dublin, Ohio, to discuss the desire and potential plans to live in a self-sustained society governed only by the U.S. Bill of Rights. They discussed both peaceful and violent means of achieving their goals. One suggestion was the kidnapping of certain governors (with a focus on Michigan). During the meeting, Croft showed the group a homemade improvised explosive device ("IED") that he made before the meeting. On July 11-12, 2020, several of the defendants and others met at a property near Madison, Wisconsin, where the group engaged in firearms and bomb-making training. Croft brought explosive devices that he created and conducted explosives training with the group. On August 23, 2020, Garbin, Harris, Franks, Caserta, and others met at Harris's residence in Lake Orion, Michigan. They discussed concerns about being infiltrated by law enforcement and were required to bring personal documents to confirm their identities. The group then discussed surveilling the Michigan Governor's vacation home in preparation for an attack. On August 29, 2020, Fox and others conducted surveillance of Governor Whitmer's vacation home.

On September 12-13, 2020, several of the defendants and others met at Garbin's property in Luther, Michigan, to finalize plans and conduct surveillance on Governor Whitmer. Croft brought what he called his "chemistry set" to the meeting, which included components for an IED. The group discussed using the IED to blow up a bridge near Governor Whitmer's home to impede the law-enforcement response during the kidnapping. The group also conducted nighttime surveillance of the Governor's house. During the surveillance, Fox stopped at a bridge that they targeted for detonation and took pictures of the underside of the bridge for places to set an explosive device.

On October 7, 2020, the Defendants and Garbin were arrested based on a criminal complaint charging the same conduct. On December 15, 2020, a grand jury returned an indictment against six individuals, including the Defendants and Garbin, for conspiring to kidnap Governor Gretchen Whitmer, in violation of 18 U.S.C. § 1201.

Breach of the U.S. Capitol on January 6, 2021



- The breach of the U.S. Capitol on January 6, 2021 brought an unprecedented number of new prosecutions and investigations to the Counterterrorism Section (CTS). As of September 1, 2021, there have been nearly 600 arrests in almost all 50 states.

- Over 175 defendants have been charged with assaulting, resisting, or impeding officers or employees, including more than 55 that have been charged with using a deadly or dangerous weapon. There are over 34 defendants charged with destruction of government property and nearly 30 more charged with theft of government property. Over 500 defendants have been charged with entering or remaining in a restricted federal building or grounds. And at least 240 defendants have been charged with corruptly obstructing, influencing, or impeding an official proceeding, or attempting to do so.

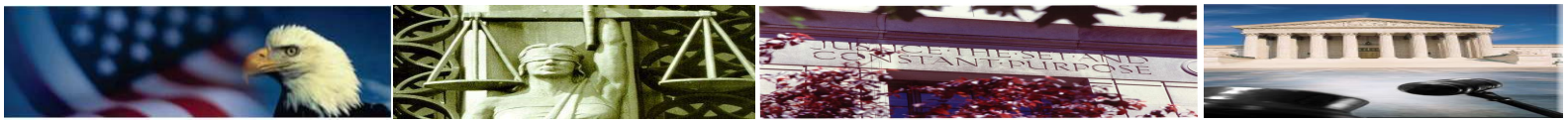
- More than 30 individuals have pleaded guilty to a variety of federal charges, from misdemeanors to felony obstruction, many of whom will face incarceration at sentencing.

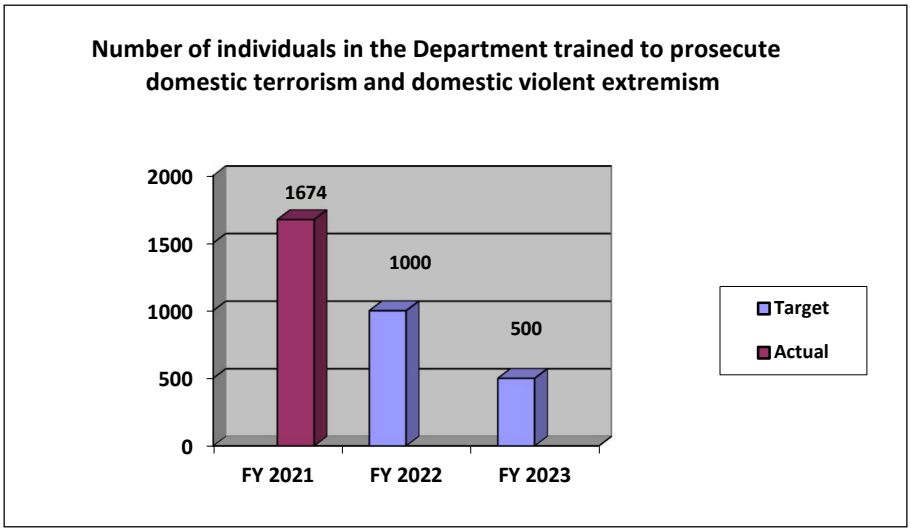
- More than 25 have pleaded guilty to misdemeanors. Eight have pleaded guilty to felonies.

- Two have pleaded guilty to felony assault on law enforcement which carries a maximum statutory penalty of eight years in prison and a $250,000 fine.

- Six defendants have had their cases adjudicated and received sentences for their criminal activity on January 6. At least 15 more defendants will be sentenced in the next 100 days.

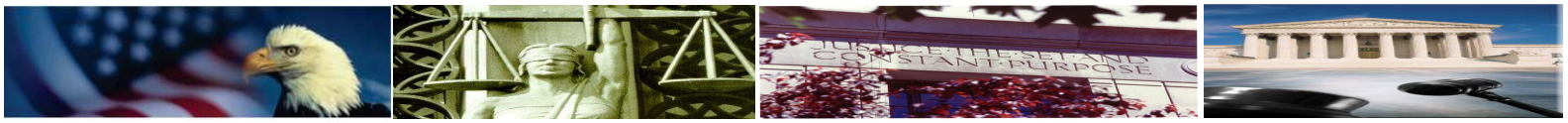
Measure: **Number of individuals in the Department trained to prosecute domestic terrorism and domestic violent extremism**
FY 2021 Target: **Not applicable**
FY 2021 Actual: **1,674**
FY 2022 Target: **1,000**
FY 2023 Target: **500**
Discussion: FY 2021 - Six webinars were conducted that included topics regarding Domestic Terrorism/Domestic Violent Extremists. There was a total of 1,674 individuals who registered to attend these webinars. NSD was able to track the number of individuals who registered for webinars, but not those who actually attended the trainings. In many instances, an individual may have registered for a webinar and then have work demands or personal reasons that prevented them from attending.
FY 2022 and FY 2023 - While the number of national security courses offered in FY 2022 and FY 2023 can be predicted, it is not possible at this time to predict whether those courses will be conducted in-person or virtually. As a result, the number of individuals who will be trained cannot be predicted with any accuracy since there would be larger numbers for webinars than for in-person training courses. In addition, even if some courses return to an in-person, classified environment, social distancing limitations imposed by the training facility may limit the number of individuals trained.

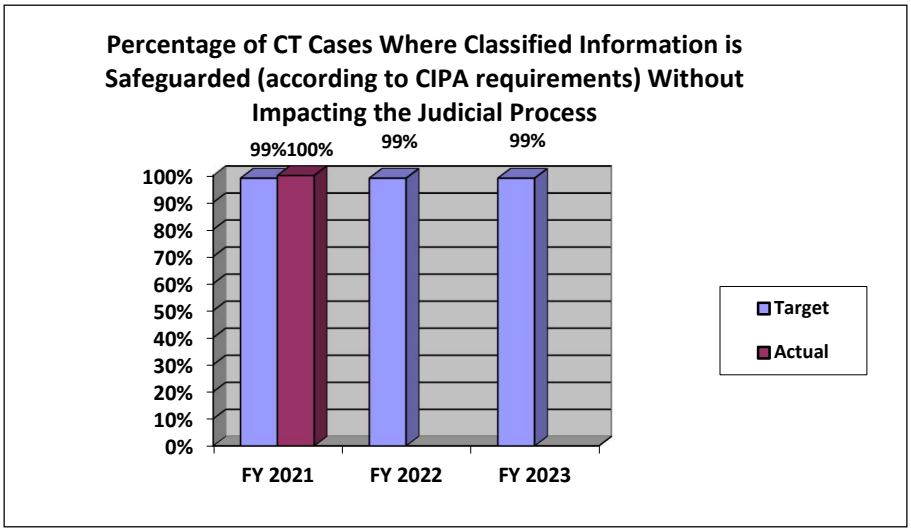




Data Definition: Training includes virtual or in-person courses and webinars.
Data Collection and Storage: LearnDOJ course views
Data Validation and Verification: Data will be validated with EOUSA's Office of Legal Education.
Data Limitations: The numbers of individuals trained in FY 22 and FY 23 will depend greatly on the ability to conduct in-person trainings or whether we will conduct webinars only as a result of the pandemic. For national security courses that can be conducted in an unclassified environment, we will continue to conduct some webinars in order to reach a larger audience of prosecutors and agents. In addition, even if some courses return to an in-person, classified environment, social distancing limitations imposed by the training facility may limit the number of individuals trained. For this purpose, we set FY 22 and FY 23 targets assuming at least some trainings will be held in person. To illustrate the impact in-person trainings vs. webinars has on the numbers, in FY 22, there have been two webinars conducted so far that included topics regarding Domestic Terrorism/Domestic Violent Extremists. There was a total of 784 individuals who registered to attend these webinars. There are three additional courses planned for FY 22 which will include topics regarding Domestic Terrorism/Domestic Violent Extremists. If those courses can be conducted in-person, it is anticipated that an approximate total of 300 individuals will be trained. If those courses must be conducted as webinars, we anticipate an approximate total of 1,000 individuals trained. In FY 23, there are four courses tentatively scheduled, which will include topics regarding Domestic Terrorism/Domestic Violent Extremists. If those courses can be conducted in-person, it is anticipated that an approximate total of 500 individuals will be trained. If those courses must be conducted as webinars, we anticipate an approximate total of 1,400 individuals trained.

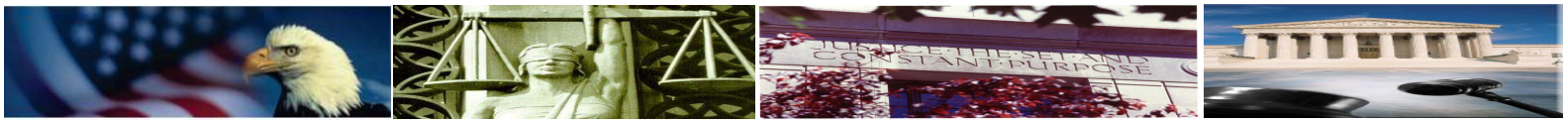
Measure: **Percentage of CT Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2021 Target: **99%**
FY 2021 Actual: **100%**
FY 2021 Target: **99%**
FY 2023 Target: **99%**
Discussion: The FY 2023 target is consistent with previous 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).

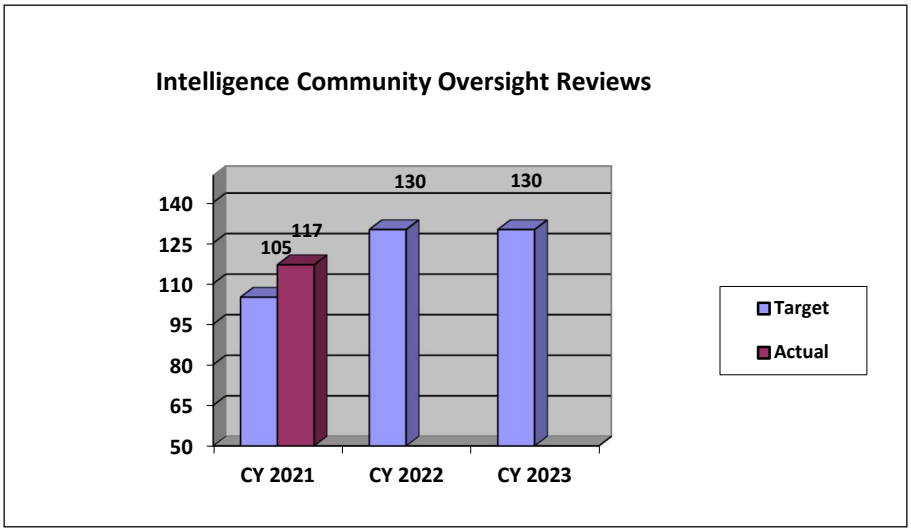




Data Definition: Classified Information - information that has been determined by the U.S. Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data as defined by the Atomic Energy 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 is not 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.

Measure: **Intelligence Community Oversight Reviews**
CY 2021 Target: **105**
CY 2021 Actual: **117**
CY 2022 Target: **130**
CY 2023 Target: **130**
Discussion: CY 2023 - The CY 2023 target is consistent with previous targets. The overall work of NSD assessing and ensuring compliance is expected to continue to increase in future years due to the growth of current oversight programs; though this is largely reflected in the targets for matters opened and closed. The scope and resources required to prepare for, and conduct, existing reviews is expected to continue to increase due to the IC's increased use of certain national security tools.

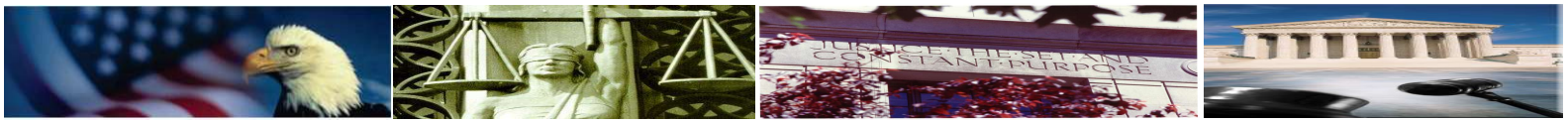


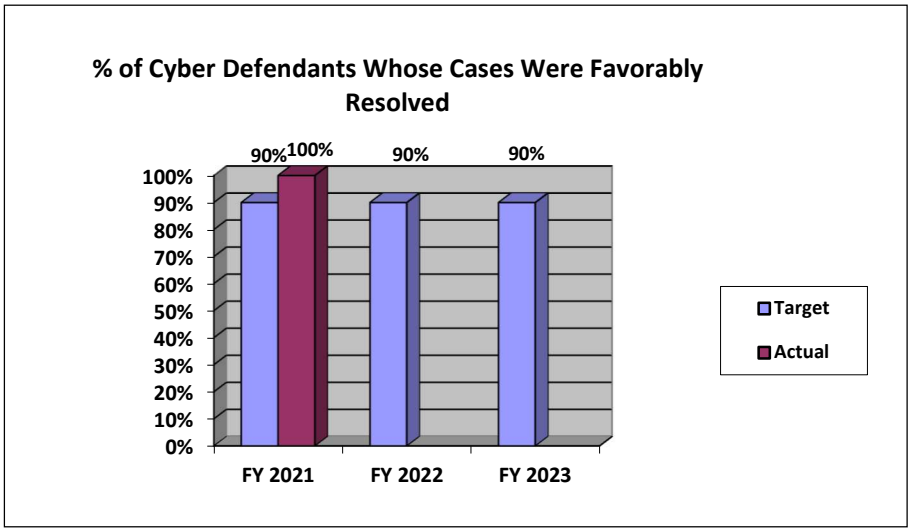


Data Definition: NSD attorneys are responsible for conducting oversight of certain activities of IC components. The oversight process involves numerous site visits to review intelligence collection activities and compliance with the Constitution, statutes, AG Guidelines, and relevant Court orders. Such oversight reviews require advance preparation, significant on-site time, and follow-up and report drafting resources. These oversight reviews cover many diverse intelligence collection programs. FISA Minimization Reviews and National Security Reviews will be counted as part of IC Oversight Reviews.
Data Collection and Storage: The information collected during each review is compiled into a report, which is then provided to the reviewed Agency. Generally, the information collected during each review, as well as the review reports, are stored on a classified database. However, some of the data collected for each review is stored manually.
Data Validation and Verification: Reports are reviewed by NSD management, and in certain instances reviewed by agencies, before being released.
Data Limitations: None identified at this time.

Objective 2.4: Enhance Cybersecurity and Fight Cybercrime

Measure: **Percentage of Cyber Defendants Whose Cases Were Favorably Resolved**
FY 2021 Target: **90%**
FY 2021 Actual: **100%**
FY 2022 Target: **90%**
FY 2023 Target: **90%**
Discussion: The FY 2023 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. Ding et al.: In July 2021, in the Southern District of California, an indictment was unsealed charging four nationals of the People's Republic of China (PRC) with a campaign to hack into the computer systems of dozens of victim companies, universities, and government entities in the United States and abroad between 2011 and 2018. The indictment alleges that much of the conspiracy's theft was focused on information that was of significant economic benefit to PRC companies and commercial sectors, including information that would allow the circumvention of lengthy and resource-intensive R&D processes. The defendants and co-conspirators sought to obfuscate the Chinese government's role in such theft by establishing a front company, Hainan Xiandun Technology Development Co. Ltd. (Hainan Xiandun), since disbanded, to operate out of Hainan Province. According to the indictment: Defendants Ding Xiaoyang, Cheng Qingmin, and Zhu Yunmin were officers in the Hainan State Security Department (HSSD), a provincial arm of China's Ministry of State Security (MSS). These HSSD officers were responsible for coordinating, facilitating, and managing computer hackers and linguists at Hainan Xiandun and other MSS front companies to conduct hacking for the benefit of China and its state-owned and sponsored instrumentalities. Targeted industries included, among others, aviation, defense, education, government, health care, biopharmaceutical, and maritime. Stolen trade secrets and confidential business information included, among other things, sensitive technologies used for submersibles and autonomous vehicles, specialty chemical formulas, commercial aircraft servicing, proprietary genetic-sequencing technology and data, and foreign information to support China's efforts to secure contracts for state-owned enterprises within targeted countries. At research institutes and universities, the conspiracy targeted infectious-disease research related to Ebola, MERS, HIV/AIDS, Marburg, and tularemia.

DarkSide: In June 2021, in the Northern District of California, DOJ announced a court-authorized operation to seize 63.7 bitcoins (valued at approximately $2.3 million). These funds represented the ransom payment from Colonial Pipeline to individuals affiliated with the group DarkSide, which had encrypted Colonial Pipeline's business network in a ransomware attack.

In May 2021, Colonial Pipeline was the victim of a highly publicized ransomware attack resulting in the company taking portions of its infrastructure out of operation. Colonial Pipeline reported to the FBI that its computer network was accessed by an organization named DarkSide, and that it had received and paid a ransom demand for bitcoins.

Microsoft Exchange Servers: In April 2021, in the Southern District of Texas, the Department of Justice announced a court-authorized operation, pursuant to Federal Rule of Criminal Procedure 41(b)(6)(B), to copy and remove malicious web shells from hundreds of vulnerable computers in the United States running on-premises versions of Microsoft Exchange Server software used to provide enterprise-level email service. Through January and February 2021, certain hacking groups exploited "zero-day" vulnerabilities in MS Exchange software to access email accounts and place web shells (pieces of code or scripts that enable remote administration) for continued access. Other hacking groups followed suit starting in early March after the vulnerability and patch were publicized. Although infected system owners successfully removed the web shells from thousands of computers, others appeared unable to do so, and hundreds of such web shells persisted unmitigated. DOJ's operation removed one early hacking group's remaining web shells, which could have been used to maintain and escalate unauthorized access to U.S. networks. The FBI conducted the removal by issuing a command through the web shell to the server, which was designed to cause the server to delete only the web shell (identified by its unique file path). The FBI provided notice of the court-authorized operation to all owners or operators of computers from which it removed hackers' web shells.

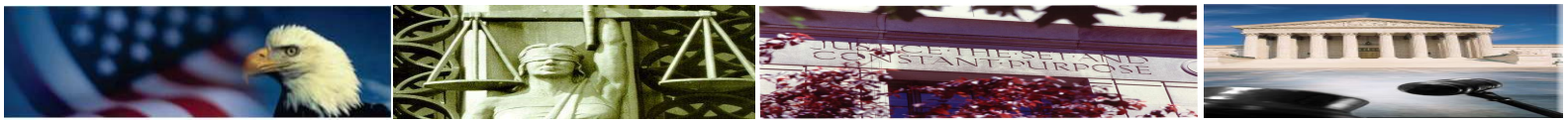
U.S. v. Hyok et al.: In February 2021, in the Central District of California, an indictment was unsealed charging three North Korean computer hackers with participating in a wide-ranging criminal conspiracy to conduct a series of destructive cyberattacks, to steal and extort more than $1.3 billion of 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).

B. Strategies to Accomplish Outcomes

NSD's performance goals support DOJ's top funding priority, Keeping our Country Safe. NSD takes a strategic, threat-driven, and multi-faceted approach to disrupting national security threats. Strategies for accomplishing outcomes within each of NSD's major programs are detailed below:

Intelligence

NSD will continue to ensure the IC is able to make efficient use of foreign intelligence information collection authorities, particularly pursuant to FISA, by representing the U.S. before the FISC. This tool has been critical in protecting against terrorism, espionage, and other national security threats. NSD will



also continue to expand its oversight operations within the IC and develop and implement new oversight programs, promote ongoing communication and cooperation with the IC, and advise partners on the use of legal authorities.

Counterintelligence and Export Control

Strategies that NSD will pursue in this area include supporting and supervising the investigation and prosecution of espionage and related cases through coordinated efforts and close collaboration with DOJ leadership, the FBI, the IC, and the 94 USAOs; overseeing and assisting with the expansion of investigations and prosecutions for unlawful export of military and strategic commodities and technology, and violations of U.S. economic sanctions; coordinating and providing advice in connection with cases involving the unauthorized disclosure of classified information and support prosecutions by providing advice and assistance with application of CIPA; and enforcing FARA and related disclosure statutes.

Foreign Investment Review

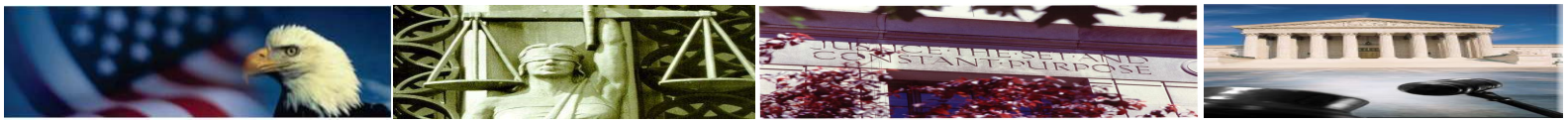
NSD will continue leading the review, investigation, and mitigation of cybersecurity, data security and privacy, telecommunications, law enforcement, and related national-security risk analyses through coordinated interagency bodies. These interagency bodies include the Committee on Foreign Investment in the United States (CFIUS), the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Team Telecom), emerging technology councils, and supply-chain regulatory bodies, such as the process established by Executive Orders 13873 and 14034 to secure the nation against national-security threats introduced via foreign investment, supply-chain compromises and vulnerabilities, and foreign participation in the U.S. telecommunications sector. NSD will continue monitoring entities subject to compliance agreements to ensure adherence to their mitigation obligations and will undertake enforcement actions when necessary and appropriate. NSD will also continue to work closely with interagency partners, including the FBI and IC, to identify strategies and priorities for its national-security reviews. In addition to leading and conducting national-security reviews of specific matters, NSD will continue its significant participation in interagency policy committees addressing issues at the intersection of technology, the law, and national security, and will continue to engage with external stakeholders in this area.

Cybersecurity

Strategies that NSD will pursue in this area include recruiting, hiring, and training additional skilled professionals to work on cyber matters; prioritizing disruption of cyber threats to the national security through the use of the U.S. Government's full range of tools, including law enforcement, diplomatic, regulatory, and intelligence methods; supporting and supervising the investigation and prosecution of national security-related computer intrusion cases through coordinated efforts and close collaboration with DOJ leadership, the FBI, the IC, other inter-agency partners, and the 94 USAOs; developing relationships with private sector entities, primarily online service or incident response providers, to increase the volume and speed of lawful threat information-sharing regarding national security cyber threats; developing relationship with foreign law enforcement entities, including prosecutors, to enable faster information sharing and foreign prosecutions and other disruptive actions that impose costs upon state-sponsored malicious cyber actors; coordinating and providing advice in connection with national security-related cyber intrusion cases involving the application of CIPA; and promoting legislative priorities that adequately safeguard national cyber security interests.

Counterterrorism

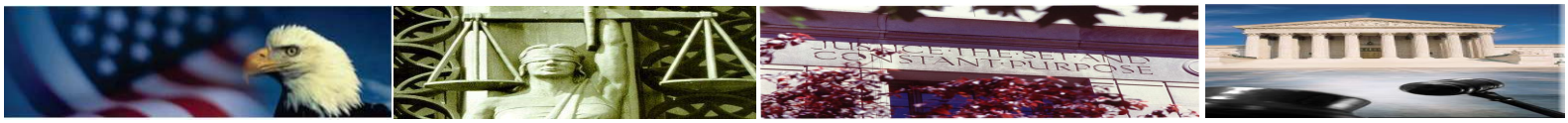
NSD will promote and oversee a coordinated national counterterrorism enforcement program, through close collaboration with DOJ leadership, the National Security Branch of the FBI, the IC, and the 94



USAOs; develop national strategies for combating emerging and evolving terrorism threats, including the threats of domestic terrorists and cyber-based terrorism; consult, advise, and collaborate with prosecutors nationwide on international and domestic terrorism investigations, prosecutions, and appeals, including the use of classified evidence through the application of the CIPA; share information with and provide advice to international prosecutors, agents, and investigating magistrates to assist in addressing international threat information and litigation initiatives; through international training programs provide capacity building for international counterparts; provide case mentoring to international prosecutors and law enforcement agents; and manage DOJ's work on counter-terrorist financing programs, including supporting the process for designating FTOs and Specially Designated Global Terrorists as well as staffing U.S. Government efforts on the Financial Action Task Force. NSD will continue to co-chair the Attorney General's Domestic Terrorism Executive Committee. In addition, to increase national-level coordination on the evolving domestic terrorism threat, NSD is adding a domestic terrorism unit within the Division's Counterterrorism Section.

C. Priority Goals

Not applicable. NSD is not a reporting component for DOJ's Priority Goals.



V. Program Increases by Item

1. Counterintelligence and Export Control, including Countering Cyber Threats to our National Security

Strategic Goal:	Goal 2: Keep our Country Safe
Strategic Objective:	Objective 2.4: Enhance Cybersecurity and Fight Cybercrime
Budget Decision Unit(s):	National Security Division
Organizational Program:	Counterintelligence and Export Control Section (CES)
Program Increase:	Positions 6 Atty 6 FTE 3 Dollars $1,362,000

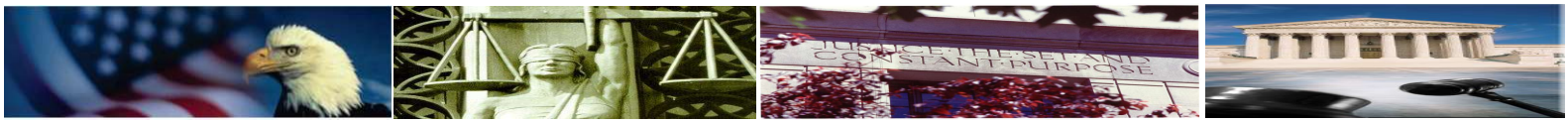
Description of Items

NSD requests 6 attorneys and $1,362,000 for its Counterintelligence and Export Control Section (CES). These new attorney positions will be dedicated to CES's work related to countering cyber threats to our national security.

Justification

Foreign nation states increasingly use cyber-enabled means to steal export-controlled technology, trade secrets, intellectual property, and personally identifying information, exert malign influence, and hold our critical infrastructure at risk to destructive or disruptive attacks. Several such states have also established themselves as safe havens for cybercriminals who have engaged in such activity, including ransomware attacks and digital extortion, for personal profit, a challenge which the Administration recognizes has grown into a national security priority.

In recent years, NSD has led a transformation in the Federal Government's response to significant cyber incidents by using traditional law enforcement tools to investigate and, in many instances, develop prosecutable cases against state actors and their proxies, arresting and prosecuting them where possible. Even when arrest is unlikely, NSD prioritizes the disruption of criminal activity that poses a threat to national security through other legal tools like legal seizure of infrastructure and targeted sharing of unclassified threat intelligence gathered as a result of NSD's criminal investigations. That threat intelligence has provided the basis for our own court-authorized disruption operations (such as botnet takedowns); enabled other government agencies' tools (such as technical operations, sanctions, trade remedies, and diplomatic efforts to rally like-minded countries); educated the American public about cyber threats; empowered network defenders and encouraged victim reporting and cooperation. Moreover, owing to the safe haven challenges mentioned above, the line between purely criminal cases and national security investigations implicating ties to foreign governments has blurred in recent years, requiring NSD to devote increasing resources to investigating the ties between criminal actors and foreign intelligence services and supporting the Criminal Division in otherwise criminal cases (such as the recent recovery of 85% of the ransom that Colonial Pipeline paid). Our ability to respond to significant incidents and develop criminal cases, other disruption options, and threat intelligence depends on attorney resources, however, and those investigations must be balanced against other, high-priority counterintelligence investigations



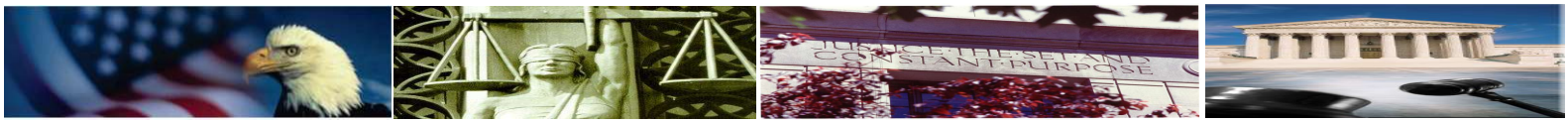
(namely, malign foreign influence, espionage, theft of trade secrets, non-traditional collectors, and proliferation) that compete for the same attorney resources.

NSD requires additional dedicated resources to address the above-described cyber threats for several reasons, including:

(1) In addition to the extraterritorial evidential challenges present in almost every significant cyber matter, national security cyber investigations often implicate foreign policy ramifications and U.S. Intelligence Community (USIC) and Department of Defense (DOD) equities. These considerations add additional time, planning, and coordination requirements, at a minimum, and can make it even less certain whether the investigation, which can easily span several years, will lead to criminal charges or other disruptive actions. Given other pressing criminal justice priorities, USAOs can be hesitant to devote resources to such investigations, especially in the early stages when it is least clear whether the investigation will result in a prosecutable case. Accordingly, NSD attorneys typically take the lead (or at least work jointly with AUSAs) during such investigations.
(2) Due to their pace, complexity (including the ephemeral nature of digital evidence), international scope, data and legal process-intensive nature, and public profile, national security cyber investigations often require multiple prosecutors to devote the majority of their time during the investigation period to engage with the victims and their counsel, support the FBI, liaise with the USIC, DOD, other departments and agencies, marshal the evidence, and prepare charges or other disruptive actions.
(3) In response to increased malign cyber activities by various foreign nation state actors and their proxies, the Department has, among other steps, established the National Security Cyber Specialists Network, the Ransomware and Digital Extortion Task Force, recently launched the Strategy for Countering Nation-State Threats, prioritized proactive disruptive actions, and placed other demands on NSD to respond to the cyber threat.

To better address the increasing caseload of significant cyber matters, NSD would commit the six (6) attorneys to work almost exclusively on cyber investigations, prosecutions, and disruption operations. Responsibilities would include:

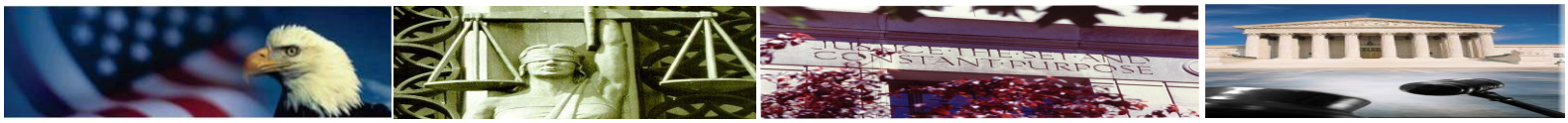
- managing a portfolio of national security cyber investigations, including by drafting prosecution memoranda and criminal charges or other legal process; engaging with victims and witnesses; conducting discovery reviews; pursuing arrest and extradition; conducting hearings and trials; and otherwise working with federal prosecutors and agents around the country in those tasks;
- identifying and securing lawful access to sources of digital evidence/threat intelligence, including by drafting legal process;
- providing legal and strategic advice and guidance to other prosecutors and law enforcement officers;
- providing training to other prosecutors and law enforcement officers;
- serving as a liaison to the IC, DOD, State Department, and other inter-agency partners;



- advising NSD and Department leadership regarding options to disrupt cyber threats to the national security;
- working with the USAOs, investigative and regulatory agencies, IC, DOD, and other departments and agencies to implement a whole-of-government approach to investigating and disrupting cyber threats to national security, including through prosecution, technical operations, economic sanctions, and diplomatic efforts; and
- working with the private sector to develop a whole-of-society approach to disrupting cyber threats and empowering network defenders.

Impact on Performance

The above requests will allow NSD to keep up with the expected increase in cyber investigations and prosecutions.



Funding

1. Base Funding

FY 2021 Enacted				FY 2022 President's Budget				FY 2023 Current Services			
Pos	Atty	FTE	Amount ($000)	Pos	Atty	FTE	Amount ($000)	Pos	Atty	FTE	Amount ($000)
49	36	41	$14,102	49	36	42	$14,604	49	36	42	$14,921

2. Personnel Increase Cost Summary

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2023 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Attorneys (0905)	6	$227	$46	($1)	$1,362	$276	($6)
Total Personnel	**3**	**$227**	**$46**	**($1)**	**$1,362**	**$276**	**($6)**

3. Non-Personnel Increase Cost Summary

Non-Personnel Item	FY 2023 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Not Applicable	$0	$0	0	$0	$0
Total Non-Personnel	**$0**	**$0**	**0**	**$0**	**$0**

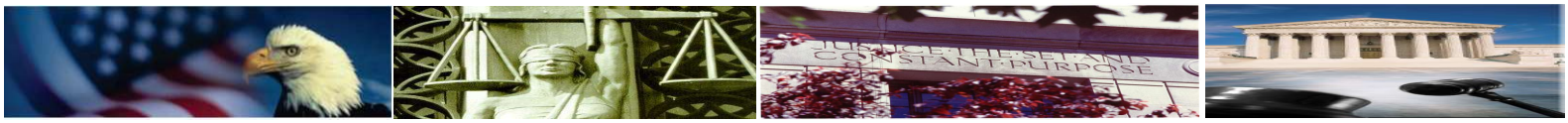
4. Justification for Non-Personnel Annualizations: N/A

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Atty	FTE	Personnel	Non-Personnel	Total	FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Current Services	49	36	42	$14,921	$0	$14,921	$0	$0
Increases	6	6	3	$1,362	$0	$1,362	$276	($6)
Grand Total	**55**	**42**	**45**	**$16,283**	**$0**	**$16,283**	**$276**	**($6)**

6. Affected Crosscuts

Counterterrorism, Cyber, Intelligence and Information Sharing, National Security



2. Intelligence Oversight

Strategic Goal:	Goal 2: Keep our Country Safe
Strategic Objective:	Objective 2.2: Counter Foreign and Domestic Terrorism
Budget Decision Unit(s):	National Security Division
Organizational Program:	Office of Intelligence (OI)
Program Increase:	Positions 8 Atty 5 FTE 4 Dollars $1,551,000

Description of Item

NSD requests eight positions (5 attorneys, 2 management and program analysts, and 1 legal administrative assistant) and $1,551,000 for its Office of Intelligence (OI) Oversight Section.

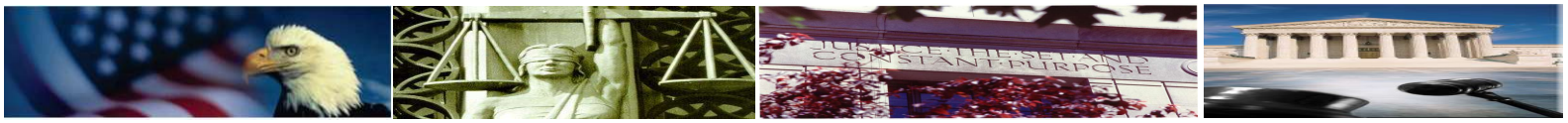
Justification

This portion of the budget request directly supports the Attorney General's top funding priority "Keeping Our Country Safe" and will 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 2023. The increase in oversight-related work that necessitates additional positions is described below.

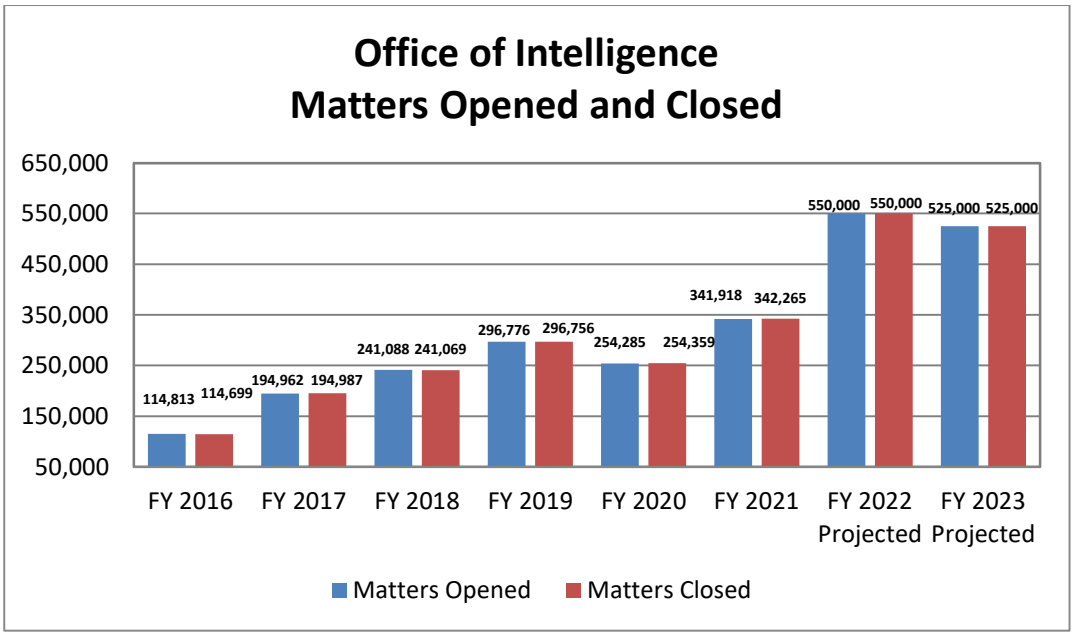
OI serves a critical role in DOJ's effort to prevent acts of terrorism and cyber-attacks and to thwart hostile foreign intelligence activities. OI ensures that: 1) IC agencies have the legal authorities necessary to conduct intelligence operations, particularly operations involving FISA; 2) OI exercises 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 2016 and FY 2021, OI experienced a roughly 198% 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. While the number of matters handled in FY 2020 fell, the FY 2020 number was still higher



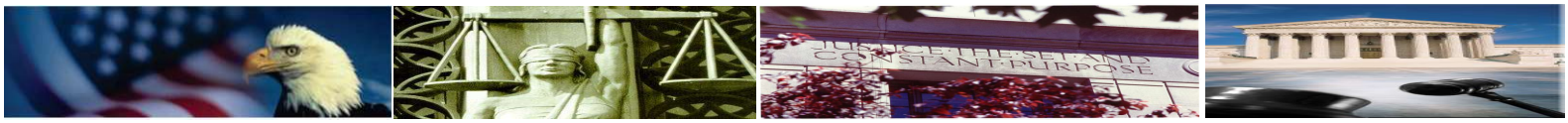
than the number of matters handled in FY 2018. Further, the number of matters handled exceeded pre-pandemic levels in FY 2021. The vast majority of the matters opened and closed that are represented in the below chart reflect the resources dedicated to OI's oversight responsibilities. The number of FISA applications handled by OI is not included in the number of matters opened and closed and are separately measured by OI.[3] 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. Prior to the COVID-19 pandemic, the number of Section 702 targets steadily increased. Between CY 2014 and CY 2019, the number of Section 702 targets increased roughly 121% from 92,707 to 204,968. The number of targets reported for CY 2020 was just below the number of targets reported for CY 2019; this slight decrease was likely due to the COVID-19 pandemic, and NSD anticipates that the upward trend will resume in CY 2022. The number of targets for CY 2021 is not yet declassified, but it will exceed the CY 2019. OI also

3 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.



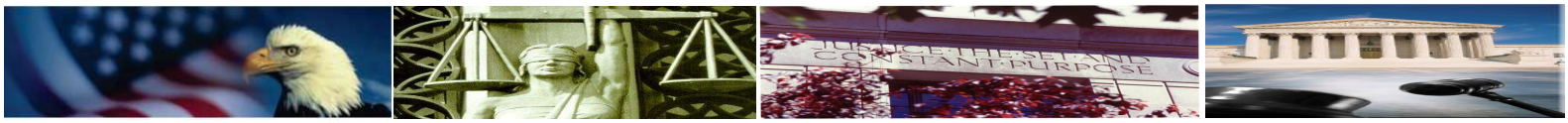
has experienced steady increases in the number of potential Section 702 incidents reported by the IC. OI dedicates substantial resources to investigating each such potential incident reported by the IC or otherwise identified by OI. OI also dedicates resources to ensure the IC properly remediates compliance incidents. OI must report the details of each Section 702 compliance incident to the FISC and to Congress. Between CY 2016 and CY 2019, the number of potential Section 702 incidents reported to OI increased 123%. While the number of potential incidents reported fell in CY 2020, this number returned to pre-pandemic levels by the end of 2021 and OI expects that the yearly increases in such compliance investigations by OI will continue in 2022 All of these reported potential incidents required dedicated OI resources to investigate the potential incidents. 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 is necessary to sustain a broader and more robust query oversight program. Over the last several years, OI has had to dedicate significant resources to these query audits, including post audit investigation and reporting.

In addition, OI expects that its oversight of the Section 702 program will continue to grow as the program expands to address the foreign intelligence priorities of the IC. By FY 2023, OI expects that it will need additional resources to oversee the IC's increased use of Section 702.

In light of the statistics provided above, NSD OI has established a record of experiencing a year-over-year increase in matters handled by the office's Oversight Section, particularly related to its oversight of the IC's implementation of Section 702. The substantial growth of NSD's Section 702 oversight program and the resulting impact on NSD's resources is also apparent from the over 400% increase in the number of matters handled by OI between FY 2014 and FY 2021. A drop experienced during 2020 was an anomaly to the severe staffing limitations at IC agencies as a result of the COVID-19 pandemic. As most IC agencies have returned to near full staffing and are expected to continue such staffing levels through 2022 and 2023, NSD must account for the ongoing, steady growth in such workload year-over-year.

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, and as noted in NSD's FY 2022 budget request , NSD OI has begun implementation of a new oversight initiative to ensure that applications submitted to the FISA Court contain all information relevant to the court's consideration of those applications. For example, OI expanded its oversight of FBI FISA applications to include completeness reviews and conducted completeness reviews of 130 FISA applications between May 2020 and January 2022. As that program has developed over the past year, OI has determined that the program is more resource intensive than initially expected. The increased staffing request for 2023 also accounts for the larger than expected burden arising from

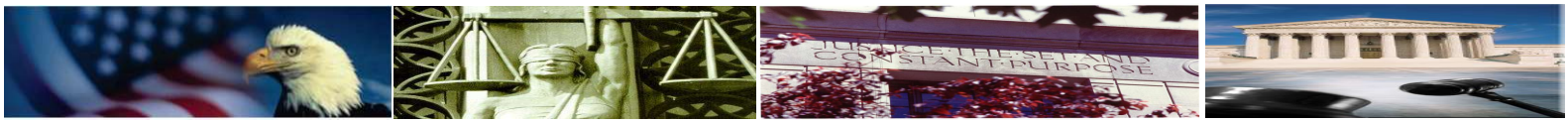


this important oversight program. In a white paper published in June 2021, the then Chairman of the Privacy and Civil Liberties Oversight Board (PCLOB) discussed the resource burdens involved in NSD's FISA-related oversight. This white paper examined certain FISA applications that had been audited by the OIG. As the Chairman found, OI's accuracy and completeness reviews are "important in ensuring the integrity of the FISA process." White Paper at 14.

In addition, in August 2020, the former Attorney General issued a memorandum to the FBI requiring the FBI to augment its internal compliance functions for its national security activities. The FBI is working to implement the requirements and has begun certain audits of its national security activities. NSD OI has, and will continue to, work closely with FBI as it works to establish robust internal oversight programs through program advice, training, and reporting. NSD OI reasonably expects that as FBI's internal oversight programs further develop and as FBI conducts FISA-related audits, this will impact NSD OI's oversight resources because of the compliance-related investigation, reporting, and trends analysis that will come from those audits.

Impact on Performance

For the above additional oversight programs and to keep pace with the increasing oversight demands that the IC's utilization of Section 702 is placing on OI, OI will need five additional attorneys, two management and program analysts, and one additional legal administrative assistant. 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. With these additional resources, NSD will 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.



Funding

1. Base Funding

FY 2021 Enacted				FY 2022 President's Budget				FY 2023 Current Services			
Pos	Atty	FTE	Amount ($000)	Pos	Atty	FTE	Amount ($000)	Pos	Atty	FTE	Amount ($000)
138	109	115	$40,610	151	119	123	$44,476	151	119	129	$46,045

2. Personnel Increase Cost Summary

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2023 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Attorneys (0905)	5	$227	$46	($1)	$1,135	$230	($5)
Management and Program Analyst (0300-0399)	2	$144	$54	$4	$288	$108	$8
Legal Admin. Assistant (0300-0399)	1	$128	$66	$5	$128	$66	$5
Total Personnel	**8**	**$499**	**$166**	**$8**	**$1,551**	**$404**	**$8**

3. Non-Personnel Increase Cost Summary

Non-Personnel Item	FY 2023 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Not Applicable	$0	$0	0	$0	$0
Total Non-Personnel	**$0**	**$0**	**0**	**$0**	**$0**

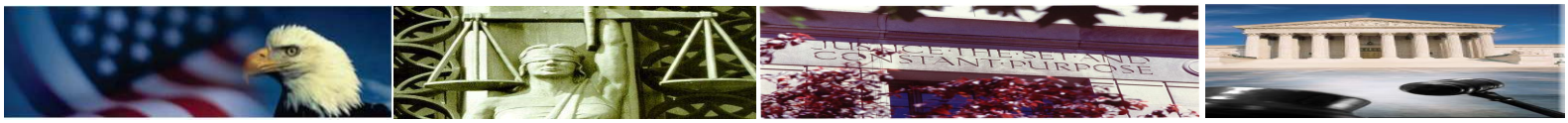
4. Justification for Non-Personnel Annualizations: N/A

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Atty	FTE	Personnel	Non-Personnel	Total	FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Current Services	151	119	129	$46,045	$0	$46,045	$0	$0
Increases	8	5	4	$1,551	$0	$1,551	$404	$12
Grand Total	**159**	**124**	**133**	**$47,596**	**$0**	**$47,596**	**$404**	**$12**

6. Affected Crosscuts

Counterterrorism, Intelligence and Information Sharing, National Security



3. Counterterrorism, including domestic terrorist threats

Strategic Goal:	Goal 2: Keep our Country Safe
Strategic Objective:	Objective 2.2: Counter Foreign and Domestic Terrorism
Budget Decision Unit(s):	National Security Division
Organizational Program:	Counterterrorism Section (CTS)
Program Increase:	Positions 5 Atty 2 FTE 2 Dollars $1,825,000

Description of Item

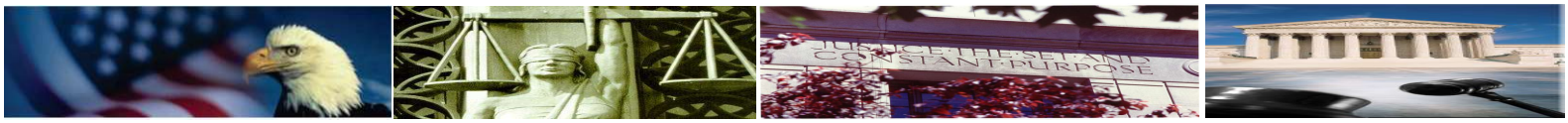
NSD requests five positions (two attorneys, one program and management analyst, and two administrative support positions) and $1,075,000 for a new case tracking system, for a total of $1,825,000, for its Counterterrorism Section (CTS).

Justification

These additional resources are needed to support combating terrorism, including the on-going domestic terrorism (DT) threat. As the threats facing this nation have become increasingly complex, and with the potential for lone wolf attacks, the Division takes an all-tools approach to disruption, which includes, among other things:

- Investigation and prosecution;
- Providing legal and policy support for partner agencies' counterterrorism disruption operations;
- Monitoring trends through review of investigations and prosecutions and tracking cases from initiation to conclusion;
- Providing support to international partners, particularly encouraging and supporting nations confronted with the return of foreign fighters from Iraq and Syria, which lead to more convictions of dangerous terrorists, putting them in prison and limiting their ability to engage in future attacks against U.S citizens and interests; and
- Managing cross-cutting and complex policy projects, including those related to combating terrorist financing, counterterrorism strategy and operations, National Security Council engagement, and international capacity building.

In March 2021, the IC released an assessment that highlighted the rising threat of DT activity. In May 2021, the FBI and DHS released, for the first time, a strategic intelligence assessment of DT activity. They noted concern over the rise DT activity. As part of the Department's ongoing efforts to prevent and disrupt terrorist activity, CTS provides a full spectrum of support to the FBI and USAOs on cases across the country with a nexus to DT or domestic violent extremism (DVE). In addition, in March 2021, the Department issued a directive to all USAOs requiring additional oversight of DT/DVE-related cases by CTS, as well as tasking CTS with new case tracking requirements, which will necessitate the creation and ongoing maintenance of an entirely new case management and tracking system with enhanced access controls and robust data analytics capabilities to support DT/DVE-related case tracking.



In addition, in January 2022, the Assistant Attorney General for National Security announced that NSD would form a new DT unit within CTS. The unit will focus on the threat from DT and DVE and will be comprised of personnel with subject matter expertise who will be primarily responsible for working with USAOs in investigating and prosecuting significant DT and DVE cases, coordinating DT and DVE-related lines of effort within the Department and with other departments and agents, and designing training and guidance in these areas for federal prosecutors and state and local law enforcement partners. The unit will also be responsible for tracking DT/DVE-related cases and trends across the country and assisting in the implementation of the President's DT strategy. For these reasons CTS must devote additional resources to this critical threat.

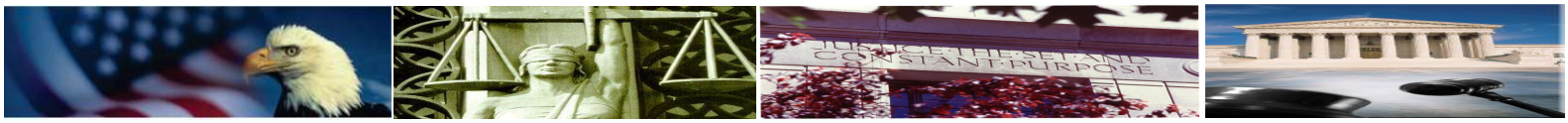
CTS provides assistance to foreign governments prosecuting returning foreign terrorist fighters, and supports interagency partners, particularly the Department of Defense, with the use of battlefield collected evidence for use in terrorism investigations and prosecutions. Separately, CTS is frequently asked to assist foreign governments in capacity-building efforts and to directly assist foreign prosecutions even where there is no U.S. nexus. Improving the capacity of foreign partners to prosecute terrorism is an important part of the national security mission, and NSD anticipates devoting more resources to these engagements in the coming years as the global terrorism threat increases.

Finally, in the past two years there has been an increase in motions practice and litigation relating to certain intelligence tools and programs, in addition to routine work to ensure the appropriate use and protection of classified information in support of counterterrorism efforts. CTS has successfully litigated the use of information acquired pursuant to FISA. CTS is also responsible for the ATAC program and acts as initial point of contact with the field on all national security related inquiries. As national security threats and classified litigation have both increased, CTS requires additional resources devoted to this important coordination role. It is also important to note that CTS has provided, and with adequate resources, plans to continue to provide significant assistance to hundreds of investigations and prosecutions stemming from the January 6th U.S. Capitol breach. And, of course, our focus on international terrorism remains high. The threats our country faces from international and domestic terrorism are daunting and CTS needs the requested resources to contribute to the Department's overall efforts to combat them.

The two requested attorneys will be integral to CTS's ability to keep pace with the growing and evolving terrorism threat. CTS requires additional personnel resources to support its wide range of activities and responsibilities. Specifically, additional non-attorney positions will enhance the investigatory and case support capabilities available to attorneys and ensure the full utilization of the case management and tracking system that will be deployed in CTS:

- **1 Program and Management Analyst** to support case tracking requirements, including the creation of reports on trends related to DT/DVE-related cases, as well as ongoing operation and maintenance of the case tracking system for DT/DVE-related cases;

- **2 Administrative Support Positions** to support the attorneys on a daily basis with a wide range of projects to ensure that attorney resources are not expended inefficiently on administrative and clerical support tasks.



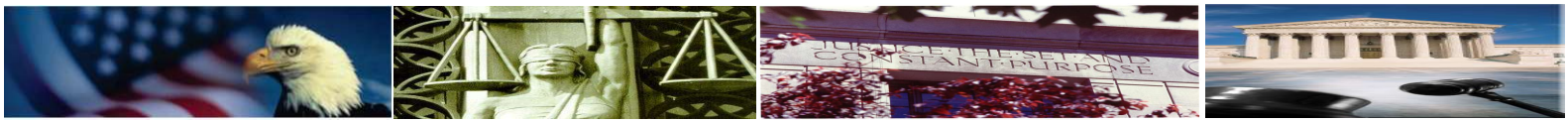
Case Management System on JCON-Unclassified System

CTS will also require additional information technology resources to establish on the Department's JCON-Unclassified system a case management tracking and reporting system with enhanced access controls to support DT/DVE-related case tracking. The following chart lays out the expected initial and ongoing costs for the creation and maintenance of the system.

Item	Description	Estimated Cost (first year)	Estimated FY 24 – 25 Cost
Software / Platform	Covers the cost of the software and licensing, security, cloud platform, and the completion of development/testing	$425,000	$260,000
Analytics / Visualization	Supports reporting, visualizations, analytics, etc.	$100,000	$50,000
Build Resources	Contractor support resources committed to implementing, configuring, and building functions within the selected software	$275,000	
Steady State Resources	Contractor support resources committed to continued support operations, configurations, and changes to the selected software	$200,000	
Compliance / ATO	Contractor support resources committed to support the initial Authority to Operate (ATO) (required for all USG Information Systems)	$75,000	
	TOTAL	**$1,075,000**	**$310,000**

Impact on Performance

With these additional increases, NSD will meet the new and evolving threats posed by DT and DVE. These positions are the driving force behind NSD's efforts to prevent, detect, deter, and prosecute terrorist activities.



Funding

1. Base Funding

FY 2021 Enacted				FY 2022 President's Budget				FY 2023 Current Services			
Pos	Atty	FTE	Amount ($000)	Pos	Atty	FTE	Amount ($000)	Pos	Atty	FTE	Amount ($000)
64	51	54	$18,606	64	51	54	$19,093	64	51	54	$19,506

2. Personnel Increase Cost Summary

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2023 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Attorneys (0905)	2	$227	$46	($1)	$454	$92	($2)
Program Management Analyst (0300-0399)	1	$128	$66	$5	$128	$66	$5
Admin. Assistant (0300-0399)	2	$84	$15	$7	$168	$30	$14
Total Personnel	**5**	**$439**	**$127**	**$11**	**$750**	**$188**	**$17**

3. Non-Personnel Increase Cost Summary

Non-Personnel Item	FY 2023 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Case Management System	$1,075	$1,075	1	($890)	($60)
Total Non-Personnel	**$1,075**	**$1,075**	**1**	**($890)**	**($60)**

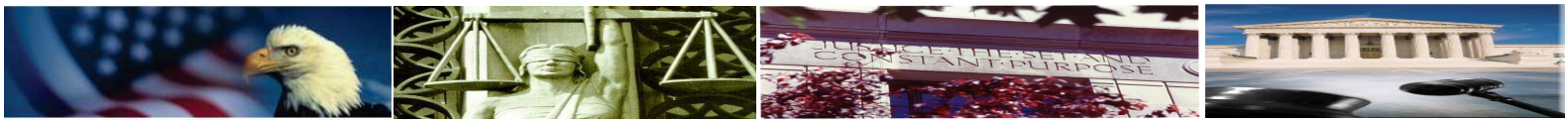
4. Justification for Non-Personnel Annualizations: As described above, anticipated out-year costs total $310,000. This includes $260,000 for software, security, and cloud platform as well as $50,000 for reporting, visualization, analytics, etc.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Atty	FTE	Personnel	Non-Personnel	Total	FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Current Services	64	51	54	$19,506	$0	$19,506	$0	$0
Increases	5	2	2	$750	$1,075	$1,825	($702)	($43)
Grand Total	**69**	**53**	**56**	**$20,256**	**$1,075**	**$21,331**	**($702)**	**($43)**

6. Affected Crosscuts

Counterterrorism, Cyber, Intelligence and Information Sharing, National Security, Domestic Terrorism



4. Remote Classified (Secret) Processing

Strategic Goal:	Goal 2: Keep our Country Safe
Strategic Objective:	Objective 2.1: Protect National Security Objective 2.2: Counter Foreign and Domestic Terrorism Objective 2.4: Enhance Cybersecurity and Fight Cybercrime
Budget Decision Unit(s):	National Security Division
Organizational Program:	Executive Office (EO)
Program Increase:	Positions 0 Atty 0 FTE 0 Dollars $2,405,000

Description of Items

In FY 2023, NSD requests $2,405,000 for the implementation of remote classified (Secret) processing.

Justification

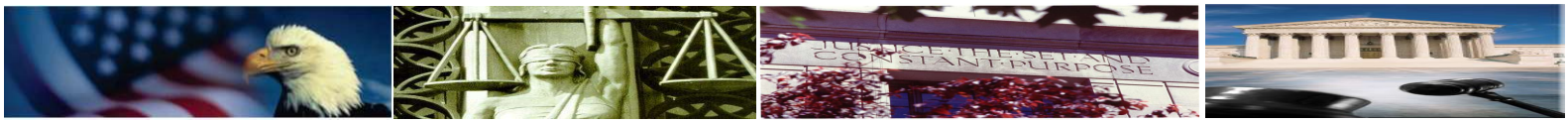
The remote Secret services would provide classified support during times of mandated social distancing, natural disasters in Washington, DC, or other events preventing employees from accessing sites in the National Capital Region, or for employees during mission-essential travel activities. Because the vast majority of our operational work with the FBI occurs via a classified network, we anticipate that NSD personnel working cases with them (including CES, CTS, OI, and FIRS) would all make heavy operational use of this system. The cases involve many of the Department's priorities including cyber and domestic terrorism investigations and prosecutions.

Specifically, examples of the anticipated use of the remote classified (Secret) capability include but are not limited to:

a. CIPA briefings (in some cases supporting activities across multiple time zones; supports operational flexibility);
b. FISA use requests processing (supporting the US Attorneys' Offices);
c. Cyber-related case support, including direct connection with FBI agents on operational actions (e.g. warrants, etc.); and
d. Classified operations of NSD's FIRS, including its work CFIUS and Executive Orders 13913 and 13873.

This remote classified processing would also provide NSD leadership with the capability to connect with the Deputy Attorney General's Office and other operational partners supporting NSD mission objectives.

Specific resource needs include:



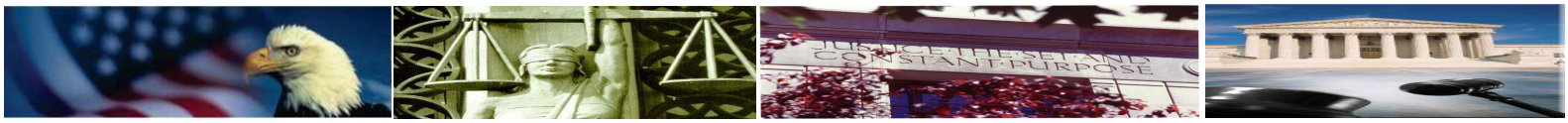
Item	Description	FY 2023 Estimated Cost	FY 2024 Estimated Cost	FY 2025 Estimated Cost	FY 2026 Estimated Cost
Implementation Resources	Contractor and equipment resources committed to deployment, implementing, configuring, functions for the remote Secret processing capability.	$2.0M	NA	NA	NA
User Devices[1]	Equipment used by the user to connect to the Secret network. Device/equipment costs are estimated $15,000 per unit.	$375,000 25 units at $15,000 each	NA	NA	$412,500 25 units at $16,500 – based on an estimated 10% cost increase per unit
Maintenance & Support[2]	Contractor resources committed to the maintenance & support of the solution.	NA	$475,000	$475,000	$475,000
Compliance / ATO	Contractor resources committed to support the initial Authority to Operate (ATO) (required for all USG Information Systems)	$30,000	NA	NA	NA
	TOTAL	**$2.405M**	**$475,000**	**$475,000**	**$887,500**

[1]In the interest of budget constraints, NSD is requesting 25 devices only to be pooled for use based on mission-critical needs. The costs would be considerably higher if NSD were to request devices for all available users.

[2]Based on an estimation of 20% of the overall solution cost (minus ATO costs).

Impact on Performance

As described above, this request would allow NSD to stand up remote classified processing, which directly supports the Administration's Executive Order 14028, Improving the Nation's Cybersecurity, as well as the Attorney General's top funding priority, "Keeping Our Country Safe."



Funding

5. Base Funding

FY 2021 Enacted				FY 2022 President's Budget				FY 2023 Current Services			
Pos	Atty	FTE	Amount ($000)	Pos	Atty	FTE	Amount ($000)	Pos	Atty	FTE	Amount ($000)
0	0	0	$0	0	0	0	$0	0	0	0	$0

6. Personnel Increase Cost Summary

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2023 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Not Applicable							
Total Personnel							

7. Non-Personnel Increase Cost Summary

Non-Personnel Item	FY 2023 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Remote Classified (Secret) Processing	$2,405	$2,405	1	($1,930)	$0
Total Non-Personnel	**$2,405**	**$2,405**	**1**	**($1,930)**	**$0**

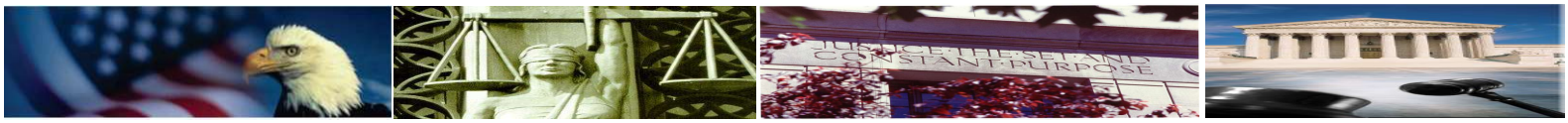
(2) **Justification for Non-Personnel Annualizations**: As described above, anticipated out-year costs total $1,837,500. This includes $475,000 annually for maintenance and an additional $412,500 in BY+3 for technology refresh.

(3) **Total Request for this Item**

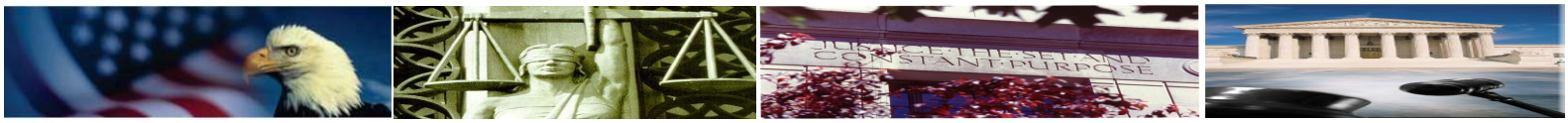
Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Atty	FTE	Personnel	Non-Personnel	Total	FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Current Services	0	0	0	$0		$0	$0	$0
Increases	0	0	0	$0	$2,405	$2,405	($1,930)	$0
Grand Total	**0**	**0**	**0**	**$0**	**$2,405**	**$2,405**	**($1,930)**	**$0**

Affected Crosscuts

Counterterrorism, Intelligence and Information Sharing, National Security



V. Program Offsets by Item (Not Applicable)



VI. EXHIBITS