FY 2024
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 keep our country safe by protecting national security, countering foreign and domestic terrorism, and enhancing cybersecurity and fighting cybercrime, which are among the Department of Justice's (DOJ) top strategic priorities. NSD requests for Fiscal Year (FY) 2024 a total of 456 positions (including 308 attorneys), 375 full-time equivalents (FTE), and $144,788,000.[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 using 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);

[1] Within the totals outlined above, NSD has included a total of 26 positions, 26 FTE, and $22,288,000 for Information Technology (IT).

- Counterterrorism Section (CTS);
- 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 94 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 94 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 counterterrorism financing programs, including supporting the process for designating Foreign Terrorist Organizations and Specially Designated Global Terrorists, as well as staffing United States Government efforts on the Financial Action Task Force.

3. Foreign Investment, Telecommunications, and Technology Supply Chains.

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

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

- Monitoring certain intelligence and counterintelligence activities of the 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.

5. Victims of Overseas Terrorism.

- Supporting United States citizen victims of overseas terrorism 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 United States 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.

6. **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 regarding 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.** Since 2020, DOJ charged more than 475 individuals for foreign fighter, domestic terrorism-related, and international terrorism-related conduct. These cases include, among others, individuals inspired by the Islamic State in Iraq and Syria (ISIS) to plot violent acts in the United States, but who were arrested before leaving the United States or disrupted before they could act, 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. Relevant counterterrorism case examples are detailed on pages 37-40.

- **January 6 – Capitol Riot Investigation.** In connection to the breach of the United States Capitol on January 6, 2021, about 500 individuals have pleaded guilty to a variety of federal charges, from misdemeanors to felony obstruction, many of whom have or will face incarceration at sentencing (as of February 7, 2023). Relevant case examples related to January 6th are detailed on pages 40–42.

- **Espionage Enforcement.** NSD continued its enforcement of the Espionage Act and Economic Espionage Act by successfully prosecuting defendants for espionage offenses. Relevant counterespionage/counterintelligence case examples are detailed on page 29.

- **Combatting Foreign Malign Influence.** NSD significantly increased its efforts to combat foreign malign 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. In 2021, the number of new registrants reached the second highest level 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. Furthermore, 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. Relevant foreign malign influence case examples are detailed on pages 31–33.

- **Export Controls and Sanctions Enforcement.** NSD continues its rigorous enforcement of export controls and sanctions, including sanctions against Russia, Iran, China, and North Korea. Relevant export control and sanction enforcement case examples are detailed on pages 30-31.

- **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 United States national security through cyber intrusions and attacks. Relevant national security cyber case examples are detailed on pages 46-48.

- **Foreign Interference in United States Elections.** NSD played a significant role in developing policies and decision frameworks to address foreign interference in United States elections. Working with the NSC and other agencies, NSD helped develop and implement Executive Order 13848, *Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election*, including helping develop sanctions pursuant to the Executive Order. 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. For example, 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 engagement in foreign-investment review supports DOJ's Strategy for Countering Nation-State Threats as well as NSD's responsibilities to enhance national security and counter foreign adversaries trying to steal, spy on, and sabotage key United States assets and technology.

    - NSD reviewed approximately 22% more submissions overall in FY 2022 than in FY 2021 regarding mergers, acquisitions, and investments. NSD is again on track to review 15% more submissions in FY 2023 than FY 2022;

    - NSD led approximately 25% of the cases in which a Joint Voluntary Notice was filed with CFIUS in FY 2022, which was approximately 14% more co-led cases and 26% higher overall number of cases than in FY 2021. In approximately 36% of DOJ co-lead cases closed, 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. Out of all CFIUS cases mitigated, DOJ co-lead 44% of such cases;

    - NSD also led (on behalf of DOJ) approximately 26% (up from 292% since FY 2020) 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);

    - NSD represents the Attorney General in his formal role as the chair of Team Telecom as required under Executive Order 13913, 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:

        - While Team Telecom reviewed 23% fewer applications in FY 2022 than in FY 2021, NSD led or co-led 100% of the reviews for FCC referrals to Team Telecom for applications for licenses; and

        - Team Telecom recommended in FY 2022 to the FCC that 83% of the reviewed applications (stemming from 52 applications the FCC referred that involved a total of 109 telecommunications authorizations, cable landing licenses, and petitions for declaratory ruling) be granted contingent on mitigation measures. NSD either led or co-led these cases.

    - NSD led the Executive Branch's participation in the FCC's Show Cause proceedings against four United States subsidiaries of People's Republic of China state-owned telecommunications firms (i.e., China Telecom, China Unicom, Pacific Networks, and ComNet), and in 2021 filed multiple responses, on behalf of Team Telecom, 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 each of these licenses. Accordingly, in October 2021 and January 2022, the FCC Commissioners voted to revoke and terminate China Telecom and China Unicom's licenses, respectively;

- In October 2022, NSD led Team Telecom's first full recommendation to the FCC to deny a subsea cable landing license. The owners of the existing ARCOS-1 cable system sought a modification of their cable landing license to include a new spur to directly connect the United States to Cuba. The cable would have landed in a landing station owned directly by the Cuban government and the capacity on the cable would have been leased entirely to the Cuban government's state-owned telecommunication firm (ETECSA). The proposed modification raised significant counterintelligence concerns regarding the Cuban government's ability to collect traffic transiting the cable, the Cuban government's growing relationship with foreign adversaries such as China and Russia, and the potential for the malicious actors to drive non-Cuban bound data through Cuba using the new spur. After delivering the recommendation to the FCC, the owners withdrew their application from FCC consideration.

- NSD continues to provide significant assistance to the Department of Commerce in administering and implementing Executive Order 13873, "Securing the Information and Communications Technology and Services (ICTS) Supply Chain" authority as well as the OMB-led Federal Acquisition Security Council (FASC) in administering its SECURE Technology Act authority. Both fora were established to address both the Government's and the private sector's exposure to national security risk through the United States ICTS supply chain. Since 2021, NSD submitted six referrals to the Secretary of Commerce which identify 14 companies of concern for investigation, as well as two referrals to the FASC identifying four companies of concern for investigation. To date, NSD remains the only United States government entity to make a referral pursuant to these new authorities and is currently developing additional referrals for Commerce and FASC review. NSD also continues to explore additional supply chain security related authorities, to include the FCC's Secure and Trusted Communications Network Act (STCNA) Covered List, that it can leverage to address the risk associated with certain foreign owned or controlled technology firms;

- NSD led 83 CFIUS cases and 109 Team Telecom cases in 2021 that resulted in 41 new national security agreements that NSD negotiated and entered with companies, and that NSD will monitor for compliance going forward. NSD also conducted 37 in-person or virtual mitigation compliance site visits in FY 2022 (184% increase from FY 2021) to monitor companies' compliance. The total number of such agreements monitored by NSD is currently around 190, which reflects an approximate 68% increase in complex mitigation matters and agreements from FY 2021 to FY 2022. This significant increase in the total number of active agreements occurred despite terminating 32 agreements in FY 2021 and 22 agreements in FY 2022 as part of NSD's ongoing initiative to reassess all lower-risk mitigation agreements and end ones that were no longer necessary; and

- In FY 2022, NSD helped promulgate the first CFIUS enforcement guidelines. These guidelines, adopted by CFIUS in FY 2023, provide the regulated public with information about how CFIUS assesses violations of the laws and regulations that govern CFIUS parties.

- **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 2021, the number of Section 702 targets increased roughly 150%. 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 FBI field offices 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 Oversight of FISA.** The NSD and FBI 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). As part of these measures, OI conducts accuracy and completeness reviews of FBI FISA applications to determine whether the applications contain any errors or omissions of material fact. OI conducted numerous such reviews during CYs 2020, 2021, and 2022. The accuracy and completeness reviews are resource intensive and have increasingly involved travel by teams of OI personnel to FBI field offices to review relevant information. Where possible, NSD intends to increase the use of in-person reviews to accomplish this oversight function.

- **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. During CY 2018 – CY 2021, NSD identified a number of FBI query-related compliance issues. During CY 2021, NSD conducted oversight reviews of multiple offices at this agency and NSD collaborated closely with that agency to implement significant system changes and training initiatives to improve compliance. NSD has expanded its review of query compliance at that agency to include reviews of at least nine offices per quarter in Q1 and Q2 of CY 2022, and NSD will continue these reviews throughout CY 2022. These efforts include audits of dozens of users at each field office, as well as travel and training delivered at the conclusion of each review. This program has consumed, and will continue to consume significant attorney resources.

- **Assisting Victims of Overseas Terrorism.** OVT assists United States 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 United States

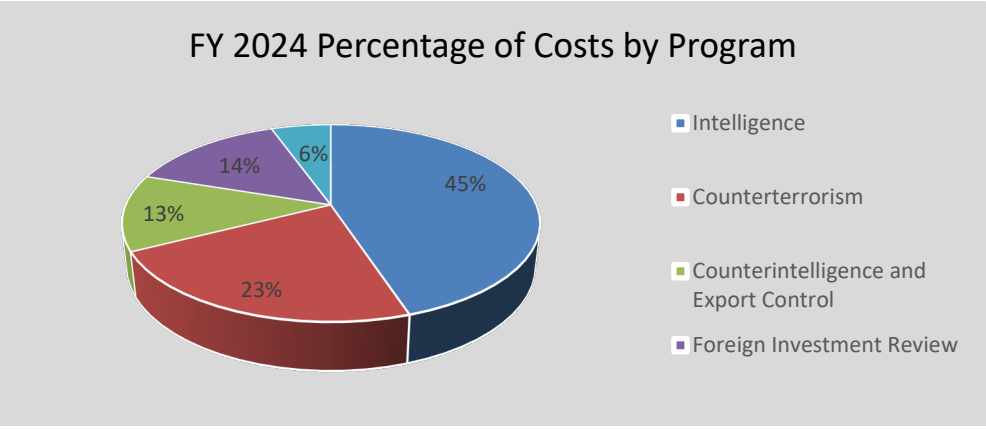
victim attendance and/or court accompaniment at seven foreign proceedings, including proceedings in Israeli Military Court, Jordanian Military Court, United Kingdom Coroner's Inquests, and Dutch civilian criminal court. In all these cases, United States victims chose to provide victim impact statements to the courts, consistent with their rights under foreign law. In FY 2022 and FY 2023, OVT supported United States victim attendance and provided court accompaniment at foreign proceedings for the 2016 Nice and Brussels attacks. OVT continued to support United States 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, and the United Kingdom.

- **Providing Training to International Partners.** In FY 2020 - 2023, OVT provided virtual training about its mission and terrorism victims' rights and access to justice to partners in Cameroon, Burkina Faso, the European Commission's Network of EU single contact points for victims of terrorism, and the 2022 United Nations Global Congress of Victims of Terrorism.

- **Supporting International Cooperation on Victims of Terrorism.** OVT has cooperated with the United States 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 United States 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 United States 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, prosecutions, and other disruptions. The theft of trade secrets and other intellectual property by or for the benefit of foreign entities is an increasingly acute and costly threat to United States national and economic security.

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

The most sophisticated of the United States adversaries employ multi-faceted campaigns to acquire valuable proprietary technologies and information through a combination of traditional and asymmetric approaches. For example, the United States nation-state adversaries increasingly rely on commercial and other non-state entities to conduct economic espionage, which is creating a new threat vector that is especially difficult to investigate. NSD plays a central role in addressing these threats through comprehensive, multi-faceted approaches that leverage the full array of options under existing legal authorities.

Also, among the most significant challenges that NSD continues to face is the rapid expansion, evolution, and sophistication of cyber threats to national security. NSD must be prepared to continue to take lessons learned over the past decade and adapt them to this expanding and sophisticated 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 speed and global span, increasing uses and theft of digital currencies, 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 NSD's present capabilities and NSD's anticipated needs in the near future will require steadfast commitment.

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.

Further, with the increasing use, types, and value of virtual currency over the past several years, some governments use hacking, ransomware, and other forms of theft and cyber-enabled sanctions evasion to obtain funding to support the government's objectives. This is especially common where the government is subject to sanctions that make it more difficult to gain revenue through trade and other forms of legitimate commerce (*e.g.*, North Korea utilizes digital currency theft to support the regime's weapons program). Other hacking groups rely on digital currencies to obfuscate their purchase and use of hacking infrastructure. Thus, adversary efforts to obtain or use such virtual currencies present a national security threat beyond the financial loss to the United States. NSD plays a central role in disrupting such revenue generation and procurement efforts, including through warning potential victims and providers of digital infrastructure, seizing virtual currency, or identifying key enablers of such schemes. Accordingly, NSD will be expected to adequately resource its virtual currency expertise and resources, including through the training of attorneys in the developing virtual currency ecosystem and in obtaining the necessary software and analytical support to understand and trace virtual currency and similar blockchain transactions.

Foreign Investment Review

NSD's foreign-investment review work has also expanded over 20% each year since FY 2020 to address growth of asymmetric threats. This work, handled through NSD's FIRS, includes the following primary lines of effort:

(1) reviewing and resolving national-security risks posed by foreign transactions and investments in matters before CFIUS;
(2) reviewing and resolving, through Team Telecom, national-security and law-enforcement risks posed by foreign entities' licenses and applications to provide telecommunications services in matters before the FCC;
(3) monitoring national security agreements for compliance (including conducting 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 United States national security to the Department of Commerce for action under Executive Order 13873, and referring those that specifically pose such risk to United States Government information technology systems to the OMB-led Federal Acquisition Security Council for potential or removal and/or exclusion from such systems.

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 FY 2022, NSD reviewed approximately 22% more submissions than in FY 2021 regarding mergers, acquisitions, and investments. In FY 2022, NSD led approximately 25% of CFIUS cases in which a Joint Voluntary Notice was filed. Further, NSD led 44% of the overall CFIUS cases that resulted in transactions being prohibited, abandoned, or mitigated, based on national security risk identified by NSD. In FY 2022, NSD led approximately 26% (up from 24% in FY 2021) of the cases in which a declaration was filed with CFIUS.

NSD supports multiple aspects of the CFIUS process. NSD performs reviews and investigations of transactions, serves as DOJ's representative on CFIUS. Overall, CFIUS matters increased 21% from FY 2021 to FY 2022. The chief drivers of that anticipated increase are filings that had been deferred because of the challenges posed by the COVID-19 pandemic and related supply chain disruptions, as well as industry's increasing familiarity with, and use of, the declaration process. 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 29% of which represent an agreement associated with a CFIUS transaction.

Second, with respect to NSD's Team Telecom work, in addition to continuing to exercise 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 FY 2022 and to date in FY 2023 of the 52 FCC referrals of applications in FY 2022 (that involved a total of 109 telecommunications authorizations, cable landing licenses, and petitions for declaratory ruling), Team Telecom recommended to the FCC that 83% of the total authorizations, licenses, and petitions for declaratory rulings be granted contingent on mitigation measures resulting in 26 new mitigation agreements. So far in FY 2023, NSD has concluded 13 additional Team Telecom referral reviews (that involved a total of 25 telecommunications authorizations, cable landing licenses, and petitions for declaratory ruling), resulting in 3 new mitigation agreements. Team Telecom continues to review 18 active referrals (55 active matters) as well. NSD also continues to monitor compliance with all mitigation agreements (approximately 190 and growing) to which DOJ is a party, approximately 70% 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 FY 2022, NSD terminated approximately 22 mitigation agreements that were no longer necessary, 41 new agreements were signed, which resulted in a total of approximately 190 agreements that were active at the end of the fiscal year (approximately 10% overall growth per year). Of the CFIUS and Team Telecom cases discussed above, 15 new CFIUS cases and 26 new Team Telecom cases led or co-led by NSD in FY 2022 resulted in national security agreements that NSD negotiated and entered 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.

Fourth, since the President signed Executive Order 13873 in May 2019 to secure the ICTS supply chain, 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 FY 2022, NSD submitted six referrals to the Department of Commerce under the new authority—and to date these are only referrals that Commerce has received from the interagency. All nine interagency referrals have been investigated, drafted, and submitted by FIRS. In addition, since the passage of the Federal Acquisition Supply Chain Security Act, FIRS has supported the Federal Acquisition Security Council, which can make recommendations the Secretaries of Defense and Homeland Security, as well as the Director of National Intelligence to remove or exclude certain high-risk vendors from federal IT systems. In FY 2022, FIRS made two referrals, naming 4 companies of concern, to the FASC for review.

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 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. 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 United States 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 United States 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. FIRS currently relies on manual data entry and tracking all case related information, resulting in significant inefficiencies, and diverting resources from its substantive work to protect national security. To meet this challenge, FIRS has been actively pursuing the acquisition of a modern, dynamic case-management system. This system, which will be funded with base resources and is expected to be awarded in FY 2023, will enable FIRS to streamline and automate tasks that have created significant administrative burden, such as retrieving case files from applicants and partner agency portals, of which the information demands are increasing significantly. FIRS leadership requires real-time reports, dashboards, performance metrics, enhanced communications and collaboration tools, and alerts on case status, cases workload management, predicative analytics capabilities, and event and milestone planning and integrated workflow scheduling functions. This new system will enable FIRS to more proactively and efficiently manage national-security reviews, analyze trends, and identify strategic priorities and gaps using big-data driven business intelligence.

NSD's foreign-investment work does face 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. This 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).

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

NSD's intelligence-related work fully supports the United States Government's national security mission, including combating the threats posed by terrorists, threats to United States 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 its 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 and related taskings over the last several years. While the number of targeting decisions remains classified, the Government reported in the 24th Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of FISA, covering the period of December 2019 – May 2020: "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 150% between CY 2014 and CY 2021. 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. The number of targets reported for CY 2021 grew 15% over the number reported for CY 2020. NSD anticipates that the upward trend will continue through CY 2023. The substantial growth of NSD's Section 702 oversight program and the resulting impact on NSD's resources is also apparent from the almost 600%[2] increase in the number of matters handled by OI, the NSD component that oversees this program, between FY 2014 and FY 2022. 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 ensure the IC properly remediates compliance incidents with efforts toward prevention for the future. OI must report each identified 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 2023. 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.

[2] Part of this increase is attributable to OI accounting for certain matters not previously included in workload reporting.

Additionally, NSD devotes significant resources to ensure that FISA-acquired information, including information acquired pursuant to Section 702, is queried in compliance with applicable minimization or querying procedures. During CY 2021 and CY 2022, NSD conducted query oversight reviews of multiple FBI field offices, and NSD collaborated closely with the FBI to implement significant system changes and training initiatives to improve compliance. NSD will continue its expanded review of query compliance at that agency throughout CY 2023. These reviews are resource intensive and have resulted in the reviews by OI attorneys of hundreds of thousands of queries and audits of dozens of agency personnel, as well as the delivery of training at multiple agency field offices.

OI continues to oversee the implementation and effectiveness of multiple corrective measures to ensure the accuracy and completeness of applications submitted to the FISC by the FBI 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 the 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 194 FISA applications between May 2020 and December 2022. These resource-intensive reviews require multiple attorneys to complete the review, and some of these reviews involve travel to the relevant FBI field office.

Additionally, 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.

During 2021, NSD experienced growth in the use of FISA information in criminal, civil, or administrative proceedings and expects this trend to continue. 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.

In the last quarter of CY 2022, OI began serving as the United States Oversight Authority for agreements entered with foreign governments pursuant to the Clarifying Lawful Overseas Use of Data (CLOUD) Act. In that role, OI oversees compliance by United States agencies and prosecutors seeking to acquire data from foreign providers under CLOUD Act agreements with multiple countries. OI has been an active participant in negotiating those agreements and the related documents. OI

expects to devote significant resources to developing training programs and conducting oversight reviews as United States agencies become familiar with this new authority over the next several years.

3. Continually Evolving Terrorism Threats.

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

The United States faces increased threats of domestic terrorism and these 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. In addition, the threat of domestic violent extremism has an increasing transnational component that requires the need to engage with foreign partners to counter the threat. These threats will continue to pose unique challenges for the foreseeable future.

In March 2021, considering 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 June 2022, NSD formed 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. In addition, the increased oversight of domestic terrorism cases, along with providing new training on the issues related to these cases, has increased the amount of travel for attorneys.

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 United States 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 United States 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 United States. Online radicalization is a particular problem as terrorists and other criminals increasingly use technology, including encryption, to conceal their crimes and avoid government detection. This poses serious challenges for public safety and adds significant burdens on law enforcement and intelligence investigations to attempt to mitigate the loss of lawful access to information.

As part of 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 United States 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 assigned multiple attorneys overseas to work with partner countries on these efforts.

Another area of ongoing concern is the increase in threats related to Iran, including threats to United States interests in the Middle East. In addition, Iranian-related actors have attempted to carry out plots against Iranian dissidents and members of the Persian community opposed to the Iranian regime or who have called out human rights abuses in Iran. There have also been ongoing threats and plots against current and former United States government officials.

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 service environment to quickly process discovery and efficiently support nationwide terrorism-related litigation.

Each of these various threats are complex, frequently involving individuals 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 United States 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 United States victims continues.

OVT assists United States citizen victims harmed in overseas terrorist attacks that result in criminal justice proceedings abroad. This international model program helps United States 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 United States 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 United States government financial support programs for United States 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, which can be administratively burdensome.

OVT supports United States 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 40 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 United States 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 United States citizen terrorism victims involved with those systems. OVT seeks to support United States 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 United States Government's commitment to United States 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 to maintain the level of support for United States victims of overseas terrorism and their participation in foreign systems during a global pandemic. OVT continues to actively monitor opportunities for United States victim participation in international large-scale trials, including the FY 2022 – FY 2023 trials for the 2016 Nice and Brussels attacks, by engaging with the United States and foreign counterparts and communicating with the United States victims and survivors.

II. Summary of Program Changes

Item Name	Description				Page
		Pos.	Estimated FTE	Dollars ($000)	
Foreign Investment Review	Additional resources to support NSD's foreign investment review work	17	8	$3,444	51
Counterintelligence and Export Control, including Countering Cyber Threats	Additional resources to support NSD's counterintelligence and export control work, including countering cyber threats	5	3	$1,002	59
Crisis Management System	Additional resources for the implementation of new hardware and support for the new Crisis Management System (CMS).	0	0	$3,597	63
National Security Memo-8 Security Enhancements	Additional resources for the implementation of hardware and software required by National Security Memorandum-8 (NSM-8)	0	0	$761	66
Grand Total: FY 2024 Enhancement Request		**22**	**11**	**$8,804**	

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, [$133,512,000] *144,788,000,* 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
2022 Enacted	403	330	$120,681,000
2023 Enacted	434	354	$133,512,000
Adjustments to Base and Technical Adjustments	0	10	$2,472,000
2024 Current Services	434	364	$135,984,000
2024 Program Increases	22	11	$8,804,000
2024 Program Offsets	0	0	$0
2024 Request	456	375	$144,788,000
Total Change 2023-2024	**22**	**21**	**$11,276,000**

National Security Division - Information Technology Breakout (of Decision Unit Total)	Direct Pos.	Estimate FTE	Amount
2022 Enacted	26	26	$15,766,000
2023 Enacted	26	26	$15,822,000
Adjustments to Base and Technical Adjustments	0	0	$0
2024 Current Services	26	26	$15,822,000
2024 Program Increases	0	0	$6,466,000
2024 Program Offsets	0	0	$0
2024 Request	26	26	$22,288,000
Total Change 2023-2024	**0**	**0**	**$6,466,000**

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 United States 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 United States are consistent with relevant law;
- In coordination with the FBI, the IC, and the USAOs, NSD's primary operational function is to prevent, deter, and disrupt terrorist and other acts that threaten the United States, including counterintelligence threats and cyber threats to the national security;
- NSD also serves as DOJ's liaison to the DNI, advises the Attorney General on all matters relating to the national security activities of the United States, and develops strategies for emerging national security threats – including cyber threats to the national security;

- NSD administers the United States 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 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 United States and foreign government and non-government services providers. OVT further provides expertise and guidance within DOJ and to United States government partners on issues important to United States 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 United States victims' rights and international best practices, OVT supports a role for terrorism victims in foreign partners' justice systems.

2. Performance and Resource Tables

PERFORMANCE AND RESOURCES TABLE										
Decision Unit: National Security Division										
RESOURCES ($ in thousands)	**Target**		**Actual**		**Target**		**Changes**		**Requested (Total)**	
	FY 2022		**FY 2022**		**FY 2023**		**Current Services Adjustments and FY 2024 Program Changes**		**FY 2024 Request**	
Workload*										
Defendants Charged	**136**		**466**		**237**		**0**		**237**	
Defendants Closed	**131**		**454**		**212**		**0**		**212**	
Matters Opened	**550,740**		**590,580**		**526,155**		**0**		**526,155**	
Matters Closed	**550,602**		**589,884**		**525,860**		**0**		**525,860**	
FISA Applications Filed**	**CY 2022: 1,500**		**CY 2022: TBD**		**CY 2023: 900**		**0**		**CY 2024: 900**	
National Security Reviews of Foreign Acquisitions	**FY 2022: 500**		**CY 2022: 783**		**FY 2023: 600**		**0**		**FY 2024: 600**	
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)	339	121,781	339	121,781	354	133,512	21	11,276	375	144,788

*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 2022**		**FY 2022**		**FY 2023**		**Current Services Adjustments and FY 2024 Program Changes**		**FY 2024 Request**	
Program Activity	Counterintelligence and Export Control and Foreign Investment Review		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
			85	32,055	85	32,055	84	32,449	12	6,596	96	39,045
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	90%		98%		90%		0%		90%	
KPI:	2.1 Protect National Security	Percent of DOJ-led foreign investment cases that were adjudicated favorably	97%		100%		97%		0%		97%	
Performance Measure:	2.1 Protect National Security	Percentage of CE defendants whose cases were favorably resolved	90%		98%		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	20		22		22		0		22	
Performance Measure:	2.1 Protect National Security	High priority national security reviews completed	100		436		150		25		175	
Program Activity	Intelligence and Counterterrorism		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
			239	84,362	239	84,362	252	94,265	4	3,506	256	97,771

PERFORMANCE AND RESOURCES TABLE													
Decision Unit: National Security Division													
RESOURCES ($ in thousands)			**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)**	
TYPE	**STRATEGIC OBJECTIVE**	**PERFORMANCE**	**FY 2022**		**FY 2022**		**FY 2023**		**Current Services Adjustments and FY 2024 Program Changes**		**FY 2024 Request**	
KPI:	2.2: Counter Foreign and Domestic Terrorism	Percent of counterterrorism defendants whose cases were favorably resolved	90%		99%		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	1,000		1,073		400		0		400	
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 2022: 130		CY 2022: 261		CY 2023: 190		0		CY 2024: 190	
Program Activity	Cybersecurity		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
			15	5,364	15	5,364	18	6,798	4	1,174	22	7,972
Performance Measure:	2.4 Enhance Cybersecurity and Fight Cybercrime	Percentage of Cyber defendants whose cases were favorably resolved	90%		N/A - No Cyber defendants' cases were closed in FY22		90%		0		90%	

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 2022	FY 2023	FY 2024
		Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Target	Actual	Target	Target
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%	98%	90%	90%
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%	100%	97%	97%
Performance Measure	Percentage of CE defendants whose cases were favorably resolved	98%	100%	100%	100%	100%	99%	95%	85%	90%	98%	90%	90%
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%	100%	99%	99%
Performance Measure	FARA inspections completed	14	14	14	15	15	20	9	20	20	22	22	22
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 2022: 430	CY 2023: 150	CY 2024: 175
Key Performance Indicator	Percent of counterterrorism defendants whose cases were favorably resolved	92%	98%	99%	91%	91%	95%	89%	99%	90%	99%	90%	90%
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	1,073	400	400
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%	100%	99%	99%
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 2022: 261	CY 2023: 190	CY 2024: 190
Performance Measure	Percentage of Cyber defendants whose cases were favorably resolved	NA	100%	100%	100%	100%	100%	N/A - No Cyber defendants' cases were closed in FY20	100%	90%	N/A - No Cyber defendants' cases were closed in FY22	90%	90%

3. Performance, Resources, and Strategies

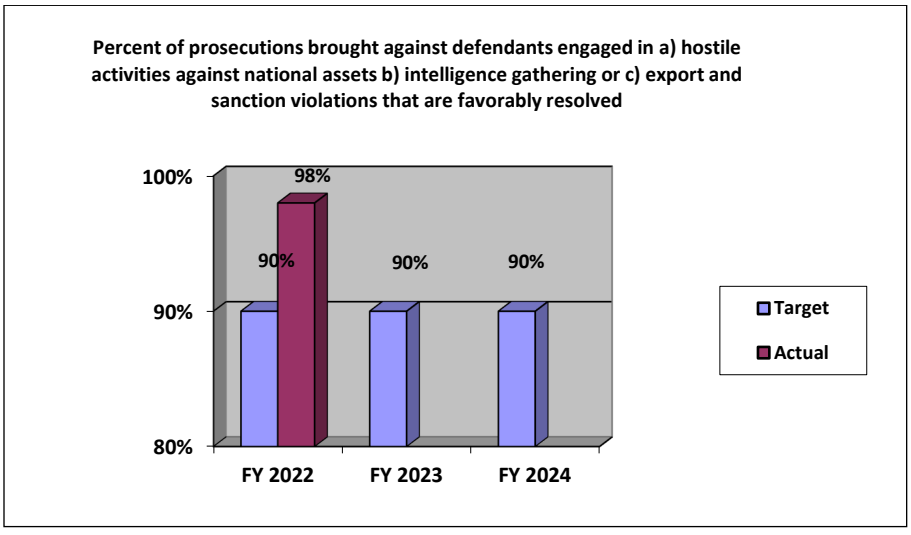
For performance reporting purposes, resources for NSD are included under DOJ Strategic Goal 2: Keep our Country Safe. Within these goals, NSD resources address Strategic Objectives 2.1: Protect National Security, 2.2: Counter Foreign and Domestic Terrorism, and 2.4: Enhance Cybersecurity and Fight Cybercrime.

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 2022 Target: **90%**
FY 2022 Actual: **98%**
FY 2023 Target: **90%**
FY 2024 Target: **90%**
Discussion: The FY 2024 target is consistent with previous fiscal years.



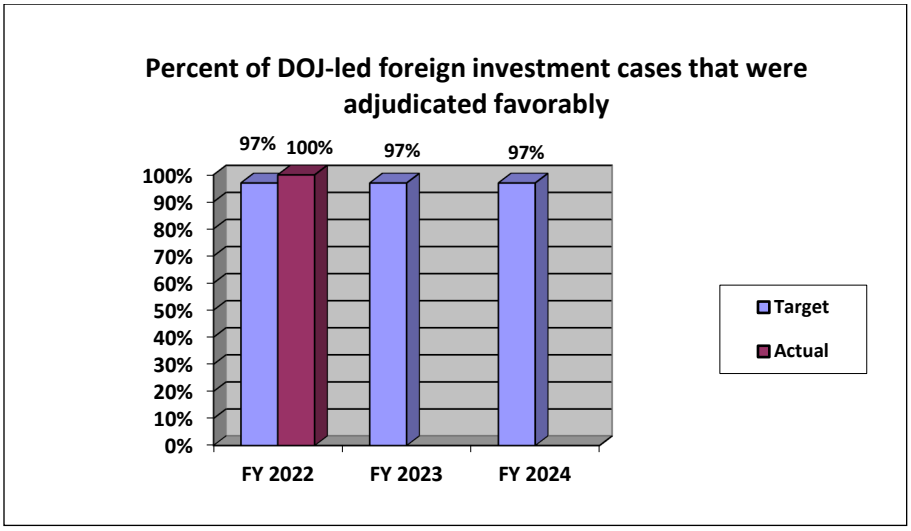
Data Definition: Defendants whose cases were favorably resolved include those defendants whose cases were closed during the fiscal year that resulted in guilty pleas or convictions. Hostile activities against national assets include activities conducted by, at the direction of, or otherwise on behalf 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 the Case Management System (CMS).

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

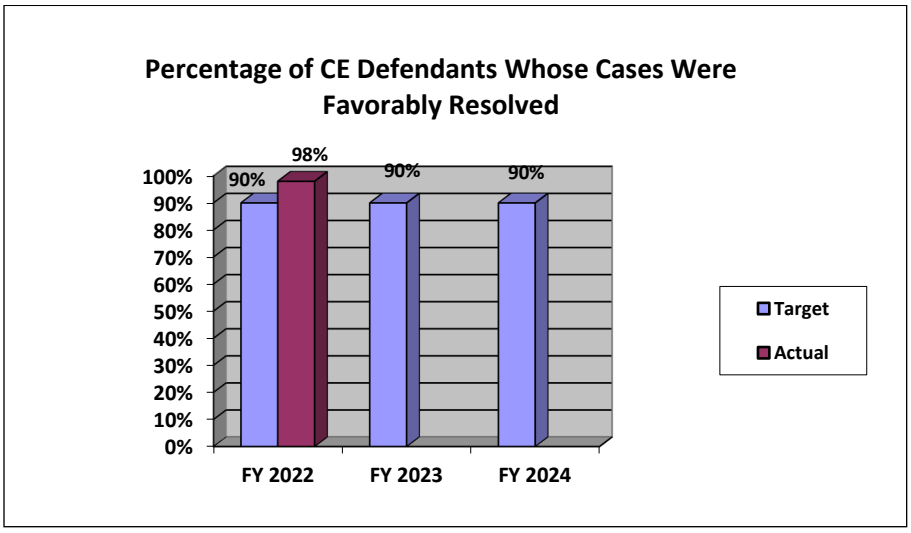
Measure: **Percent of DOJ-led foreign investment cases that were adjudicated favorably**
FY 2022 Target: **97%**
FY 2022 Actual: **100%**
FY 2023 Target: **97%**
FY 2024 Target: **97%**
Discussion: The FY 2024 target is consistent with previous fiscal years.



Data Definition: Percentage of cases co-led by the DOJ in CFIUS, Team Telecom, and Executive Order 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: Data is collected, stored, and verified manually and stored in generic files; however, management is pursuing the acquisition of a modern dynamic case management system.
Data Validation and Verification: Currently, data is manually validated and verified by FIRS management.
Data Limitations: Given the expanding nature of the program area, a more centralized, automated data system is required.

Measure: **Percentage of CE Defendants Whose Cases Were Favorably Resolved**
FY 2022 Target: **90%**
FY 2022 Actual: **98%**

FY 2023 Target: 90%
FY 2024 Target: 90%
Discussion FY 2023 and FY 2024: 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 United States 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

- *United States 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. In November 2022, Jonathan was sentenced to 19 years and 4 months in prison and fined $45,700; Diana was sentenced to 21 years and 10 months in prison and fined $50,000.

- *United States v. Xiaorong You*: In May 2022, Xiaorong You was sentenced to 14 years in prison after being convicted in the Eastern District of Tennessee for economic espionage related to "BPA-free" coatings, as part of a plan to set up a competing business in China.

Highlights from Recent Export Control and Sanctions Enforcement Cases

- *United States 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 United States 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 United States 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 United States Government's largest-ever forfeiture actions for weapons and fuel shipments from Iran. United States 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 United States subsequently transferred approximately 1.1 million barrels of refined petroleum from the four vessels. The United States now has sold that petroleum.

- *United States 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 face 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 United States 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.

- *United States v. Zangakani et al.*: In March 2021, in the Central District of California, DOJ announced charges against 10 Iranian nationals for running a nearly 20-year-long scheme to evade United States 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 UAE. In addition, DOJ filed a forfeiture complaint seeking a money laundering penalty in the amount of $157,332,367.

- *United States v. Shuren Qin et al.*: In September 2021, in the District of Massachusetts, Shuren Qin was sentenced to 24 months in prison after pleading guilty to illegally procuring and exporting United States-origin goods to Northwestern Polytechnical University in the People's Republic of China, which is heavily involved in military research.

- In May 2022, authorities in Fiji executed a seizure warrant on the Motor Yacht 'Amadea', a $300 million luxury vessel owned by sanctioned Russian oligarch Suleiman Kerimov. Fijian law enforcement acted pursuant to a mutual legal assistance request from the Department following issuance of a seizure warrant from United States District Court in the District of Columbia, which found the 'Amadea' is subject to forfeiture based on probable cause of violations of United States law, including the International Emergency Economic Powers Act (IEEPA), money laundering, and conspiracy.

- 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 United States terrorism forfeiture laws; the United States District Court later granted the Government's motion for interlocutory sales of the petroleum.

Highlights from Recent Foreign Malign Influence Cases

- *United States 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 UAE in the United States at the direction of senior UAE officials by influencing the foreign policy positions of a campaign in the 2016 United States presidential election and, subsequently, the foreign policy positions of the United States 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 United States 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 United States government officials on issues related to United States foreign policy in the Middle East. Barrack also sought appointment to a senior role in the United States Government. As alleged in the indictment, the defendants used Barrack's status as an advisor to the campaign and, subsequently, to senior United States 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.

- *United States v. Michel et al.*: In June 2021, in the District of Columbia, a federal grand jury returned a superseding indictment charging a United States 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 DOJ both to drop an investigation in connection with the international strategic and development company known as 1Malaysia Development Berhad (1MDB), in violation of 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 United States 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.

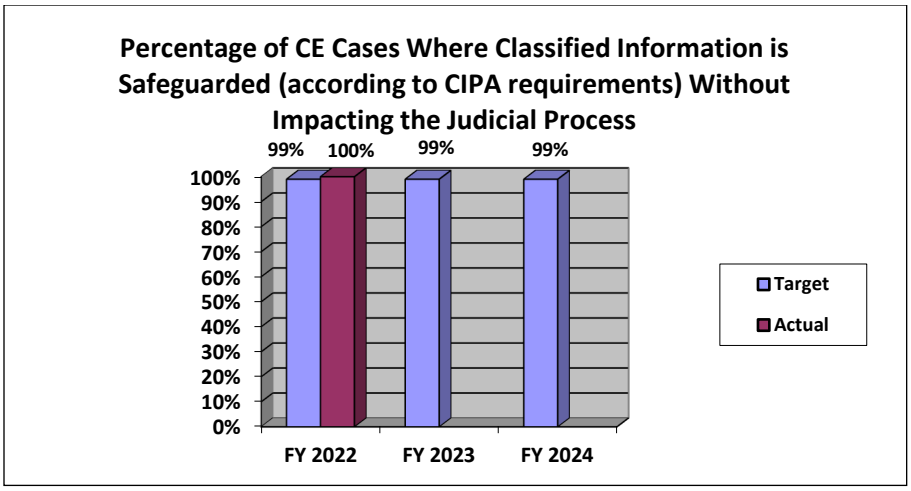
- *United States v. Babakov et al.:* In April 2022, in the Southern District of New York, three citizens of the Russian Federation were indicted for conspiring to use an agent in the United States as an unregistered agent of Russia without prior notice to the Attorney General, conspiring to violate United States sanctions, and conspiring to commit visa fraud. As alleged, Aleksandr Mikhaylovich Babakov, a member of the Russian legislature; Aleksandr Nikolayevich Vorobev, Babakov's chief of staff; and Mikhail Alekseyevich Plisyuk, another

member of Babakov's staff, used a nonprofit organization based in Russia as a front for a global foreign influence campaign to advance Russia's foreign policy objectives. Through operations aimed at influencing the course of international affairs, the defendants worked to weaken United States partnerships with European allies, undermine Western sanctions, and promote Russia's actions designed to destroy the sovereignty of Ukraine. The defendants schemed to affect United States policy towards Russia through staged events, paid propaganda, and the recruitment of at least one American citizen to do their bidding.

- *United States v. Branson:* In March 2022, in the Southern District of New York, dual Russian/United States citizen Elena Branson was charged with acting and conspiring to act in the United States illegally as an agent of the Russian government, willfully failing to register under FARA, and conspiring to commit visa fraud and making false statements to the FBI. As alleged, Branson worked on behalf of the Russian government to advance Russian interests in the United States, including by coordinating meetings for Russian officials to lobby United States political officials and businesspersons, and by operating organizations in the United States for the purpose of publicly promoting Russian government policies, though Branson never notified the Attorney General as she was required to, including by registering under FARA.

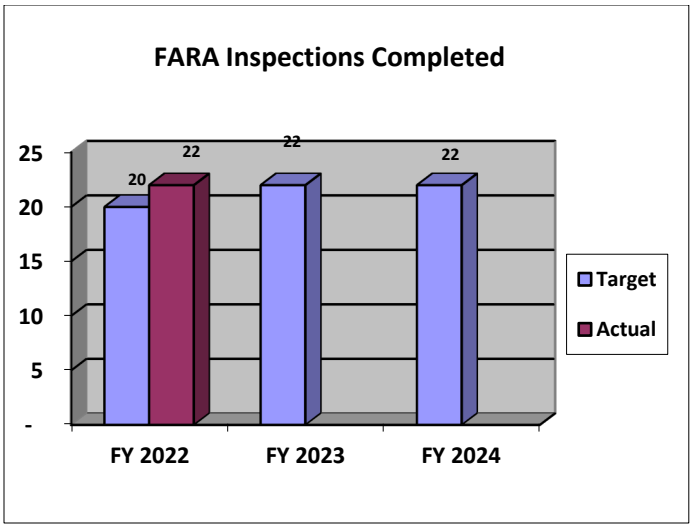
- *United States v. Afasiabi*: In January 2021, NSD obtained criminal charges against Kaveh Lotfolah Afrasiabi for acting and conspiring to act as an unregistered agent of the government of the Islamic Republic of Iran, in violation of FARA. Afrasiabi has identified or portrayed himself as a political 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.

Measure: **Percentage of CE Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2022 Target: **99%**
FY 2022 Actual: **100%**
FY 2023 Target: **99%**
FY 2024 Target: **99%**
Discussion: The FY 2024 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.



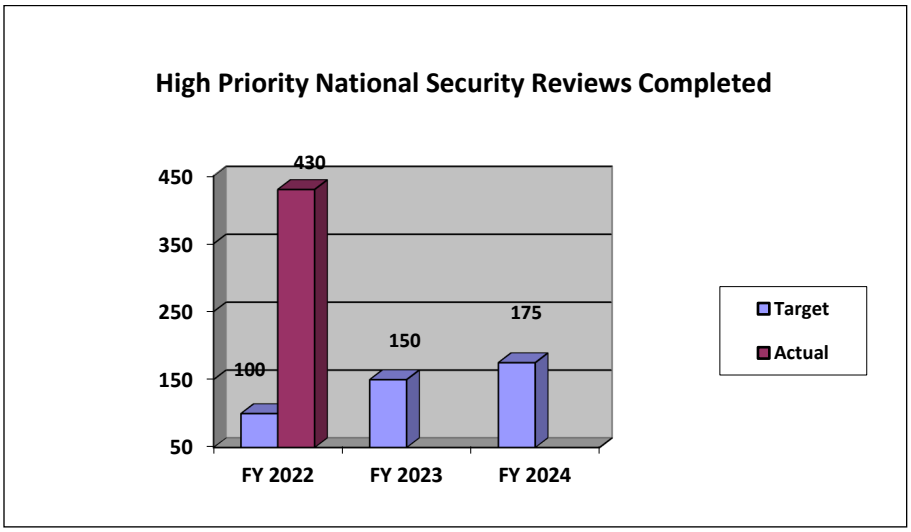
Data Definition: Classified Information - information that has been determined by the United States Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data as defined by the 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 2022 Target: **20**
FY 2022 Actual: **22**
FY 2023 Target: **22**
FY 2024 Target: **22**
Discussion: The FY2023 and FY 2024 targets are slightly higher than prior fiscal years. Performing targeted inspections allows the FARA Unit to enforce compliance more effectively 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**
FY 2022 Target: **100**
FY2022 Actual: **430**
FY 2023 Target: **150**
FY2024 Target: **175**
Discussion: The FY 2024 target is slightly increased from previous fiscal years. NSD will continue to work with its partners to perform these high priority reviews.



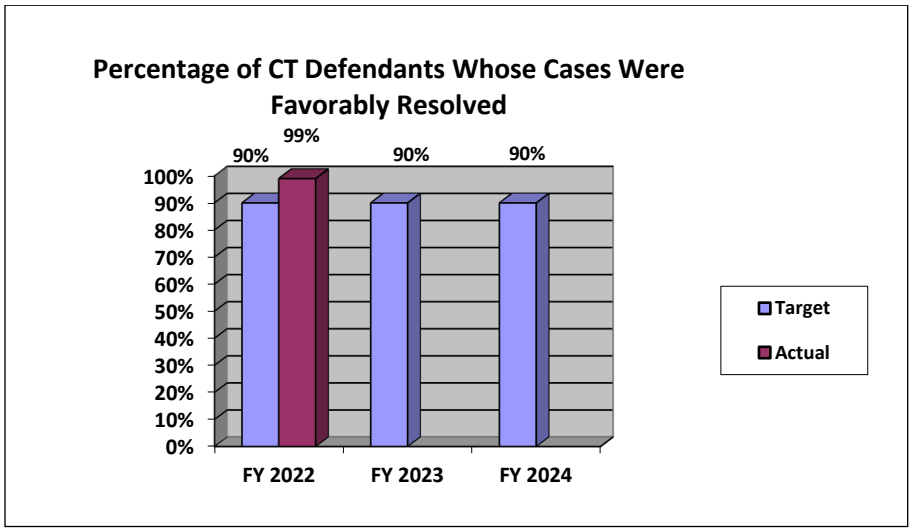
Data Definition: High Priority National Security Reviews include:

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;
4. Mitigation monitoring site visits;
5. Supply-chain referrals and determinations by DOJ (including referrals to the Department of Commerce Under Executive Orders 13873 and 14034, referrals to the Federal Acquisition Security Act of 2018, and determinations for the Federal Communications Commission's Covered List under the Secure and Trusted Communications Networks Act of 2019); and
6. Civil enforcement action.

Data Collection and Storage: Data is collected, stored, and verified manually and stored in generic files; however, management is pursuing the acquisition of a modern dynamic case management system.
Data Validation and Verification: Currently, data is manually validated and verified by FIRS' management.
Data Limitations: Given the expanding nature of the program area, a more centralized, automated data system is required.

Objective 2.2: Counter Foreign and Domestic Terrorism

Measure: **Percentage of CT Defendants Whose Cases Were Favorably Resolved**
FY 2022 Target: **90%**
FY 2022 Actual: **99%**
FY 2023 Target: **90%**
FY 2024 Target: **90%**
Discussion: The FY 2024 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 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.

Guilty Verdict in Trial of Individual Who Killed Eight People on NYC Bike Path

On January 26, 2023, in the Southern District of New York, Sayfullo Habibullaevich Saipov (Saipov) was convicted on all charges following a jury trial. Saipov is facing the death penalty. The penalty phase of the trial began February 6, 2023.

Saipov was charged in a superseding indictment on June 19, 2018 with eight counts of murder in aid of racketeering and ten counts of attempted murder in aid of racketeering, in violation of 18 U.S.C. §§ 1959(a)(1) and (a)(5); eight counts of assault with a dangerous weapon

and attempted murder in aid of racketeering activity, in violation of 18 U.S.C. §§ 1959(a)(3) and 1959(a)(5); one count of providing and attempting to provide material support to a designated Foreign Terrorist Organization (FTO), the Islamic State of Iraq and al-Sham (ISIS), in violation of 18 U.S.C. § 2339B; and one count of violence and destruction of a motor vehicle that resulted in multiple deaths, in violation of 18 U.S.C. §§ 33-34.

On October 31, 2017, at approximately 3:00 p.m., a flatbed truck traveled from New Jersey over the George Washington Bridge and entered New York City. After entering New York City, the truck proceeded onto the bike lane and pedestrian walkway of the West Side Highway. The truck then drove down the walkway for several blocks and struck numerous civilians, ultimately killing eight people and injuring another twelve. The truck eventually collided with a school bus, which was carrying occupants, and came to a halt. The defendant then exited the truck with two objects in his hands that appeared to be firearms. Moments after Saipov got out of the truck, he yelled, "Allahu Akbar," which translates to "God is Great" in Arabic.

Saipov was subsequently shot by a law enforcement officer and taken into custody. A bag was recovered near where Saipov was shot that contained among other things, three knives. The firearms were determined to be a paintball gun and a pellet gun. Law enforcement also recovered, approximately ten feet from the driver's door of the truck, a document that contained Arabic and English text. The Arabic portion of the document states, in substance and in part, "No God but God and Muhammad is his Prophet," and "Islamic Supplication. It will endure," a phrase commonly used to refer to ISIS.

After the defendant was taken into custody, he was read and verbally waived his *Miranda* rights. During that interview, Saipov admitted that approximately one year prior he began planning an attack in the United States, and, approximately two months prior, he decided to use a truck to inflict maximum damage against civilians. In particular, Saipov was motivated to commit the attack after viewing a video in which Abu Bakr al-Baghdadi, then the leader of ISIS, questioned what Muslims in the United States and elsewhere were doing to respond to the killing of Muslims in Iraq. Saipov chose October 31, Halloween, for the attack because he believed there would be more civilians on the street for the holiday. On or about November 2, 2017, ISIS publicly discussed the attack in its weekly newsletter known as "al-Naba." In particular, ISIS claimed Saipov as "a soldier of the caliphate."

<u>Three Illinois Men Sentenced to Prison for Their Roles in Bombing of Dar al-Farooq Islamic Center</u>

On April 12, 2022, in the District of Minnesota, Michael McWhorter (McWhorter) and Joe Morris (Morris), both of Clarence, Illinois, were sentenced to 190 months and 170 months in prison, respectively, for firearms violations, arson, use of a destructive device, and federal civil rights violations in connection with the 2017 bombing of Dar al-Farooq (DAF) Islamic Center in Bloomington, Minnesota. Previously, on September 13, 2021, Emily Claire Hari, formerly known as Michael B. Hari (Hari) was sentenced to 53 years in prison as part of the same case.

On January 24, 2019, in the District of Minnesota, McWhorter and Morris, of Clarence, Illinois, pled guilty to counts two and four of an indictment charging them with intentionally obstructing, and attempting to obstruct, by force and threat of force, the free exercise of religious beliefs, in violation of 18 U.S.C. § 247(a)(2); and carrying and using a destructive device during and in relation to crimes of violence, in violation of 18 U.S.C. § 924(c). These charges stem from the bombing of the mosque in Bloomington, Minnesota. McWhorter and Morris concurrently pled guilty to counts one through three of a superseding indictment from the Central District of Illinois, transferred under Fed. R. Crim. P. 20, charging them with unlawful possession of a machinegun, in violation of 18 U.S.C. § 922(o); conspiracy to interfere with commerce by threats and violence, in violation of 18 U.S.C. § 1951; and attempted arson, in violation of 18 U.S.C. § 844(i). These charges stem from their possession of assault rifles from October 2017 to March 2018.

On June 20, 2018, an indictment was returned in the District of Minnesota charging McWhorter, Morris, and Hari for throwing an explosive device into the Dar al-Farooq Islamic Center in Bloomington, Minnesota on August 5, 2017. The device exploded and caused significant damage. The indictment charged the three defendants with one count of intentionally defacing, damaging, and destroying any religious real property because of the religious character of that property, in violation of 18 U.S.C. § 247(a)(1); one count of intentionally obstructing, and attempting to obstruct, by force and threat of force, the free exercise of religious beliefs, in violation of 18 U.S.C. § 247(a)(2); one count of conspiracy to commit federal felonies by means of fire and explosives, in violation of 18 U.S.C. § 844(h) and 844(m); one count of carrying and using a destructive device during and in relation to crimes of violence, in violation of 18 U.S.C. § 924(c); and Hari was charged with one count of possession of an unregistered destructive device, in violation of 26 U.S.C. § 5845(a) and 5861(d).

Sentencing and Guilty Verdict in ISIS Hostage Taking Cases

On April 29, 2022, in the Eastern District of Virginia, Alexanda Kotey (Kotey) was sentenced to life imprisonment. On September 2, 2021, Kotey, previously a citizen of the United Kingdom, entered a guilty plea to all charges in an eight-count indictment. Kotey was 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 United States 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 resulting in death, in violation of 18 U.S.C. § 2339A, and one count of conspiring to provide material support to ISIS resulting in death, in violation of 18 U.S.C. § 2339B.

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 United States 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' propaganda campaign. ISIS informed

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

On April 14, 2022, a jury returned a verdict of guilty on all counts in the trial against Elsheikh. The jury also made a finding of "resulting in death" on all applicable counts. On August 19, 2022, Elsheikh was sentence to life in prison.

Florida Man Pleads Guilty to Possessing Ricin in Plot to Kill Former Wife

On May 10, 2022, in the Middle District of Florida, Kevin Deane Jones (Jones), pled guilty to the unlawful possession of ricin, a biological toxin, and possessing two firearms as a convicted felon, in violation of 18 U.S.C. §§ 175b(a) & 922(g)(1). Jones was sentence to ten years in prison on January 17, 2023.

According to the plea agreement, on December 6, 2021, the FBI received a complaint that Jones had manufactured ricin intending to use it to kill his former wife. Law enforcement officers then learned that Jones had ordered numerous items online to produce ricin, had reportedly tested water guns to see which ones leaked, and had said that he would go on vacation immediately after spraying his former wife in the face with the ricin, so that he would have an alibi when she died.

On December 17, 2021, law enforcement officers learned that Jones intended to travel out of state to where his former wife lived. Officers stopped Jones, who admitted to manufacturing ricin. Officers located a plastic water gun in Jones' truck, as well as five tubes filled with liquids that later tested positive for ricin. A search of Jones' residence revealed additional tubes containing ricin, along with castor beans, documents pertaining to ricin, and approximately 200 rounds of various types of ammunition.

Additional investigation revealed that on December 6, 2021, Jones was questioned by agents from the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) regarding his possession of weapons. Following the ATF visit, Jones removed multiple firearms and ammunition and took them to a storage unit rented in his name. Law enforcement officers later searched the storage unit and found a rifle, handgun, silencer, and approximately 3,000 rounds of various types of ammunition. Jones is a previously convicted felon and is prohibited from possessing a firearm or ammunition under federal law.

Seditious Conspiracy Trials Related to Events at United States Capitol

On January 12, 2022, Elmer Stewart Rhodes III (Rhodes), Edward Vallejo (Vallejo), Kelly Meggs (Meggs), Kenneth Harrelson (Harrelson), Jessica Watkins (Watkins), Joshua James (James), Roberto Minuta (Minuta), Joseph Hackett (Hackett), David Moerschel (Moerschel), Thomas Caldwell (Caldwell), and Brian Ulrich (Ulrich) were charged with seditious conspiracy, in violation of 18 U.S.C. § 2384; conspiracy to obstruct an official proceeding, in violation of 18 U.S.C. § 1512(k); obstruction of an official proceeding and aiding and abetting, in violation of 18 U.S.C. §§ 1512(c)(2) and 2; and conspiracy to prevent an officer from discharging any duties, in violation of 18 U.S.C. § 372. Meggs, Harrelson, Watkins, Hackett, and Moerschel were charged with destruction of government property and aiding and abetting, in violation of 18

U.S.C. §§ 1361 and 2. Watkins and James were charged with civil disorder and aiding and abetting, in violation of 18 U.S.C. §§ 231(a)(3) and 2. James was charged with assaulting, resisting, or impeding certain officers, in violation of 18 U.S.C. § 111(a)(1). Caldwell, Ulrich, Moerschel, Hackett, Minuta, James, Harrelson, Meggs, and Rhodes were charged with tampering with documents or proceedings and aiding and abetting, in violation of 18 U.S.C. §§ 1512(c)(1) and 2.

Wilson and others conspired to stop the lawful transfer of presidential power by January 20, 2021, by deploying force to prevent, hinder, and delay the execution of the laws of the United States governing the transfer of presidential power. They used encrypted and private communications, equipped themselves with a variety of weapons, donned combat and tactical gear, and were prepared to answer Rhodes' call to take up arms. On December 31, 2020, Rhodes added Wilson to a Signal group chat and referred to Wilson as the leader of the group of Oath Keepers from Sampson County, North Carolina. Rhodes described Wilson and others to the Signal group chat as "some of the NC leaders and experienced prior op veterans from NC."

Based on Rhodes' directive on January 5, 2021, Wilson drove himself from North Carolina to Washington, D.C. Wilson brought with him an AR-6 15-style rifle, a 9-millimeter pistol, approximately 200 rounds of ammunition, body armor, a camouflaged combat uniform, pepper spray, a large walking stick intended for use as a weapon, and a pocketknife. While on his drive, Wilson declared to the Signal group chat, "It's going to hit the fan tonight!" and "That's why I have all my gear with me." On January 6, 2021, Wilson, Rhodes, and others traveled together in the same car from their hotel in Virginia to Washington, D.C. At 2:34 p.m., Wilson entered the Capitol—the first of the co-conspirators to breach the building. By 2:38 p.m. Wilson had marched through the Rotunda to the east side of the Capitol where he joined in the center of a mob of people trying to push open the Rotunda Doors from inside of the building. After exiting the Capitol at 2:55 p.m., Wilson gathered with Rhodes and several co-conspirators approximately 100 feet from the northeast corner of the Capitol.

On March 2, 2022, James pled guilty to seditious conspiracy, in violation of 18 U. S.C. § 2384, and obstruction of an official proceeding, in violation of 18 U.S.C. §§ 1512(c)(2). On April 29, 2022, Ulrich pled guilty to seditious conspiracy, in violation of 18 U.S.C. § 2384, and obstruction of an official proceeding, in violation of 18 U. S.C. §§ 1512(c)(2).

On May 4, 2022, in the District of Columbia, William Todd Wilson (Wilson) pled guilty to seditious conspiracy, in violation of 18 U.S.C. § 2384, and obstruction of an official proceeding, in violation of 18 U.S.C. § 1512(c)(2). Wilson's guilty plea is part of a cooperation plea agreement.

On November 29, 2022, in the District of Columbia, a jury found all five defendants in the Oath Keepers prosecution guilty of various criminal charges related to the events of January 6, 2021. Rhodes and Meggs were found guilty of seditious conspiracy, in violation of 18 U.S.C. § 2384. Meggs and Jessica Watkins were found guilty of conspiracy to obstruct an official proceeding, in violation of 18 U.S.C. § 1512(k), and all five defendants were found guilty of obstruction of an official proceeding, in violation of 18 U.S.C. § 1512(c)(2) and 2. Meggs, Harrelson, and Watkins were found guilty of conspiracy to prevent members of Congress from discharging their duties, in violation of 18 U.S.C. § 372. Rhodes, Meggs, Harrelson, and Thomas

Caldwell were found guilty of tampering with documents or proceedings, in violation of 18 U.S.C. 1512(c)(1). Watkins was found guilty of civil disorder, in violation of 18 U.S.C. § 231. Meggs, Harrelson, and Watkins were found not guilty of destruction of government property, in violation of 18 U.S.C. § 1361.

On January 23, 2023, a jury found all four defendants in the second Oath Keepers trial guilty of seditious conspiracy, in violation of 18 U.S.C. § 2384, for their conduct related to the breach of the U.S. Capitol on January 6, 2021. Defendants Minuta, Hackett, Moerschel, and Vallejo were also found guilty of conspiracy to obstruct an official proceeding, in violation of 18 U.S.C. § 1512(k); obstruction of an official proceeding and aiding and abetting, in violation of 18 U.S.C. §§ 1512(c)(2) and 2; and conspiracy to prevent an officer from discharging any duties, in violation of 18 U.S.C. § 372. The jury found Hackett and Moerschel not guilty of destruction of government property and aiding and abetting, in violation of 18 U.S.C. §§ 1361 and 2. The jury found Hackett guilty of tampering with documents or proceedings and aiding and abetting, in violation of 18 U.S.C. §§ 1512(c)(1) and 2, but acquitted Minuta and Moerschel of this charge.

Breach of the United States Capitol on January 6, 2021

- The breach of the United States Capitol on January 6, 2021 brought an unprecedented number of new prosecutions and investigations to CTS. As of February 7, 2023, there have been more than 985 arrests in almost all 50 states.

- Over 315 defendants have been charged with assaulting, resisting, or impeding officers or employees, including more than 105 that have been charged with using a deadly or dangerous weapon. There are over 55 defendants charged with destruction of government property and over 35 more charged with theft of government property. Nearly 900 defendants have been charged with entering or remaining in a restricted federal building or grounds. And at least 300 defendants have been charged with corruptly obstructing, influencing, or impeding an official proceeding, or attempting to do so.

- Approximately 500 individuals have pleaded guilty to a variety of federal charges, from misdemeanors to felony obstruction, many of whom will face incarceration at sentencing. There have been three guilty pleas to a charge of seditious conspiracy.

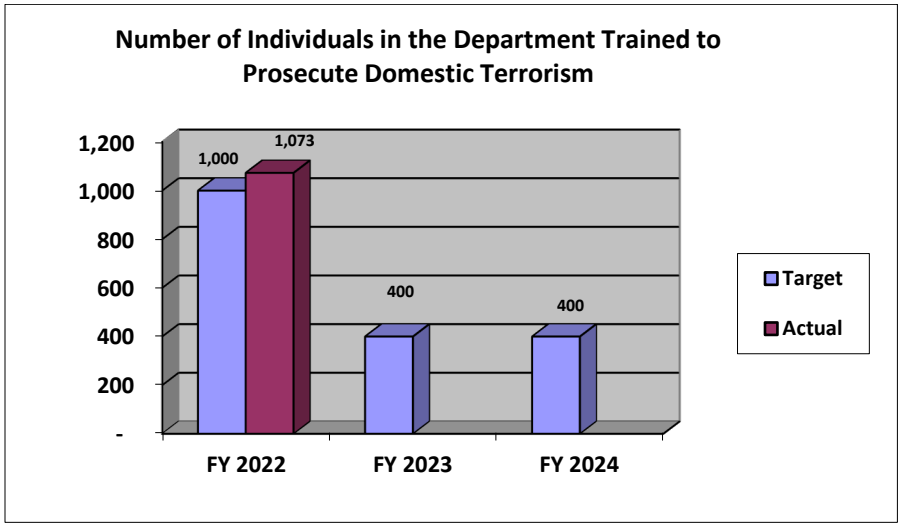
- More than 375 have pleaded guilty to misdemeanors. Over 120 have pleaded guilty to felonies.

- Fifty-five 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.

- Nearly 400 defendants have had their cases adjudicated and received sentences for their criminal activity on January 6. At least 220 have been sentenced to period of incarceration.

Measure: **Number of individuals in the Department trained to prosecute domestic terrorism and domestic extremism**
FY 2022 Target: **1,000**
FY 2022 Actual: **1,073**
FY 2023 Target: **400**
FY 2024 Target: **400**
Discussion: FY 2021 - Six webinars were conducted that included topics regarding Domestic Terrorism. 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.

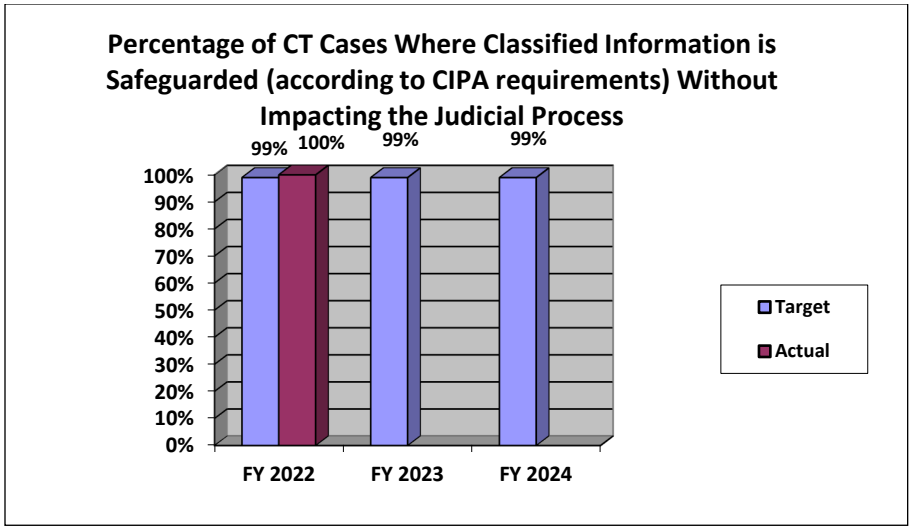
FY 2022 - FY 2024 – Currently there are no facility restrictions as a result of COVID and in-person training is planned for FY 2023 and the first quarter of FY 2024. However, the number of individuals who will be trained cannot be predicted with any accuracy because the training facilities impose limitations based on the status of COVID in the community at that time and is subject to change.



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 Executive Office of U.S. Attorneys' Office of Legal Education.
Data Limitations: The numbers of individuals trained in FY 2022 – FY 2024 will depend greatly on the ability to conduct in-person trainings or whether NSD will conduct webinars only because of the pandemic. For national security courses that can be conducted in an unclassified environment, NSD will continue to conduct some webinars 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, NSD set FY 2022 – FY 2024 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 2022, there were two webinars conducted that included topics regarding Domestic Terrorism. There was a total of 784 individuals who registered to attend

these webinars. There were three additional courses planned for FY 2022 which included topics regarding Domestic Terrorism. While those courses were able to be conducted in-person, there were facility limits on the number of attendees allowed because of the pandemic. As a result, approximately 300 individuals were trained. In FY 2023, there are four courses tentatively scheduled, which will include topics regarding Domestic Terrorism. If all those courses can be conducted in-person but facility limitations are still in effect, it is anticipated that an approximate total of 400individuals will be trained. If those courses must be conducted as webinars, NSD anticipates an approximate total of 1,400 individuals trained.

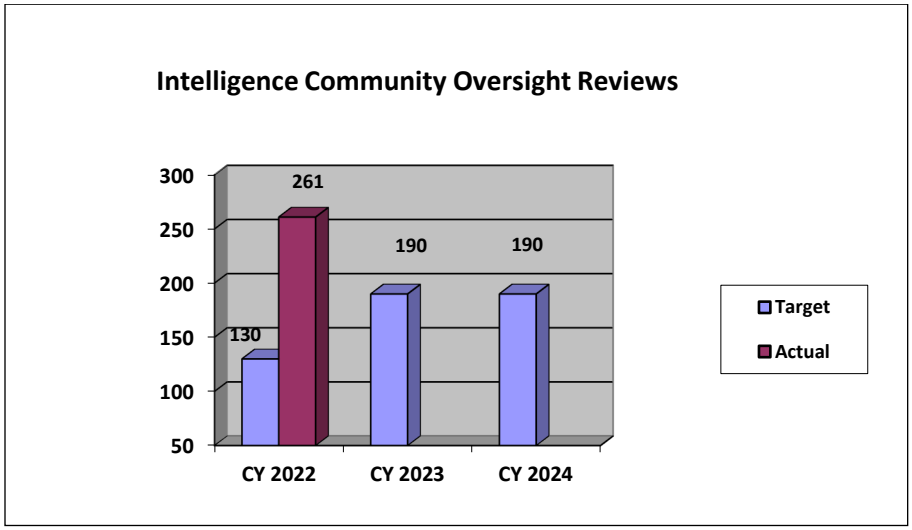
Measure: **Percentage of CT Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2022 Target: **99%**
FY 2022 Actual: **100%**
FY 2023 Target: **99%**
FY 2024 Target: **99%**
Discussion: The FY 2024 target is consistent with previous 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 States 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.

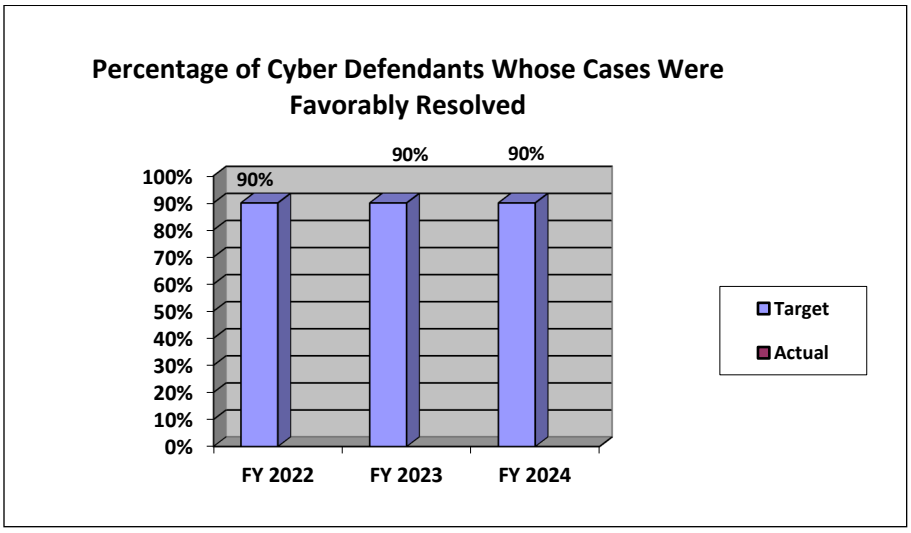
Measure: **Intelligence Community Oversight Reviews**
CY 2022 Target: **130**
CY 2022 Actual: **261**
CY 2023 Target: **190**
CY 2024 Target: **190**
Discussion: CY 2023 and 2024 - The CY 2023 and 2024 targets reflect an increase over CY 2022 to account for additional FY 2023 resources. The overall work 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.
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 2022 Target: 90%
FY 2022 Actual: N/A - No Cyber defendants' cases were closed in FY22
FY 2023 Target: 90%
FY 2024 Target: 90%
Discussion: The FY 2024 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 United States companies and companies operating in the United States.



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

Court-Authorized Disruption of Botnet Controlled by the GRU: In April 2022, in the Western District of Pennsylvania, the Department announced a court-authorized operation to disrupt a two-tiered global botnet of thousands of infected network hardware devices under the control of a unit within the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). The operation copied and removed malware from the vulnerable devices that the GRU actors used for command and control (C2) of thousands of other compromised devices (*i.e.*, the "bots") worldwide, thereby severing those underlying devices

from the C2 device's control. The operation also closed the external management ports that the GRU was using to access the compromised C2 devices, thereby mitigating against reinfection.

United States v. Akulov, et al.: In March 2022, in the District of Kansas, the Department unsealed an indictment that charged three Russian hackers, all of whom were officers in Military Unit 71330 or "Center 16" of the Federal Security Service (FSB) for their role in a two-phased conspiracy between 2012 and 2017 to target the Industrial Control System and Supervisory Control and Data Acquisition (SCADA) systems of hundreds of energy sector entities worldwide, which would have provided the Russian government with the ability to, among other things, disrupt and damage such computer systems at a future time of its choosing. The first phase of their campaign, which took place between 2012 and 2014, involved a supply chain attacks that compromised the computer networks of ICS/SCADA system manufacturers and software providers and then hiding malware – known publicly as "Havex" – inside legitimate software updates for more than 17,000 such systems. The second phase, which took place between 2014 and 2017, focused on spearphishing attacks targeting more than 3,300 users at more than 500 United States and international companies and entities and "watering hole" attacks that leveraged compromised websites to infect computers and steal login credentials of ICS/SCADA engineers visiting such sites. Shortly after the unsealing of the indictment, the Department of State's Rewards for Justice Program offered a reward of up to $10 million for information regarding the defendants' activities.

United States v. Gladkikh: In March 2022, in the District of Columbia, the Department unsealed an indictment that charged a Russian computer programmer employed by a Russian Ministry of Defense-affiliated research institute for his role in a campaign to hack industrial control systems (ICS) and operational technology (OT) of global energy facilities using techniques designed to enable future physical damage with potentially catastrophic effects. Between May and September 2017, the defendant and co-conspirators hacked the system of a foreign refinery and installed the "Triton" malware on a refinery safety system. The conspirators designed the malware to prevent the refinery's safety systems from functioning (*i.e.*, by causing the ICS to operating in an unsafe manner while appearing to operate normally), granting the defendant and his co-conspirators the ability to cause damage to the refinery, injury to anyone nearby, and economic harm. The running of this malware caused two separate emergency shutdowns at the refinery. The conspiracy subsequently attempted to hack the computers of a United States company that managed similar critical infrastructure entities in the United States. Shortly after the unsealing of the indictment, the Department of Treasury's Office of Foreign Assets Control (OFAC) designated Gladkikh and two other employees of the employing Russian research institute pursuant to Section 224(a)(1)(B) of the Countering America's Adversaries Through Sanctions Act, and the Department of State's Rewards for Justice Program offered a reward of up to $10 million for information regarding their activities.

United States v. Seyyed Kazemi, et al.: In November 2021, in the Southern District of New York, the Department unsealed an indictment that charged two Iranian nationals for their involvement in a cyber-enabled campaign to intimidate and influence American voters, and to otherwise undermine voter confidence and sow discord, in connection with the 2020 United States presidential election. The defendants and their co-conspirators obtained confidential United States voter information from at least one state election website, sent threatening email messages to intimidate and interfere with voters, created and disseminated a video containing disinformation about purported election infrastructure vulnerabilities, attempted to access,

without authorization, several states' voting-related websites, and successfully gained unauthorized access to a United States media company's computer network that, if not for the successful DOJ and victim company efforts to mitigate, would have provided the conspirators another vehicle to disseminate false claims after the election. Concurrent with the unsealing of the indictment, the Department of Treasury's Office of Foreign Assets Control (OFAC) designated the Iranian company that employed the defendants and the company's leadership pursuant to Executive Order 13848, and the Department of State's Rewards for Justice Program offered a reward of up to $10 million for information regarding the defendants' activities.

United States v. Marc Baier, et al.: In September 2021, in the District of Columbia, the Department announced a deferred prosecution agreement (DPA) with three former members of the United States intelligence community or military for their provision of hacking-related services to a foreign government between 2016 and 2019. Despite being informed on several occasions that their work for a United Arab Emirates-based company constituted a "defense service" requiring a license from the State Department's Directorate of Defense Trade Controls (DDTC) under the International Traffic in Arms Regulations (ITAR), the defendants proceeded to provide such services without a license. These services included the provision of support, direction, and supervision in the creation of a sophisticated "zero-click" computer hacking and intelligence gathering system – *i.e.*, one that could compromise a device without any action by the target. The DPA restricted the defendants' future activities and employment and required the payment of $1,685,000 in penalties.

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 United States 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 United States 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 CFIUS, 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 United States 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 United States 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 United States 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

NSD assists with DOJ's efforts to meet its FY 2023 Agency Priority Goal (APG) related to combating ransomware attacks. Specifically, NSD plays a critical role, along with other Department components, in identifying those who engage in these attacks and in developing lawful options to disrupt and dismantle the infrastructure, networks, and foreign safe havens used to carry them out. NSD can provide additional information when this APG has been finalized.

V. Program Increases by Item

1. Foreign Investment Review

Strategic Goal: Goal 2: Keep Our Country Safe

Strategic Objective: Objective 2.1: Protect National Security

Budget Decision Unit(s): National Security Division

Organizational Program: Foreign Investment Review Section (FIRS)

Program Increase: Positions: 17 Atty: 12 FTE: 8 Dollars: $3,444,000

Description of Items

For its Foreign Investment Review Section, NSD requests seventeen (17) new positions, including twelve (12) attorneys, one (1) administrative specialist, two (2) research support specialists, one (1) program and management analyst, and one (1) technology and science advisor and $3,444,000.

Justification

FIRS' Critical Role in Protecting National Security

NSD works to proactively identify, prevent, and disrupt national security threats—not just react to them after the fact. That work is particularly critical in the fields of counterintelligence (preventing foreign intelligence services from accessing sensitive information and technology) and cybersecurity (preventing foreign adversaries from exploiting vulnerabilities in hardware, software, and services). NSD does this work in part through FIRS, which identifies, mitigates, prevents, and disrupts national security and law enforcement risks before they materialize. FIRS assesses risks in the context of foreign investments, transactions, and involvement in United States businesses across every major sector and industry, telecommunications, and the global information and communications technology and services (ICTS) supply chain. FIRS also mitigates any risks through agreements with the companies involved and disrupts these risks using other regulatory authorities. Within this space, NSD prioritizes those matters that could pose risks to the security of sensitive data (such as personal or proprietary information or privacy), information, and communications, the United States telecommunications sector, and law enforcement and intelligence equities (e.g., tools, techniques, facilities, and jurisdiction), , as well as transactions that may otherwise give a foreign adversary access to a collection platform in the United States. With ubiquitous national and global reliance on communications networks, including the underlying equipment, software, and services, a supermajority of FIRS' work involves regulating cybersecurity and data security across industries and sectors.

FIRS' work has two main components: (1) case-specific national security reviews (measured by the performance metric *national security reviews of foreign acquisitions worked on*); and (2) special investigations and projects (measured by the performance metric *matters*

opened/matters closed). In its case-specific national security reviews, FIRS protects national security through four portfolios of work:

- *Foreign investment.* FIRS serves as DOJ's representative on CFIUS, an interagency group that reviews foreign investments in, acquisitions of, and other transactions involving United States companies to identify and mitigate any risks to national security.
- *Telecommunications.* FIRS carries out the Attorney General's responsibilities as Chair of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (also known as Team Telecom), an interagency group that identifies and mitigates national security and law enforcement risks through recommendations to the Federal Communications Commission on certain telecommunications licenses and authorizations that include foreign ownership.
- *Supply chain.* FIRS investigates transactions involving ICTS (including connected software applications) connected to foreign adversaries that may pose unacceptable risks to national security. When FIRS identifies such a risk, FIRS refers the technology or service for potential action, as appropriate, to other agencies or interagency bodies with supply-chain authorities, including the Department of Commerce under Executive Orders 13873 and 14034, the Federal Acquisition Security Council (FASC) under the Federal Acquisition Supply Chain Act of 2018, the Federal Communications Commission under the Secure and Trusted Communications Networks Act of 2019, and the Department of Defense under section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019.
- *Compliance and enforcement.* FIRS develops, drafts, and negotiates National Security Agreements (NSAs) that mitigate national security and law enforcement risks, and then monitors, supervises, and enforces companies' compliance with their NSAs.

FIRS's work directly supports key pillars of the President's National Security Strategy, released in October 2022. As that strategy explains, the United States is the "early years of a decisive decade" that requires cooperation on shared challenges while strategically competing with the China, Russia, and other autocracies and foreign adversaries. "Three interlinked lines of effort are of paramount importance" to this strategy, and DOJ's work through FIRS is critical to at least two of them: out-competing China and constraining Russia, and "shaping the rules of the road for technology, cybersecurity, and trade and economics." These additional resources are needed to support our efforts to protect our country's critical infrastructure, key technologies and their supply chains, and sensitive information from foreign adversaries seeking to exploit, steal, spy on, and sabotage them. These threats have become increasingly complex, and China, Russia, and other foreign adversaries are becoming more aggressive and capable in these efforts than ever before. FIRS's foreign-investment screening through CFIUS and management of the Attorney General's role as Chair of Team Telecom, for example, directly advances the National Security Strategy's call for "modernizing and strengthening" our foreign investment screening mechanisms to "ensure strategic competitors cannot exploit foundational American and allied technologies, know-how, or data to undermine American and allied security" and the President's Executive Order 14083 on Ensuring Robust Consideration of Evolving National Security Risks by CFIUS.

FIRS's significant and expanding role in broader international and interagency policy work contributes directly to shaping the rules of the road for technology, cybersecurity, and trade and economics, one of the key pillars of the National Security Strategy. FIRS is increasingly called upon to assist our international partners in standing up their own foreign investment screening

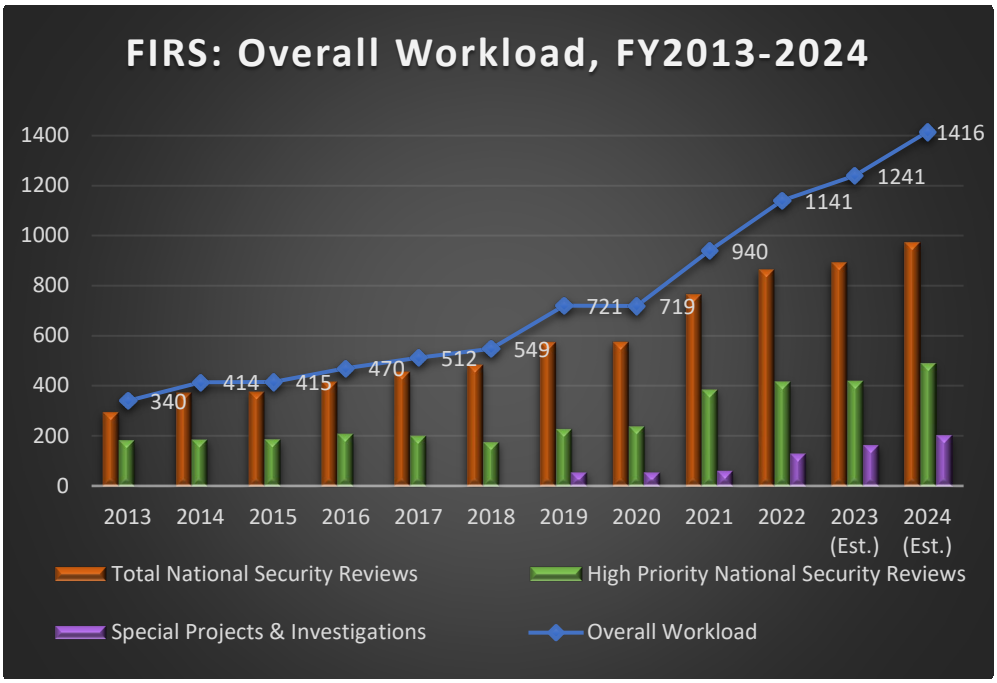
regimes and addressing emerging and evolving risks to the security of data, telecommunications, and supply chains for critical technologies. Because of its important legal and policy role in interagency efforts, FIRS is often also a force multiplier in driving and developing a range of nascent authorities that support the Administration's National Security Strategy and other priorities.

NSD continues to have an outsized role in all these lines of effort. For example: NSD co-led 25% of all CFIUS cases in FY 2022 and now co-leads 100% of Team Telecom cases given the Attorney General's role as Chair of Team Telecom. NSD has proactively used new authorities that the President and Congress have provided without hesitation. DOJ, through NSD/FIRS, is the only agency to have made ICTS referrals to the Department of Commerce under Executive Order 13873 and to the FASC under the Federal Acquisition Supply Chain Act of 2018. Team Telecom, through DOJ's leadership, made two of the first three national security determinations under the Secure and Trusted Communications Networks Act of 2019 to add certain telecommunications services that pose national security risks to the FCC's Covered List. NSD has initiated and led all the civil monetary penalties imposed by CFIUS. NSD also proactively develops strategic initiatives to address emerging national security and law enforcement threats in this space, including an initiative to address potential national security concerns arising from foreign acquisitions of debtors and distressed United States companies' assets in bankruptcy proceedings, and partnerships with law enforcement and intelligence agencies to disrupt threats to sensitive data, national assets, and critical infrastructure using national security regulatory authorities.

NSD is also uniquely situated in its interagency work. NSD provides legal advice and support for DOJ and the various interagency bodies in its role representing the Attorney General and all of DOJ's components (including litigating components) on CFIUS, Team Telecom, supply-chain interagency bodies, and other fora. Thus, in addition to its national security and policy work, NSD must interpret and apply the laws governing these authorities, provide advice, and coordinate the varied legal specialties that affect the exercise of these authorities. Unlike its counterpart offices in other agencies that bifurcate legal and policy functions, NSD consists of lawyers who perform both functions and blends legal, policy, and scientific and technological expertise into a single office. No counterpart office in any other agency performs these integrated functions.

Request for New Attorney Positions

NSD requests 12 new attorney positions to meet FIRS' projected workload demands across its various responsibilities for FY 2024. FIRS' overall workload has continued to increase in volume and complexity:



As shown above, the total volume of FIRS' overall workload of case-specific national security reviews and special investigations increased to 1,141 matters in FY 2022—which represents an average growth rate of over 27% each year since FY 2020. Likewise, FIRS' total complex workload (measured by the performance metric *high priority national security reviews worked on*) increased to 411 total matters in FY 2022—which represents an average annual growth rate of 27.5% since FY 2020.

FIRS' overall workload has already increased disproportionately to its human capital resources even since the office's last significant personnel expansion in FY 2020. While FIRS' attorney ceiling has increased by 11.5% (3 positions) from FY 2020 to FY 2022, the total volume of FIRS' workload has increased by over 58.7% during that same period and its total complex workload has increased by over 72.7% during that same period.

As detailed below, the substantial increase in FIRS' current and projected overall workload is attributable to significant increases in volume and complexity across each of its portfolios of case-specific national security reviews. In addition, FIRS' special investigations and projects increased to 183 matters for FY 2022—which would be an increase of over 194% since FY 2020.

Foreign investment. FIRS' Foreign Investment Team requests an additional 5 attorney positions.

- Total volume. FIRS reviewed 533 total CFIUS cases in FY 2022. FIRS has already reviewed 228 total CFIUS cases so far in FY 2023 and thus is on track to review approximately 566 total CFIUS cases in FY 2023—which represents an average growth rate of over 24% each year since FY 2018. Even assuming a more conservative projected growth rate of 4.8% each year, FIRS is projected to review 593 total CFIUS cases in FY 2024. Each attorney can reasonably handle an annual total caseload of approximately 40 CFIUS cases, in addition to

special investigations and projects.[3] As a result, the projected FY 2024 volume of total CFIUS cases will require a minimum of approximately 15 attorneys, which includes 5 new positions.

Telecommunications and supply chain. FIRS' Telecom & Supply Chain Team requests an additional 3 attorney positions.

- Total volume. FIRS reviewed 88 total Team Telecom cases and made 8 supply-chain referrals, and closed 93 supply-chain related matters for a total volume of 189 telecom and supply chain matters in FY 2022. FIRS has already handled at least 121 telecom and supply chain matters so far in FY 2023 and is on track to handle approximately 174 telecom and supply chain matters in FY 2023—which represents an average annual growth rate of over 13% each year since FY 2019. While Team Telecom reviewed 23% fewer applications in FY 2022 than FY 2021r, NSD led or co-led 100% of the reviews for FCC referrals to Team Telecom for applications for licenses. Even assuming a more conservative projected growth rate of 8% each year, FIRS is projecting 213 total telecom and supply chain matters in FY 2024. Each attorney can reasonably handle an annual total caseload of approximately 16 telecom and supply chain matters (14 Team Telecom cases and 2 supply-chain referrals), in addition to special investigations and projects as assigned.

Compliance and enforcement. FIRS' Compliance & Enforcement Team requests an additional 4 attorney positions.

- Total volume. FIRS negotiated, monitored, terminated, and otherwise handled 332 CFIUS and Team Telecom mitigation agreements and matters in FY 2021 and 373 in FY 2022.[4] FIRS has already handled 265 mitigation agreements and matters so far in FY 2023 and thus is on track to handle 427 total mitigation agreements and matters in FY 2023. Based on average historical growth rates in mitigation matters and conservative annual growth rates in CFIUS and Team Telecom caseload,[5] FIRS is projected to handle 499 CFIUS and Team Telecom mitigation agreements and matters in FY 2024. Each attorney can reasonably

[3] Unless otherwise noted, the annual number of total matters and complex matters that each attorney position can reasonably handle is based on the historical average caseload for each FIRS Attorney-Advisor for FY 2020 through FY 2022, with adjustments to reflect operating capacity and current circumstances.

[4] The total volume of the Compliance & Enforcement Team's annual workload consists of the following: (1) monitoring and enforcing existing active CFIUS and Team Telecom mitigation agreements; (2) monitoring and enforcing new CFIUS and Team Telecom mitigation agreements; (3) drafting, developing, negotiating, and providing other mitigation-related support on DOJ co-led CFIUS and Team Telecom matters likely to result in mitigation; (4) evaluating and terminating outdated mitigation agreements that are no longer necessary to protect United States national security; (5) conducting physical and virtual site visits of companies; (6) monitoring and evaluating bankruptcy cases referred by the United States Trustee and others for potential national security risks raised by the sale of United States businesses' assets to foreign buyers; and (7) special investigations and projects.

[5] The projected growth in FIRS' compliance and enforcement workload for any future year is based on the following: (1) the number of existing active CFIUS and Team Telecom mitigation agreements carried over from the prior year; plus (2) the projected number of new CFIUS and Team Telecom mitigation agreements based on the average percentage, from 2018 to 2022, of DOJ co-led CFIUS joint voluntary notices and Team Telecom cases that result in mitigation agreements; plus (3) the projected number of DOJ co-led CFIUS and Team Telecom matters requiring mitigation support; plus (4) the projected number of terminations of CFIUS and Team Telecom agreements that are no longer necessary, based on the average historical percentage of terminations; plus (5) the projected number of physical and virtual site visits; plus (6) the projected number of bankruptcy-case referrals.

handle an annual total caseload of approximately 40 mitigation agreements and matters, in addition to special investigations and projects as assigned.

Request for New Non-Attorney Positions

NSD requests 5 new non-attorney positions to provide support for FIRS' projected FY 2024 and future workload. Non-attorney support for FIRS includes administrative specialists, analysts, research support specialists, technical information systems specialists, and technology and science advisors. These professional support staff are essential to FIRS' ability to protect national security.

Based on historical average staffing ratios from FY 2013 through FY 2019, one administrative specialist supported approximately 10 attorneys. With the addition of attorney positions in FY 2020 through FY 2022, the current ratio of 29 attorney positions to 1 administrative specialist is unsustainable. Each administrative specialist will be expected to provide administrative support for 18 attorneys. As a result of projected increase in FIRS matters and resource requirements for additional attorneys in FY 2024, FIRS would need 2.9 administrative specialists, which would require 2 new administrative specialist positions.

Based on historical average staffing ratios from FY 2013 through FY 2022, one non-administrative program support staff member is needed for approximately every four attorneys.

Impact on Performance

These additional resources will enhance NSD's ability to ensure that Americans' sensitive personal and proprietary data, sensitive technologies, and critical infrastructure are protected from foreign adversaries. These resources will directly advance DOJ's priorities, including NSD's Strategy for Countering Nation-State Threats.

This request supports Strategic Objectives 2.1 (Protect National Security). Its success is measured in part by Key Performance Indicator 2.1.3 (Percent of DOJ-led foreign investment cases that were adjudicated favorably) and by DOJ performance metrics for *National Security Reviews of Foreign Acquisitions*, *High Priority National Security Reviews Completed*, and *matters opened/matters closed* (which measures FIRS' workload of special investigations and projects).

Funding

1. Base Funding

FY 2022 Enacted				FY 2023 Enacted				FY 2024 Current Services			
Pos	**Atty**	**FTE**	**Amount ($000)**	**Pos**	**Atty**	**FTE**	**Amount ($000)**	**Pos**	**Atty**	**FTE**	**Amount ($000)**
35	26	31	$11,211	35	26	32	$11,459	35	26	32	$11,839

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2024 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Clerical and Office Svcs (0300-0399) – Research Support Specialist	$228	2	$173	$23	$16	$46	$32
Clerical and Office Svcs (0300-0399) – Program and Management Analyst	$147	1	$240	$59	$5	$59	$5
Clerical and Office Svcs (0300-0399) – Administrative Specialist	$83	1	$128	$20	$8	$20	$8
Attorneys (0905)	$2,757	12	$352	$49	($1)	$588	($12)
Info Technology Mgmt (2210) – Technology and Science Advisor	$230	1	$352	$49	($1)	$49	($1)
Total Personnel	**$3,444**	**17**	**$1,245**	**$200**	**$27**	**$762**	**$32**

3. Non-Personnel Increase/Reduction Cost Summary

Not applicable.

4. Justification for Non-Personnel Annualizations

Not Applicable.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Atty	FTE	Personnel	Non-Personnel	Total	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Current Services	35	26	32	$11,839	$0	$11,839	$0	$0
Increases	17	12	9	$3,444	$0	$3,444	$762	$32
Grand Total	**52**	**38**	**41**	**$15,283**	**$0**	**$15,283**	**$762**	**$32**

6. Affected Crosscuts

Counterterrorism, Intelligence and Information Sharing, National Security

2. Counterintelligence and Export Control, including Countering Cyber Threats

Strategic Goal:	Goal 2: Keep Our Country Safe
Strategic Objective:	Objective 2.1: Protect National Security 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: 5 Atty: 4 FTE: 3 Dollars: $1,002,000

Description of Item

The Counterintelligence and Export Control Section (CES) requests 5 positions, including four attorneys, three to assist with its cybersecurity workload and one for its Foreign Agents Registration Act (FARA) Unit, and one administrative specialist position for the FARA Unit. The total request is for $1,002,000.

Justification

Cyber-Related Matters
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. 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, arresting and prosecuting them where possible. Even when arrest is unlikely, NSD prioritizes the disruption of criminal activity through other legal tools like legal seizure of infrastructure and targeted sharing of unclassified threat intelligence gathered because of NSD's criminal investigations. That threat intelligence has: provided the basis for NSD's 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 supporting the Criminal Division in otherwise criminal cases (such as the recent recovery of 85% of the ransom that Colonial Pipeline paid). NSD's ability to respond to significant incidents and develop criminal cases 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 threat 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 IC and 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 IC, DOD, other departments and agencies, and the NSC, 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 Ransomware and Digital Extortion Task Force, 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, CES would commit three attorneys to work almost exclusively on cyber investigations, prosecutions, and disruption operations. Responsibilities would include:

- managing a portfolio of national security cyber investigations;
- providing legal and strategic advice and guidance to other prosecutors and law enforcement officers;
- identifying and securing lawful access to sources of digital evidence/threat intelligence;
- 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, UIC, 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 approach to disrupting cyber threats and empowering network defenders.

FARA Unit

As a result of NSD's efforts over the last several years to increase the visibility of FARA and its enforcement, more lobbyists and members of the bar are coming to the FARA Unit seeking advisory opinions under § 5.2 of the regulations (28 C.F.R. § 5.2). After receiving the FARA Unit's opinion as to the application of the Act to the proposed conduct, more parties have begun disputing the FARA Unit's decisions. It has become increasingly likely that NSD will need to enforce its conclusions that parties must register under FARA through civil injunctive actions. For example, in 2019 a party sued the Department to prevent the FARA Unit from enforcing the party's registration obligation. In the resultant litigation, the Department cross-sued for injunctive relief and was, ultimately, successful in obtaining a court order requiring registration. In 2022, the Department brought its first affirmative civil lawsuit to enforce compliance with the Act in over 30 years. Such lawsuits require extensive resources from the FARA Unit to successfully litigate.

Similarly, in 2020, for the first time since 1988, the FARA Unit resumed issuing notices of deficiency to registrants who are not compliant with their disclosure requirements. The FARA Unit now follows a streamlined procedure for issuing such notices. While most registrants correct their deficiencies upon receipt of such a notice, some will not, thereby necessitating court action. These increased litigation demands justify an attorney position for a litigator with extensive civil experience to handle the expected influx of new civil matters.

In addition to these increasing litigation demands, the FARA Unit continues to see year to year increases in new registrants. In 2021, the FARA Unit processed 90% more new registrants than it did in 2016, despite the obstacles presented by the COVID-19 pandemic. While the FARA Unit added a new attorney in 2021 and a FARA analyst in 2022, the FARA Unit has not hired an administrative support professional since 2011 and requires this type of support to help meet increased workload demands.

Impact on Performance

The above request will allow NSD to better address the increasing caseload of significant cyber matters to keep up with the tracking demands required for registration obligations under FARA and handle the expected increase in civil administrative enforcement of the FARA statute. These resources directly relate to DOJ Strategic Objective 2.1, Protect National Security and Objective 2.4, Enhance Cybersecurity and Fight Cybercrime.

Funding

1. Base Funding

FY 2022 Enacted				FY 2023 Enacted				FY 2024 Current Services			
Pos	Atty	FTE	Amount ($000)	Pos	Atty	FTE	Amount ($000)	Pos	Atty	FTE	Amount ($000)
49	36	42	$14,604	55	42	44	$16,289	55	42	47	$17,089

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2024 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Clerical and Office Svcs (0300-0399) – Administrative Specialist	$83	1	$128	$20	$8	$20	$8
Attorneys (0905)	$919	4	$352	$49	($1)	$196	($4)
Total Personnel	**$1,002**	**5**	**$480**	**$69**	**$7**	**$216**	**$4**

3. Non-Personnel Increase/Reduction Cost Summary

Not Applicable.

4. Justification for Non-Personnel Annualizations

Not Applicable.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Atty	FTE	Personnel	Non-Personnel	Total	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Current Services	55	42	45	$17,089	$0	$17,089	$0	$0
Increases	5	4	3	$1,002	$0	$1,002	$216	$4
Grand Total	**60**	**46**	**48**	**$18,092**	**$0**	**$18,092**	**$216**	**$4**

6. Affected Crosscuts

Counterterrorism, Cybersecurity, Intelligence and Information Sharing, National Security

3. Crisis Management System

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: Division-Wide

Program Increase: Positions: 0 Atty: 0 FTE: 0 Dollars: $3,597,000

Description of Item

NSD requests $3,597,000 for the implementation of new hardware and support for the new Crisis Management System (CMS) secure telecommunications system.

Justification

The National Security Division has a continuing need for a CMS secure telecommunications system providing voice and video capabilities. NSD currently uses a CMS overseen by the White House Communications Agency (WHCA), which recently took over the management of CMS from the Defense Information Systems Agency (DISA).

Based upon recent information from WHCA, NSD anticipates, at a minimum, a substantial increase in the annual operation and maintenance costs for CMS compared to prior years and costs for a technical refresh of the CMS hardware and infrastructure. Further, depending on a determination by WHCA, if NSD cannot continue to use the current CMS, the Division will be required to identify and implement an alternative solution, which NSD estimates will require a substantial investment of funds. CMS is an important tool enabling NSD to conduct secure telecommunications with the White House and Intelligence Community entities.

Specific resource needs include:

Item	Description	FY 2024 Estimated Cost
Implementation Resources	Contractor and equipment resources committed to deployment and implementation of CMS	$163,111
Hardware	Devices required to establish the alternative secure telecommunication system	$2,287,784
Software and Licensing	Software and licensing costs associated with the alternative secure telecommunication system	$1,146,151
	TOTAL	**$3,597,046**

Impact on Performance

This request will allow NSD to implement and maintain an alternative secure telecommunication system. Failure to implement this solution will result in an unacceptable gap in secure telecommunications for the Division and will severely impact NSD's ability to connect efficiently and effectively with the White House and IC.

Funding

1. Base Funding

FY 2022 Enacted				FY 2023 Enacted				FY 2024 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

2. Personnel Increase Cost Summary

Not applicable

3. Non-Personnel Increase/Reduction Cost Summary

NSD requests $3,597,000 for the implementation of new hardware and support for the new CMS that will allow secure telecommunications, as required by the White House. The request includes contractor and equipment resources committed to deployment and implementation of CMS and hard/software required to establish and maintain the alternative secure telecommunication system.

Non-Personnel Item	FY 2024 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Crisis Management System	$3,597	$3,597	1	($2,372)	$24
Total Non-Personnel	**$3,597**	**$3,597**	**1**	**($2,372)**	**$24**

4. Justification for Non-Personnel Annualizations

Anticipated out-year costs total $3,748,000 for contractor support as well as software and licensing costs.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Atty	FTE	Personnel	Non-Personnel	Total	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Current Services	0	0	0	$0	$0	$0	$0	$0
Increases	0	0	0	$0	$3,597	$3,597	($2,372)	$24
Grand Total	**0**	**0**	**0**	**0**	**$3,597**	**$3,597**	**($2,372)**	**$24**

6. Affected Crosscuts

Counterterrorism, Intelligence and Information Sharing, National Security

4. National Security Memorandum-8 Security Enhancements

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: Division-Wide

Program Increase: Positions: 0 Atty: 0 FTE: 0 Dollars: $761,000

Description of Item

NSD requests $761,000 for the implementation of hardware and software required by National Security Memorandum-8 (NSM-8) *Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems* (January 19, 2022), in support of the President's Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).

Justification

NSM-8 requires additional security enhancements within the classified enclaves of government agencies, including requiring implementation of Zero Trust Architecture (addressing both internal and external traffic) and Raise the Bar compliancy within cross-domain solutions. These items will enhance the security of the NSD classified enclaves, allowing for additional security layers and protection within those enclaves. NSD will need to take certain actions to ensure timely and effective compliance with NSM-8.

Specific resource needs include:

Item	Description	FY 2024 Estimated Cost
Implementation Resources	Contractor and equipment resources committed to deployment and implementation of zero trust architecture	$23,384.00
Hardware	Equipment needed to ensure NSD's cross-domain solution meets "Raise the Bar" requirements.	$220,000
Software and Licensing	Software and licensing costs associated with cross-domain solutions and zero trust architecture.	$517,158
	TOTAL	**$760,542**

Impact on Performance

This request will allow NSD to implement Zero Trust Architecture and a Raise the Bar cross-domain solution, which directly supports Executive Order 14028 and NSM-8. NSD's failure to implement NSM-8's requirement could result in certifying agencies not allowing the Division's classified systems to operate without these measures and, therefore, not acting presents an unacceptable risk to critical NSD operations.

Funding

1. Base Funding

FY 2022 Enacted				FY 2023 Enacted				FY 2024 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

2. Personnel Increase Cost Summary

Not applicable

3. Non-Personnel Increase/Reduction Cost Summary

NSD requests $761,000 for the implementation of hardware and software that will allow for additional security layers and protections within the classified enclaves, as required by NSM-8.

Non-Personnel Item	FY 2024 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
National Security Memo-8 Security Enhancements	$761	$761	1	($535)	$0
Total Non-Personnel	**$761**	**$761**	**1**	**($535)**	**$0**

4. Justification for Non-Personnel Annualizations

Anticipated out-year costs total $676,000 for software and licensing costs.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Atty	FTE	Personnel	Non-Personnel	Total	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Current Services	0	0	0	$0	$0	$0	$0	$0
Increases	0	0	0	$0	$761	$761	($535)	$0
Grand Total	**0**	**0**	**0**	**0**	**$761**	**$761**	**($535)**	**$0**

6. Affected Crosscuts

Counterterrorism, Cybersecurity, Intelligence and Information Sharing, National Security

VIII. Exhibits