FY 2025
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) 2025 a total of 456 positions (including 312 attorneys), 375 full-time equivalents (FTE), and $143,540,000.[1]

Electronic copies of the DOJ's Congressional Budget Justifications and Capital Asset Plan and Business Case exhibits can be viewed or downloaded from the Internet using the Internet address: https://www.justice.gov/doj/budget-and-performance

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 cyber-enabled threats to national security using all available tools, by investigating, prosecuting, and otherwise disrupting cyber threat actors with United States Government, foreign, and private sector partners;
- 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

[1] Within the totals outlined above, NSD has included a total of 26 positions, 26 FTE, and $15,822,000 for Information Technology (IT), and amounts included herein referring to the FY 2024 Continuing Resolution reflect an Annualized Continuing Resolution level.

the effectiveness of DOJ's national security efforts by ensuring greater coordination and unity of purpose between prosecutors, law enforcement agencies, intelligence attorneys, and the IC.

NSD is comprised of the following offices and sections:

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

- Providing advice and contributing to the interagency development of the Department of Treasury's (TREAS) implementation of the outbound-investment program under Executive Order 14105 (August 9, 2023), which regulated United States investments in certain technology sectors in countries of concern;

- 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 (April 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;

- Negotiating and monitoring transactions approved pursuant to both the CFIUS and Team Telecom processes for compliance with any mitigation agreements, and investigating and undertaking enforcement actions, when appropriate, for breaches of agreements and other violations;

- Addressing national security threats posed by foreign-sourced technology, software, services, and equipment through the interagency exercise of a range of information and communications technology and services (ICTS) supply-chain authorities and other authorities, including making referrals to the Department of Commerce (DOC) under Executive Order 13873 (May 15, 2019) and Executive Order 14034 (June 9, 2021), making referrals to the Federal Acquisition Security Council, and contributing to determinations to add equipment and services to the FCC's Covered List; and

- Providing legal and litigation advice and policy support on broader legislative and policy matters involving issues at the intersection of national security, technology, and business, trade, and investment, including developing and commenting on proposed legislation and regulations, executive orders, National Security Council (NSC) policy committees, congressional briefings, international engagements with foreign partners and allies, and public outreach.

4. Cyber Threats to National Security.

- Developing and supervising the investigation, prosecution, and disruption of cyber-enabled attacks, theft, intelligence-gathering, foreign malign influence and related cases through coordinated efforts and close collaboration with DOJ leadership, the FBI, the IC, and the 94 USAOs;

- Coordinating, developing, and supervising national strategies for combating cyber-enabled attacks, intelligence-gathering, malign influence;

- Providing advice and assistance to prosecutors nationwide regarding the application of CIPA in cyber-related investigations;

- Coordinating with interagency and foreign partners the use of all tools to protect United States and allied national assets from state-sponsored and other cyber threats to national security, including use of law enforcement tools, economic sanctions, and diplomatic solutions; and

- Conducting corporate and community outreach relating to cybersecurity.

5. **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.

6. **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, and offering training to, interagency, foreign governmental, and private partners to assist United States citizen terrorism victims and help make terrorism prosecutions worldwide more trauma-informed and victim-centered;

- 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.

7. **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 February 2023, DOJ charged over 75 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 41-49.

- **January 6 – Capitol Riot Investigation.** In connection to the breach of the United States Capitol on January 6, 2021, the USAO for the District of Columbia is tracking that since January 2023, an additional 230 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. This is in addition to the roughly 480 individuals who pleaded guilty prior to January 2023. These numbers reflect total defendants charged for conduct related to the Capitol Breach – only a portion of these defendants have been further classified as domestic violent extremism (DVE)-related by the FBI. Relevant case examples related to January 6th are detailed on page 40.

- **Espionage Enforcement.** NSD continues 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 pages 32-33.

- **Combating Foreign Malign Influence.** NSD continues to combat foreign malign influence through, among other things, aggressive FARA enforcement. In FY 2023, NSD's FARA Unit conducted 25 inspections of registrants' books and records to ensure their continuing compliance with the statute—the largest number of inspections since 1985. As a result of these and other enforcement efforts, 113 new entities registered under FARA during FY 2023. Relevant foreign malign influence case examples are detailed on page 35.

- **Export Controls and Sanctions Enforcement.** NSD continues its rigorous enforcement of export controls and sanctions, including sanctions against Russia, Iran, China, and the Democratic People's Republic of DPRK (DPRK). Relevant export control and sanction enforcement case examples are detailed on pages 35-36.

- **National Security Cyber Investigations.** NSD, now acting through NatSec Cyber, continues to focus resources on disrupting and deterring adversaries' efforts to harm United States national security through cyber intrusions and attacks. NSD has been an integral part of a larger transformation in the Federal Government's response to significant cyber incidents by using traditional law enforcement tools to investigate and disrupt nation state actors. NSD's primary focus is to disrupt state-sponsored malicious cyber activity by using legal tools such as seizure of infrastructure and targeted sharing with private sector and United States Government and foreign partners of threat intelligence gathered as a result of NSD's criminal investigations. This threat intelligence provided the basis for NSD court-authorized disruption operations such as the 12 botnet takedowns or similar court-authorized disruption operations since 2018, and also enabled other government agencies to deploy their respective tools and authorities through technical operations, intelligence operations, sanctions, trade remedies, and diplomatic efforts. Sharing threat intelligence developed through national security investigations also empowers private sector network defenders, encourages victim reporting and cooperation, and serves to educate the American public about cyber threats, thereby enhancing the nation's collective cybersecurity. In parallel to these efforts, NSD works to develop prosecutable cases against the same actors, including approximately 40 prosecutions since the inception of NSD's cyber program in 2014. NSD plays a critical role in driving a whole-of-government response and supporting private sector partnerships. Such efforts demand considerable resources and are essential to an effective response. Relevant national security cyber case examples are detailed on pages 54-56.

- **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 continues to prioritize cases involving unauthorized disclosures of classified information in the mass media. For example, in April 2023, Jack Douglas Teixeira was charged in the District of Massachusetts for unauthorized retention and transmission of national defense information that was posted on the Internet.

- **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 and 3% more from FY 2022 to FY 2023 regarding mergers, acquisitions, and investments;

    - NSD led approximately 16.2% of the cases in which a Joint Voluntary Notice (JVN) was filed with CFIUS in FY 2023. In approximately 82% of DOJ co-lead cases closed, the transaction was prohibited, abandoned, or mitigated, based on national security risks identified by NSD, up from 40% in FY 2022. Out of all CFIUS cases mitigated, DOJ co-led 21% of such cases;

    - NSD also led (on behalf of DOJ) approximately 6% in FY 2023 (down from 26% since FY 2022) 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 co-led several particularly challenging cases in FY 2023. In one case, NSD was able to resolve national security risks that arose when a Chinese-based company purchased a network of private schools in the United States. NSD was able to craft mitigation that ensured no student data would be accessible to the Chinese company or that the parent company had a role in school curriculum.

        - NSD has continued to expand its international outreach efforts with allied countries in order to promote and strengthen those countries' investment screening processes. NSD met with counterparts in Belgium, Sweden, the United Kingdom, and Spain, among other countries, in FY 2023.

    - 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 18% fewer applications in FY 2023 than in FY 2022, NSD led or co-led 100% of the reviews for FCC referrals to Team Telecom for applications of licenses.

- Team Telecom recommended in FY 2022 to the FCC that 70% of the reviewed and completed applications (stemming from 43 FCC referrals that involved a total of 89 telecommunications authorizations, cable landing licenses, and petitions for declaratory ruling) be granted contingent on mitigation measures. NSD either led or co-led these cases.

- In FY 2023, Team Telecom also stood up its process to review existing FCC licenses that it or its previous ad hoc predecessor reviewed but now present new or additional national security or law enforcement risk or whether the license holder has material noncompiled with existing mitigation terms. During FY 2023, Team Telecom initiated 10 such reviews, all of which remain ongoing.

- NSD continues to provide significant assistance to the DOC 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 seven referrals to the Secretary of Commerce which identify 15 companies of concern for investigation, as well as two referrals to the FASC identifying four companies of concern for investigation. To date, NSD remains one of two United States Government entities to make a referral pursuant to these new authorities and is currently developing additional referrals for Commerce and FASC review;

- NSD led and completed 39 CFIUS joint voluntary notice cases and 102 Team Telecom cases in FY 2023 that resulted in 27 new national security agreements that NSD negotiated and entered with companies, and that NSD will monitor for compliance going forward. NSD also conducted approximately 52 in-person or virtual mitigation compliance site visits in FY 2023 (41% increase from FY 2022) to monitor companies' compliance. The total number of such agreements monitored by NSD is currently 199, which reflects an approximate 85% increase in complex mitigation matters and 12% increase in active agreements from FY 2020 to FY 2022. This significant increase in complex mitigation matters reflects an increase in monitoring site visits, growth of new mitigation agreements, and a surge in agreement terminations. A total of 32 agreements were terminated in FY 2022 and 16 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;

- Starting in FY 2022 and continuing in FY 2023, NSD led a CFIUS penalty proceeding to levy the largest ever financial penalty for violations of national security commitments. NSD further reviewed, on behalf of DOJ, for concurrence an additional three penalty proposals by other members of CFIUS; and

- In FY 2023, NSD has conducted approximately 52 site visits to companies subject to national security commitments under both Team Telecom and CFIUS. These site visits assess compliance of those commitments and have led to further actions by companies to reduce risks to national security.

- **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 2022, the number of Section 702 targets increased roughly 165%. The substantial growth of NSD's Section 702 oversight program and the resulting impact on NSD's resources is also apparent from the over 700% increase in the number of matters handled by the Office of Intelligence (OI), the NSD component that oversees this program, from FY 2014 through FY 2023. 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 CY 2021 and has continued to increase each year since then. The yearly increase from CY 2022 through CY 2023 exceeded 8% and OI expects the increase in such compliance investigations by OI will continue in 2024.
    - Additionally, in CY 2019, NSD conducted over 30 reviews at IC agency headquarters locations and just under 30 reviews of 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 CY 2022 exceeded those levels with NSD completing 230 reviews at IC agency headquarters and 31 at FBI field offices. In CY2023, NSD completed 254 oversight reviews. This includes reviews at IC components and the USAOs, as part of NSD's CLOUD Act oversight.

- **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, 2022, and 2023. The accuracy and completeness reviews are resource intensive and sometimes involve travel by teams of OI personnel to FBI field offices to review relevant information. In total, NSD completed 41 accuracy and completeness reviews in CY 2022. In 2023, NSD completed 36 such reviews of 97 FISA dockets. Where possible, NSD intends to continue 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 by the applicable IC agencies (NSA, CIA, FBI, and NCTC). During CY 2018 – CY 2021, NSD identified a number of FBI query-related compliance issues. During CY 2021, NSD conducted oversight reviews of multiple FBI field offices, 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 FBI to include 28 reviews in CY 2022, and 36 reviews in CY 2023. These efforts include audits of many 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.

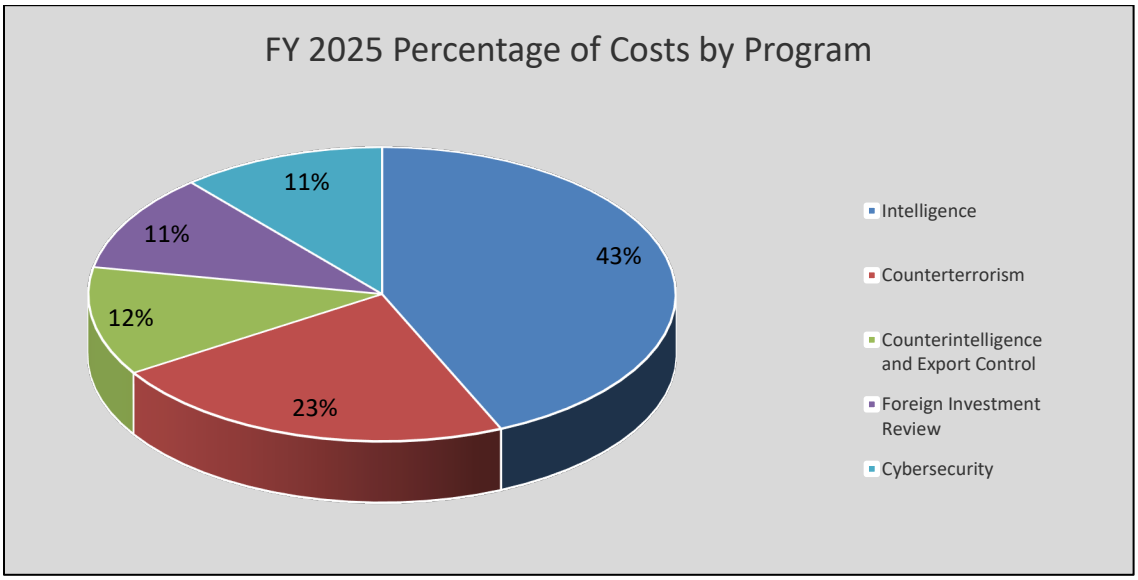
- **Assisting Victims of Overseas Terrorism.** In FY 2020 - FY 2023, NSD's Office for Justice of Victims of Overseas Terrorism (OVT) continued to support United States victims of international terrorism by providing them with foreign legal system information and communicating with foreign counterparts around the world, such as Bangladesh, Belgium, France, Germany, Indonesia, Israel, Kenya, New Zealand, and the United Kingdom. In FY 2022 - FY 2023, OVT provided travel assistance to facilitate the foreign trial attendance of multiple victims of the 2016 Nice and Brussels attacks. Trial attendance can prove to be an important element of the victim's journey, can help the victims seek accountability, and help them understand what happened and that they are part of a larger community.

- **Providing Training to Domestic and International Partners.** In FY 2020 - FY 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 European Network for Victims Rights. OVT provided in-person training and information about OVT's mission and subject matter to Kenyan partners in FY 2022 and Sri Lankan and Maldivian counterparts in FY 2023, and to the United Nations first Internal Congress for Victims of Terrorism in FY 2022. OVT also provided virtual victim and witness assistance training to DOJ's Office of Prosecutorial Development, Assistance, and Training in FY 2023.

- **Supporting International Cooperation on Victims of Terrorism.** OVT has cooperated with the United States Department of State's (DOS) Bureau of Counterterrorism on 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 their September 2022 International Congress 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 countering foreign malign influence

One of NSD's top priorities is the protection of national assets through counterintelligence investigations and prosecutions, enforcement of export controls and sanctions, and countering foreign malign influence. 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. In February 2023, the DOJ and the DOC launched the Disruptive Technology Strike Force. Under the leadership of NSD and Commerce's Bureau of Industry and Security, the strike force brings together experts throughout the United States Government to target illicit actors and protect critical technological assets from being acquired by nation-state adversaries.

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, 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.

Among these authorities is NSD's continued aggressive enforcement of and education about FARA. FARA requires certain agents of foreign principals who are engaged in political activities or other activities specified under the statute to register and make periodic public disclosures about their relationship with the foreign principal. Thus, FARA is an important tool to identify foreign influence in the United States and address threats to national security. Since 2016, more than 100 new registrants have registered pursuant to FARA each year.

New National Security Cyber Section for Cyber-Related Investigations and Prosecutions

Among the most significant challenges that NSD continues to face is the rapid expansion, evolution, and sophistication of cyber threats to national security. Cyber threats with national security implications are evolving and growing; foreign nation-states increasingly use cyber-enabled means to steal export-controlled technology, intellectual property, trade secrets, and personally identifying information; exert malign influence; and hold United States critical infrastructure at risk to destructive or disruptive attacks. In addition, there is a rising "blended threat" under which nation-states and criminal actors are forming alliances that enable malicious cyber activity to proliferate in ways that pose profound national security implications. This threat includes both nation-state directed cyber activity as a means to generate income for those governments, as well as nation states that provide safe harbor for cyber criminals and turn a blind eye to their activities, often in exchange for such criminals being "on call" for those governments' intelligence services.

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 for a dedicated 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.

To meet these many challenges, as well as the strategic objectives set out in the President's National Cybersecurity Strategy and the related Implementation Plan, NSD changed its organizational structure to add a new National Security Cyber Section (NatSec Cyber). This change will allow NSD to increase the volume and speed of disruption campaigns and prosecutions of foreign intelligence service-employed hackers, state-sponsored cybercriminals, associated money launderers, and other cyber-enabled threats to national security.

This reorganization and increased focus on cyber-enabled threats allows NSD 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, data-intensive, and complex investigative and prosecutorial work involving substantial resources. Among many challenges, national security cyber threat investigations frequently present novel policy, technical, operational, and legal issues; difficulties of attribution; challenges in obtaining and using electronic evidence; challenges in responding to the speed and global span of malicious cyber activity; and the need to balance appropriately various law enforcement, intelligence, and diplomatic interests.

For example, this past year, the United States Government and foreign and private sector partners highlighted a then-recently discovered cluster of activity of interest associated with a People's

Republic of China (PRC) state-sponsored cyber actor, also known as Volt Typhoon, which targets computer networks across United States and allied critical infrastructure sectors. The Volt Typhoon actors are adept at evading network defenders through a technique of "living off the land," which uses built-in network administration tools to perform their objectives, as opposed to custom tools that are easier to identify as anomalous network activity. As described in the IC's February 2023 Annual Threat Assessment, the PRC would consider leveraging these accesses to "impede United States decision making, induce societal panic, and interfere with the deployment of United States forces" in the event the PRC anticipated an imminent major conflict with the United States. NSD, working alongside the FBI and other federal and private sector partners, is at the forefront of investigating and disrupting such activity on domestic networks using unique law enforcement tools and by sharing best practices of NSD's investigations with network defenders.

Additionally, recent ransomware attacks underscore the growing threat that ransomware and digital extortion pose to the United States, 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, often with partners in the IC and other relevant agencies, 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.

Further, with the increasing use, types, and value of virtual currency and digital assets 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.*, the DPRK utilizes virtual currency theft to support the regime's weapons program). Other hacking groups rely on virtual 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 investigating and 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 support the Department's National Cryptocurrency Enforcement Team, 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 24% 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 DOC for action under Executive Order 13873 or to the FBI to make "determination" that the foreign adversary connected entity be added to the FCC's Covered List under the Secure and Trusted Communications Networks Act (STCNA), 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 20% more submissions than in FY 2021 and 66% more than in FY 2020 regarding mergers, acquisitions, and investments. However, in FY 2023 the Committee reviewed 9% fewer submissions than in FY 2022. In FY 2023, NSD led approximately 16% of CFIUS cases in which a Joint Voluntary Notice was filed. Further, NSD led 28% of the overall CFIUS cases (down from 44% in FY 2022) that resulted in transactions being prohibited, abandoned, or mitigated, based on national security risk identified by NSD. In FY 2023, NSD led approximately 6% (down from 26% in FY 2022) 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 and serves as DOJ's representative on CFIUS. The chief drivers of CFIUS-related workload increase that anticipated —and the corresponding demands on resources—are filings that had been deferred because of the challenges posed by the COVID-19 pandemic and related supply chain disruptions (drivers that are now receding in importance), 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 30% 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 2023 (that involved working a total of 102 applications from 66 referrals for telecommunications authorizations, cable landing licenses, and petitions for declaratory ruling) and recommended to the FCC that 70% of the total authorizations, licenses, and petitions for declaratory rulings be granted contingent on mitigation measures resulting in 17 new mitigation agreements. In the first quarter of FY 2024, NSD has led or co-led 13 FCC referrals made and has concluded 7 Team Telecom referral reviews (that involved a total of 11 telecommunications authorizations, cable landing licenses, and petitions for declaratory ruling), resulting in 1 new mitigation agreement (from 8 applications). Team Telecom continues to review 19 active referrals (25 active matters) and 6 existing FCC licenses that were previously reviewed by the Committee but may present new or additional national security or law enforcement risk as well. NSD also continues to monitor compliance with all mitigation agreements (199) 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 and complexity of CFIUS and Team Telecom cases increases, the volume of mitigation agreements that NSD must monitor will also steadily increase. Although in FY 2023, NSD terminated 16 mitigation agreements that were no longer necessary, 27 new agreements were signed, which resulted in a total of approximately 199 agreements that were active at the end of the fiscal year (approximately 6% growth from FY 2022). Of the CFIUS and Team Telecom cases discussed above, 10 new CFIUS agreements and 17 new Team Telecom originated agreements went into effect, originating from 9 CFIUS NSD-led case and 15 Team Telecom referrals in FY 2023. These national security agreements that NSD negotiated and entered with companies will be monitored by FIRS 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. In recent years, NSD has worked with DOJ components and CFIUS agencies to identify bankruptcy proceedings that may involve national security concerns and potential foreign investment. This initiative has resulted in several filings before bankruptcy courts notifying the courts of potential CFIUS and Team Telecom processes following the resolution of bankruptcy proceedings.

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 DOC draft regulations to implement this new authority and continues to assist DOC administer its ICTS Supply Chain risk management regulatory process. In FY 2023, NSD submitted two referrals to the DOC under the new authority—and to date NSD's referrals are the only referrals that Commerce has received from the interagency. All ten interagency referrals have been investigated, drafted, and submitted all or in part by FIRS. In addition, since the passage of the Federal Acquisition Supply Chain Security Act, FIRS has supported the Federal Acquisition Security Council (FASC), 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. FIRS did not make any referrals to the FASC during FY 2023 but has one such referral in draft.

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 non-attorney personnel and technology resources have not kept pace with the expansion of its mission, and the lack of these resources is increasingly affecting FIRS's ability to protect our national assets from foreign adversaries. FIRS currently relies on manual data entry to track all case related information and records, resulting in significant inefficiencies, and diverting resources from its substantive work to protect national security. Furthermore, FIRS is reliant on its attorneys to perform much of this data entry, as well as a range of other administrative, paralegal, and analytic functions, placing a heavy burden on the existing workforce to perform tasks requiring a broad, mixed skillset. To meet this challenge, NSD has been actively pursuing the acquisition of a modern, dynamic case-management system and additional contractor support personnel. This system, which is expected to be funded with base NSD resources and developed and launched in FY 2024, 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.

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 26th Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of FISA, covering the period of December 2020 – May 2021: "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 165% from CY 2014 through CY 2022. 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. The number of targets reported for CY 2022 grew 5.5% over the number reported for CY 2021. NSD anticipates that the upward trend will continue. The substantial growth of NSD's Section 702 oversight program and the resulting impact on NSD's resources is also apparent from the over 700%[2] increase in the number of matters handled by OI, the NSD component that oversees this program, from FY 2014 through FY 2023. 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 CY 2021 and has continue to increase each year since then. The yearly increases from CY 2022 through CY 2023 exceeded 8% and OI expects the increase in such compliance investigations by OI will continue in 2024. In addition, as part of its oversight of the IC's use of Section 702, OI dedicates substantial resources to auditing the IC's querying of unminimized information collected pursuant to Section 702.

The President's own Intelligence Advisory Board (PIAB) and Intelligence Oversight Board (IOB) in a report issued publicly on July 31, 2023, strongly urged Congress to reauthorize Section 702 with additional compliance-related reforms. They noted that the failure to reauthorize Section 702 would be "one of the worst intelligence failures of our time." PIAB Report at 2. In a statement from National Security Advisor Jake Sullivan and Principal Deputy National Security Advisor Jon Finer on that same day, they noted that Section 702 of FISA is one of the nation's most critical intelligence tools used to protect the homeland and the American people from threats posed by the People's Republic of China, rally the world against Russian atrocities in Ukraine, locate and eliminate terrorists intent on causing harm to America, enable the disruption of fentanyl trafficking, and mitigate the Colonial Pipeline ransomware attack. In a statement issued by the White House on July 31, 2023, the White House noted that they agreed with the unanimous conclusion reached by the President's Intelligence Advisory Board that Section 702 should be reauthorized "with measures that build on proven reforms to enhance compliance and oversight."

[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 through and CY 2023, NSD conducted query oversight reviews of multiple FBI field offices and 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 2024. 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 223 FISA applications between May 2020 through December 2023. 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 2023, 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 FISA 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 June 2022, NSD formed a domestic terrorism unit, within CTS, to further ensure national-level coordination and tracking of all domestic terrorism cases. Relatedly, in November 2022, the Justice Manual was revised to incorporate these new reporting requirements and requires additional approval of certain DT/DVE matters by NSD.[3] 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.

In June 2023, the Office of the Inspector General published its audit of the Department's strategy to address the DVE threat.[4] The audit made seven recommendations to the DOJ. The recommendations centered around building and empowering the DT Unit through additional training, coordination, and data tracking mechanisms.

With respect to international terrorism, the IC predicts 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,

3 JUSTICE MANUAL 9-2.137: Notification, Consultation, and Approval Requirements in Matters Involving Domestic Violent Extremism, Including Domestic Terrorism.
4 UNITED STATES DEPARTMENT OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, No. 23-078, Audit of the Department of Justice's Strategy to Address the Domestic Violent Extremism Threat (June 2023).

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.

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.

Moreover, 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.

On October 7, 2023, Hamas perpetrated its most violent, large-scale terrorist attack to date, when Hamas sent armed operatives into Israel, where they murdered and kidnapped large numbers of civilians, including American citizens, and Israeli soldiers. As a result of the attack, Israel Defense Forces (IDF) launched a large-scale invasion within the Gaza Strip. The Israel-Hamas conflict has had global impacts – leading to an increase in both domestic and international terrorism-related conduct.

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 is the Department's primary expression of the following emphasized language in its FY 2022 - FY 2026 Strategic Plan, Objective 2.2: Counter Foreign and Domestic Terrorism, Strategy 2: Strengthen Federal, State, Local, Tribal, and International Counterterrorism Partnerships, "…And the Department will support foreign government efforts to investigate and prosecute, in their own courts, terrorists who threaten United States national security, through information sharing with foreign law enforcement, capacity building, and, ***where consistent with foreign law, the optional participation of United States victims of overseas terrorism in foreign justice processes.***"

OVT's mission is to support United States victims of terrorism overseas by helping them navigate foreign criminal justice systems and by advocating for their voices to be heard around the world. OVT advocates for United States victims and their families to obtain information, be present during foreign terrorism prosecutions, and have a voice during the proceedings, as permitted by foreign law. OVT further provides policy advocacy on overseas terrorism victims' issues both within the United States Government and throughout the world.

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 in 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 and 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 intensive victims' services during and leading up to foreign criminal justice proceedings and is committed to offering trauma-informed methods of interacting with victims. 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.

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 and the September 2023 Brussels sentencing, 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.	FTE	Dollars ($000)	
Countering National Security Cyber Threat	Additional resources to support NSD's countering national security cyber threats work	22	11	$5,000	60
	Grand Total: FY 2025 Enhancement Request	**22**	**11**	**$5,000**	

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] *$143,540,000* 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
2023 Enacted	434	354	$133,512,000
2024 Annualized Continuing Resolution	431	361	$133,512,000
Adjustments to Base and Technical Adjustments	3	3	$5,028,0000
2025 Current Services	434	364	$138,540,000
2025 Program Increases	22	11	$5,000,000
2025 Program Offsets	0	0	$0
2025 Request	456	375	$143,540,000
Total Change 2024-2025	**25**	**14**	**$10,028,000**

***National Security Division* - Information Technology Breakout (of Decision Unit Total)**	Direct Pos.	Estimate FTE	Amount
2023 Enacted	26	26	$15,822,000
2024 Annualized Continuing Resolution	26	26	$15,822,000
Adjustments to Base and Technical Adjustments	0	0	$0
2025 Current Services	26	26	$15,822,000
2025 Program Increases	0	0	$0
2025 Program Offsets	0	0	$0
2025 Request	26	26	$15,822,000
Total Change 2024-2025	**0**	**0**	**$0**

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-governmental 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 2023		**FY 2023**		**FY 2024**		**Current Services Adjustments and FY 2025 Program Changes**		**FY 2025 Request**	
Workload*										
Defendants Charged	**231**		**491**		**241**		**3**		**244**	
Defendants Closed	**206**		**454**		**216**		**3**		**219**	
Matters Opened	**551,090**		**713,893**		**551,181**		**36**		**551,217**	
Matters Closed	**550,810**		**713,333**		**550,883**		**33**		**550,916**	
FISA Applications Filed**	**CY 2023: 900**		**CY 2023: TBD**		**CY 2024: 900**		**0**		**CY 2025: 900**	
National Security Reviews of Foreign Acquisitions	**600**		**773**		**600**		**0**		**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)	354	133,512	358	133,512	361	133,512	14	10,028	375	143,540

*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		Target		Changes		Requested (Total)	
TYPE	STRATEGIC OBJECTIVE	PERFORMANCE	FY 2023		FY 2023		FY 2024		Current Services Adjustments and FY 2025 Program		FY 2025 Request	
Program Activity	Counterintelligence and Export Control and Foreign Investment Review		FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
			84	32,449	81	31,822	80	31,822	0	786	80	32,608
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%		96%		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%		96%		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	22		25		23		1		24	
Performance Measure:	2.1 Protect National Security	High priority national security reviews completed	150		479		175		0		175	
Program Activity	Intelligence and Counterterrorism		FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
			252	94,265	245	92,443	247	92,443	-1	2,305	246	94,748

PERFORMANCE AND RESOURCES TABLE												
Decision Unit: National Security Division												
RESOURCES ($ in thousands)			**Target**		**Actual**		**Target**		**Changes**		**Requested (Total)**	
TYPE	**STRATEGIC OBJECTIVE**	**PERFORMANCE**	**FY 2023**		**FY 2023**		**FY 2024**		**Current Services Adjustments and FY 2025 Program**		**FY 2025 Request**	
KPI:	2.2: Counter Foreign and Domestic Terrorism	Percent of counterterrorism defendants whose cases were favorably resolved	90%		100%		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	400		496		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 2023: 130		CY 2023: 245		CY 2024: 135		5		CY 2025: 140	
Program Activity	Cybersecurity		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
			18	6,798	32	9,247	34	9,247	15	6,937	49	16,184
Performance Measure:	2.4 Enhance Cybersecurity and Fight Cybercrime	Percentage of Cyber defendants whose cases were favorably resolved - *discontinued in FY24 and replaced with an interal measure*	90%		N/A - No cyber defendants' cases were closed in FY23		N/A		N/A		N/A	




PERFORMANCE MEASURE TABLE												
Decision Unit: National Security Division												
Performance Measures			FY 2015	FY 2016	FY 2017	FY 2018	FY 2019	FY 2020	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025
			Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Target	Target
2.1: Protect National Security	**Key Performance Indicator**	Percent of prosecutions brought against defendants engaged in a) hostile activities against national assets b) intelligence gathering or c) export violations that are favorably resolved	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	98%	96%	90%	90%
2.1: Protect National Security	**Key Performance Indicator**	Percent of DOJ-led foreign investment cases that were adjudicated favorably	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	100%	100%	100%	97%	97%
2.1: Protect National Security	**Performance Measure**	Percentage of CE defendants whose cases were favorably resolved	100%	100%	100%	100%	99%	95%	85%	98%	96%	90%	90%
2.1: Protect National Security	**Performance Measure**	Percentage of CE cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	100%	100%	100%	100%	100%	100%	100%	100%	100%	99%	99%
2.1: Protect National Security	**Performance Measure**	FARA inspections completed	14	14	15	15	20	9	20	22	25	23	24
2.1: Protect National Security	**Performance Measure**	High priority national security reviews completed	197	220	212	370	354	373	453	467	479	175	175
2.2: Counter Foreign and Domestic Terrorism	**Key Performance Indicator**	Percent of counterterrorism defendants whose cases were favorably resolved	98%	99%	91%	91%	95%	89%	99%	99%	100%	90%	90%
2.2: Counter Foreign and Domestic Terrorism	**Key Performance Indicator**	Number of individuals in the Department trained to prosecute domestic terrorism and domestic violent extremism	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	NA - New measure in FY22	1,674	1,073	496	400	400
2.2: Counter Foreign and Domestic Terrorism	**Performance Measure**	Percentage of CT cases where classified information is safeguarded (according to CIPA requirements) without impacting the judicial process	100%	100%	100%	100%	100%	100%	100%	100%	100%	99%	99%
2.2: Counter Foreign and Domestic Terrorism	**Performance Measure**	Intelligence Community Oversight Reviews	CY 2015: 100	CY 2016: 110	CY 2017: 102	CY 2018: 110	CY 2019: 97	CY 2020: 70	CY 2021: 117	CY 2022: 130	CY 2023: 245	CY 2024: 130	CY 2024: 130
2.4: Enhance Cybersecurity and Fight Cybercrime	**Performance Measure**	Percentage of Cyber defendants whose cases were favorably resolved - *discontinued in FY24 and replaced with an interal measure*	100%	100%	100%	100%	100%	NA - No Cyber defedants' cases were closed in FY20	100%	100%	NA - No Cyber defedants' cases were closed in FY23	N/A	N/A

3. Performance, Resources, and Strategies

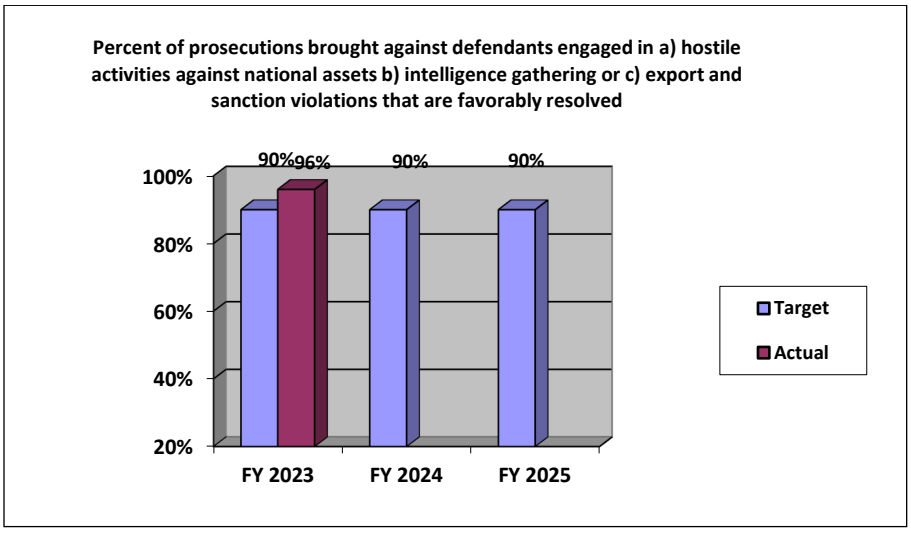
For performance reporting purposes, resources for NSD are included under DOJ Strategic Goal 2: Keep our Country Safe. Within these goals, NSD resources address Strategic Objectives 2.1: Protect National Security, 2.2: Counter Foreign and Domestic Terrorism, and 2.4: Enhance Cybersecurity and Fight Cybercrime.

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 2023 Target: **90%**
FY 2023 Actual: **96%**
FY 2024 Target: **90%**
FY 2025 Target: **90%**
Discussion: The FY 2025 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

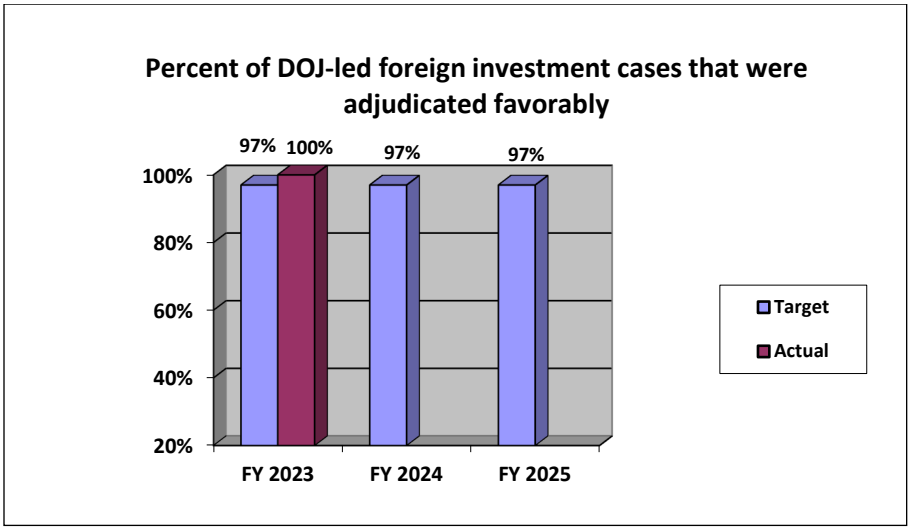
Export Control Reform Act (ECRA), and the International Emergency Economic Powers Act (IEEPA), excluding those violations of the AECA having no relationship to foreign relations.

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 2023 Target:	**97%**
FY 2023 Actual:	**100%**
FY 2024 Target:	**97%**
FY 2025 Target:	**97%**

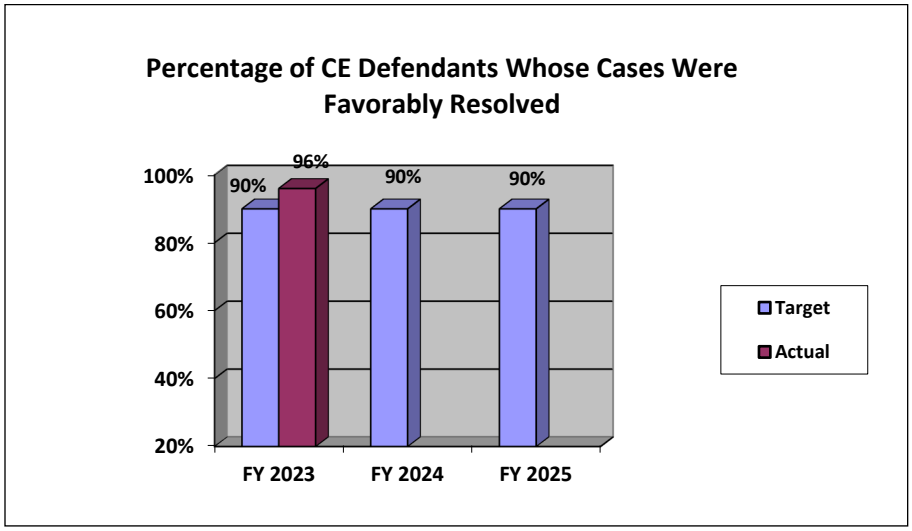
Discussion: The FY 2025 target is consistent with previous fiscal years.



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 2023 Target:	**90%**
FY 2023 Actual:	**96%**

FY 2024 Target: 90%
FY 2025 Target: 90%
Discussion: The FY 2025 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. Brown*: In December 2022, in the Middle District of Florida, Jeremy Brown was found guilty of possession of unregistered firearms and grenades; unlawful storage of explosive material; and willful retention of national defense information. This is an example of NSD's effective prosecution of those who unlawfully retain classified national defense information. Brown, a retired member of the United States Special Forces, retained highly sensitive information about DOD intelligence-gathering tactics, techniques, and procedures, including information about a human source that, if released, could have caused the source to be arrested, tortured, or killed. NSD assisted in the preparation of a criminal search warrant, which resulted in the recovery of this information, as well as classified litigation to protect our national security. Ultimately, with NSD's participation, Brown was convicted after a jury trial and sentenced to seven years and three months in prison.

- *United States v. Zheng*: In January 2023, in the Northern District of New York, Xiaoqing Zheng was sentenced to 24 months in prison for conspiring to steal trade secrets, knowing or

intending to benefit the People's Republic of China (PRC). This case demonstrates NSD's success in prosecuting economic espionage. Zheng, a former engineer at General Electric (GE), was convicted of conspiracy to commit economic espionage. NSD not only assisted in the investigation but played a key role in the trial, which established that Zheng and others in China conspired to steal GE's trade secrets relating to ground-based and aviation-based turbine technologies, knowing or intending to benefit the PRC and one or more foreign instrumentalities, including China-based companies and universities that research, develop, and manufacture parts for turbines.

Highlights from Recent Export Control and Sanctions Enforcement Cases

- *United States v. Deripaska et al.*: In September 2022, in the Southern District of New York, the DOJ announced the unsealing of an indictment charging three citizens of the Russian Federation and one United States citizen with violating new United States sanctions against Russia. The investigation was coordinated through DOJ's Task Force KleptoCapture (TFKC), an interagency law enforcement task force dedicated to enforcing the sanctions, export controls, and economic countermeasures that the United States imposed in response to Russia's military invasion of Ukraine. According to court documents: Russian nationals Oleg Vladimirovich Deripaska and Natalia Mikhaylovna Bardakova and United States national Olga Shriki were charged with conspiring to violate United States sanctions imposed on Deripaska and one of Deripaska's corporate entities. Shriki was arrested. Shriki also was charged with obstruction of justice, based on deletion of electronic records relating to her participation in Deripaska's sanctions evasion scheme following receipt of a grand jury subpoena. Bardakova was charged with one count of making false statements to agents of the FBI. Additionally, Russian national Ekaterina Olegovna Voronina was charged with making false statements to agents of the Department of Homeland Security at the time of her attempted entry into the United States for the purpose of giving birth to Deripaska's child. Deripaska – the owner and controller of Basic Element Ltd., a private investment and management company for Deripaska's various business interests – was subjected to United States economic sanctions in 2018. The TREAS's Office of Foreign Assets Control (OFAC) designated Deripaska as a Specially Designated National in connection with its finding that the actions of the Russian Government with respect to Ukraine constitute an unusual and extraordinary threat to the national security and foreign policy of the United States. Deripaska was sanctioned for having acted on behalf of, directly or indirectly, a senior official of the Russian Government, as well as for operating in the energy sector of the Russian Federation economy.

- *United States v. Grinin et al.*: In December 2022, in the Eastern District of New York, in an example of Task Force KleptoCapture's mission to enforce Russian export restrictions, a 16-count indictment was unsealed charging five Russian nationals – including a suspected Federal Security Service (FSB) officer – and two United States nationals for a global procurement and money laundering scheme on behalf of the Russian government in which the defendants allegedly conspired to obtain military-grade and dual-use technologies from United States companies for Russia's defense sector, and to smuggle sniper rifle ammunition, in violation of United States sanctions imposed earlier in 2022. According to the indictment: Russian nationals Yevgeniy Grinin, Aleksey Ippolitov, Boris Livshits, Svetlana Skvortsova, and Vadim Konoshchenok, and United States nationals Alexey Brayman and Vadim

Yermolenko established a conspiracy to defraud the United States as to the enforcement of export controls and economic sanctions; to violate the Export Control Reform Act (ECRA); to smuggle goods; and to fail to comply with the Automated Export System relating to the transportation of electronics. The defendants unlawfully purchased and exported highly sensitive and heavily regulated electronic components, some of which could be used in the development of nuclear and hypersonic weapons, quantum computing, and other military applications. As alleged, the defendants were affiliated with Serniya Engineering and Sertal LLC, Moscow-based companies that operate under the direction of Russian intelligence services to procure advanced electronics and sophisticated testing equipment for Russia's military industrial complex and research and development sector.

- *United States v. British American Tobacco*: In April 2023, in the District of Columbia, British American Tobacco (BAT) and its subsidiary, BAT Marketing Singapore (BATMS), agreed to pay combined penalties of more than $629 million to resolve charges by United States authorities arising out of the companies' scheme to do business in the DPRK through a third-party company in Singapore, in violation of the bank fraud statute and the International Emergency Economic Powers Act (IEEPA). It was the largest DPRK sanctions penalty in the history of the DOJ. BATMS pleaded guilty to a criminal information charging BAT and BATMS with conspiracy to commit bank fraud and conspiracy to violate IEEPA. BAT entered into a deferred prosecution agreement related to the same charges. Between 2007 and 2017, BAT and BATMS engaged in an elaborate scheme – running payments for tobacco sold to the DPRK entities through the third-party company, resulting in approximately $418 million of United States dollar cash and correspondent banking transactions for the DPRK. The TREAS also announced a civil enforcement action against BAT and BATMS. Separately, charges also were unsealed against a DPRK banker and Chinese facilitators for their roles in the illicit sale of tobacco products in the DPRK. DPRK banker Sim Hyon-Sop and Chinese facilitators Qin Guoming and Han Linlin were indicted for a multi-year scheme to facilitate DPRK tobacco sales. The defendants conspired to purchase leaf tobacco for DPRK state-owned cigarette manufacturers and used front companies and false documentation to cause United States financial institutions to process transactions worth approximately $74 million, which otherwise would have been frozen, blocked, or declined, had institutions known the transactions were connected to trade with the DPRK.

- *United States v. Ahmad et al.*: In April 2023, in the Eastern District of New York, a nine-count indictment was unsealed charging Nazem Ahmad and eight co-defendants with conspiring to defraud the United States and foreign governments, evade United States sanctions and customs laws, and conduct money laundering transactions by securing goods and services for the benefit of Ahmad – who was sanctioned by the United States for being a financier for Hezbollah, a foreign terrorist organization. According to court documents: Despite being sanctioned and prohibited from engaging in transactions with United States persons since December 2019, Ahmad and his co-conspirators relied on a complex web of business entities to obtain valuable artwork from United States artists and art galleries and to secure United States-based diamond-grading services – all while hiding Ahmad's benefit from these activities. Approximately $160 million worth of artwork and diamond-grading services were transacted through the United States financial system. One defendant was arrested in the United Kingdom at the request of the United States; Ahmad and the remaining

defendants remain at large. The United States Government obtained seizure warrants for millions of dollars in assets.

Highlights from Recent Foreign Malign Influence Cases

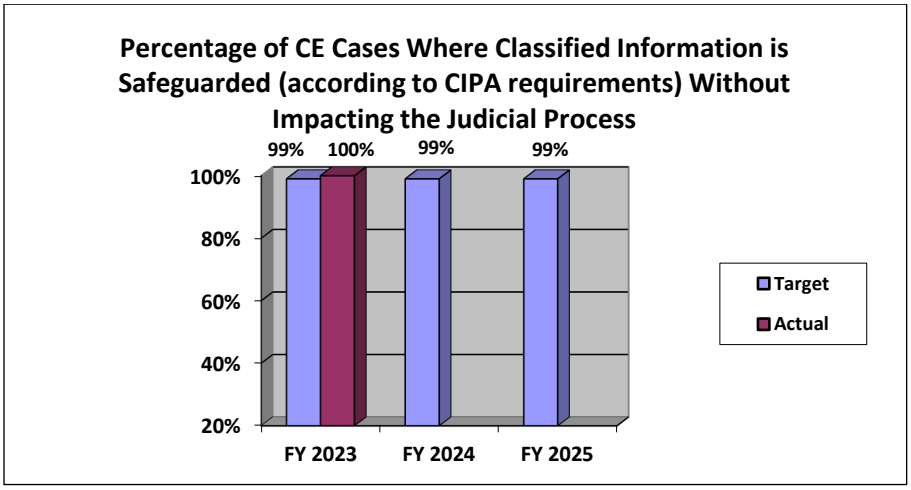
- *United States v. Ionov et al.*: In April 2023, in the Middle District of Florida, a grand jury returned a superseding indictment charging four United States citizens and three Russian nationals – including two Russian intelligence officers – with working on behalf of the Russian Government and in conjunction with Russia's FSB to conduct a multi-year foreign malign influence campaign in the United States. The indictment alleges that the Russian defendants recruited, funded, and directed United States political groups to act as unregistered agents of the Russian government, sow discord, and spread pro-Russian propaganda. According to the indictment, Moscow resident Aleksandr Ionov was the president of the Anti-Globalization Movement of Russia (AGMR), an organization funded by the Russian Government. Ionov utilized AGMR to carry out Russia's malign influence campaign. Ionov's influence efforts were directed by Moscow-based FSB officers, including Aleksey Sukhodolov and Yegor Popov. Ionov, Sukhodolov, and Popov conspired to directly influence democratic elections in the United States by clandestinely funding and directing the political campaign of a particular candidate for local office in St. Petersburg, Florida, in 2019. Moreover, from at least November 2014 until July 2022, Ionov recruited members of separatist political factions within the United States – including groups in Florida, Georgia, and California – to act as agents of Russia in the United States, including indicted United States citizen defendants Omali Yeshitela, Penny Joanne Hess, Jesse Nevel, and Augustus Romain Jr.

- *United States v. Ji*: In January 2023, in the Northern District of Illinois, Ji Chaoqun was sentenced to eight years prison following his conviction for acting as an agent of the People's Republic of China (PRC) without first notifying the Attorney General and for making a materially false statement to the United States Army. Ji's conviction was the result of a multi-jurisdiction investigation in which NSD helped coordinate and prepare multiple successful prosecutions of a Chinese intelligence officer and his assets, highlighting NSD's central role in responding to nation-state threats. Evidence presented at trial revealed that Ji worked at the direction of high-level intelligence officers in the Jiangsu Province Ministry of State Security (JSSD), a provincial department of the PRC Ministry of State Security. Ji, a Chinese citizen residing in Chicago, was tasked by Xu Yanjun, a Deputy Division Director within the Ministry of State Security, with providing biographical information on certain individuals for possible recruitment by the JSSD and also joined the United States Army with the long-term goal of providing the PRC with sensitive United States information. This tasking was part of an effort by the Jiangsu provincial department to obtain access to advanced aerospace and satellite technologies being developed by companies within the United States. Xu Yanjun was sentenced to 20 years in federal prison after being convicted in the Southern District of Ohio of conspiracy and attempting to commit economic espionage and theft of trade secrets.

- *United States v. Liang*: In May 2023, in the District of Massachusetts, United States citizen Litang Liang was indicted for conspiracy and acting as an agent of a foreign government without providing notice to the Attorney General. According to the indictment, from 2018 to

2022, Liang acted within the United States as an agent of the People's Republic of China (PRC). Liang's acts included providing the PRC government with information on Boston-area individuals and organizations, organizing a counter-protest in the United States against pro-democracy dissidents, providing photographs of and information about United States-based dissidents to PRC Government officials, and providing the names of potential recruits to the PRC Ministry of Public Security.

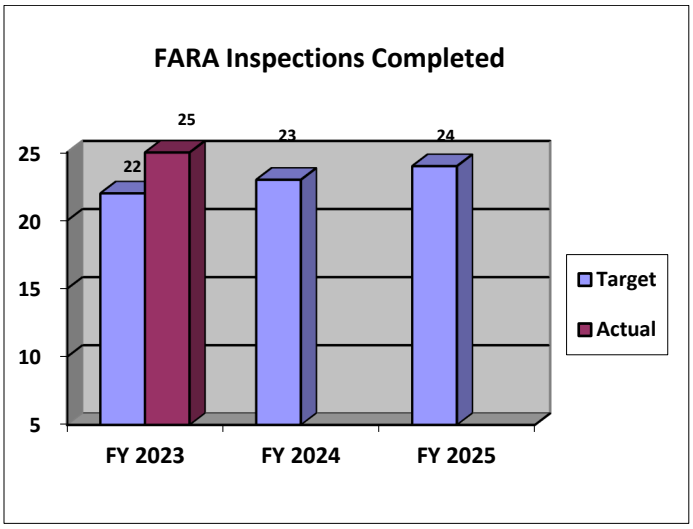
Measure: **Percentage of CE Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2023 Target: **99%**
FY 2023 Actual: **100%**
FY 2024 Target: **99%**
FY 2025 Target: **99%**
Discussion: The FY 2025 target is consistent with previous 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.

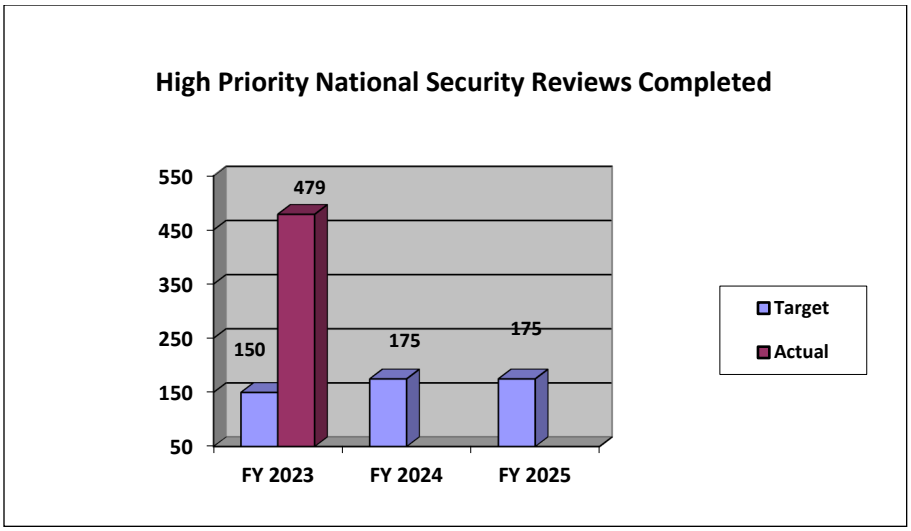
Measure: **FARA Inspections Completed**

FY 2023 Target: **22**
FY 2023 Actual: **25**
FY 2024 Target: **23**
FY 2025 Target: **24**
Discussion: The FY 2025 target is consistent with 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 2023 Target: **150**
FY 2023 Actual: **479**
FY 2024 Target: **175**
FY 2025 Target: **175**
Discussion: The FY 2025 target is consistent with the previous fiscal year. NSD will continue to work with its partners to perform these high priority reviews. Note: This measure is now tracked on a fiscal year basis for ease of reporting.



Data Definition: High Priority National Security Reviews include:

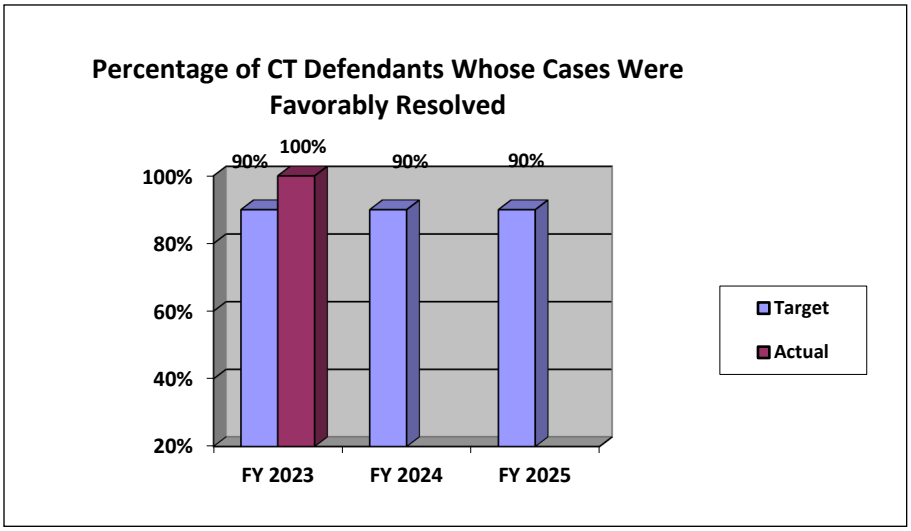
1. CFIUS case reviews of transactions in which DOJ is a co-lead agency in CFIUS due to the potential impact on DOJ equities;
2. CFIUS case reviews, which result in a mitigation agreement to which DOJ is a signatory;
3. Team Telecom case reviews which result in a mitigation agreement to which DOJ is a signatory;
4. Mitigation monitoring site visits;
5. Supply-chain referrals and determinations by DOJ (including referrals to the DOC 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 2023 Target: 90%
FY 2023 Actual: 100%
FY 2024 Target: 90%
FY 2025 Target: 90%
Discussion: The FY 2025 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.

CTS Leads Prosecution of 11 Charged and Five Sentenced to Life in Prison in Connection with Plot to Kill Haitian President

On July 7, 2021, President Jovenel Moise of Haiti was assassinated inside his home in Port-au-Prince, Haiti; the First Lady was shot multiple times and grievously injured, but survived the attack. Investigation to date has revealed that Moise's assassination was organized and coordinated largely by individuals operating security and government contracting businesses located in the Southern District of Florida, with critical assistance from co-conspirators in Haiti

and Colombia. The plot was financially motivated, as the conspirators sought to replace President Moise with a new President who would direct valuable governmental contracts to the companies and individuals involved in the plot.

From the earliest stages of the case, CTS has played a leading role, with CTS trial attorneys traveling to the Southern District of Florida and to Haiti on multiple occasions to coordinate with law enforcement and foreign investigative partners; identify, obtain, and exploit physical evidence; identify relevant witnesses and conduct interviews; and develop a theory of the case. This led to CTS attorneys drafting a series of prosecution memoranda and superseding indictments in close coordination with AUSAs in the Southern District of Florida, which to date has resulted in four superseding indictments. Those indictments have charged a total of 11 individuals with their roles in the Moise assassination plot, including on charges relating to providing and conspiring to provide material support and resources resulting in death; conspiring to murder or kidnap outside the United States; and violating or conspiring to violate the Neutrality Act by taking part in a military expedition against Haiti.

CTS continues to spearhead all litigation under CIPA and has filed and will defend briefing under Section 4 of CIPA and related litigation. In addition, CTS has taken a laboring oar in coordinating and reviewing unclassified discovery, and CTS paralegals are providing crucial assistance in managing massive volumes of data for production to the case's discovery coordinator. Finally, CTS is also playing a primary role in developing and maintaining relationships with cooperating witnesses, which has resulted in six guilty pleas to date. Of those six defendants, five have been sentenced to terms of life in prison. The five remaining defendants are expected to proceed to trial, which is presently set for May 6, 2024. CTS attorneys will serve as trial counsel during the proceedings and all related litigation.

CTS Integral to Iranian Revolutionary Guard Corps Member Charged for Plot to Murder the Former National Security Advisor

On August 10, 2022, in the District of Columbia, a criminal complaint was unsealed charging Iranian national Shahram Poursafi (Poursafi) in connection with a plot to murder the former National Security Advisor, John Bolton. Poursafi was using interstate commerce facilities in the commission of murder-for-hire and providing and attempting to provide material support to a transnational murder plot. Poursafi is a member of the Iranian Revolutionary Guard Corps (IRGC).

According to the complaint, beginning in October 2021, Poursafi began attempting to arrange the murder of the former National Security Advisor, likely in retaliation for the January 2020 death of Iran's Islamic Revolutionary Guard Corps – Qods Force (IRGC-QF) commander Qasem Soleimani. Poursafi asked an individual in the United States to take photographs of the former National Security Advisor, claiming the photographs were for a book Poursafi was writing. That individual later introduced Poursafi to an individual, referred to in the complaint as the confidential human source (CHS). Poursafi sought to hire the CHS to arrange the murder of the former National Security Advisor.

Specifically, Poursafi offered the CHS $250,000 to hire someone to "eliminate" the former National Security Advisor. This amount would later be negotiated up to $300,000. Poursafi added that he had an additional "job," for which he would pay $1 million. Poursafi directed the CHS through the process of evaluating possible locations to conduct the murder, including the former National Security Advisor's workplace and home. As noted in the complaint, Poursafi provided the CHS with specific information regarding the former National Security Advisor's schedule that do not appear to have been publicly available.

CTS attorneys directed and managed numerous key functions in the investigation and the inter-agency coordination that resulted in the charges. For example, CTS managed the development of legal process such as search warrants in partnership with the USAO, and administrative processes such as authorization to engage in certain investigative steps, all of which enabled the investigation to proceed as it did. CTS partnered with the USAO to provide counsel to FBI agents in the field and at FBI headquarters to synchronize investigative efforts in a way that moved the investigation forward, met obligations to the victim(s), and anticipated or avoided potential litigation issues. CTS also engaged extensively with inter-agency partners, discovering, and assessing information potentially relevant to the case. In following its usual protocols, CTS ensured that in any future prosecution the Government would be able to meet its discovery obligations without endangering intelligence information, sources, or methods.

CTS Supports Successful Prosecution of Members of Oath Keepers Sentenced for Seditious Conspiracy and Other Offenses Related to United States Capitol Breach

Multiple CTS attorneys played integral roles in the prosecution of twelve defendants associated with the Oath Keepers, who were charged with seditious conspiracy (among other offenses) for their conduct in relation to the breach of the Capitol on January 6, 2021. Two CTS Trial Attorneys participated at the earliest stages of the investigation, assisting law enforcement with legal process, participating in proffers, negotiating with defense counsel on plea and cooperation agreements, and successfully securing guilty pleas to seditious conspiracy, among other offenses. CTS Trial Attorneys served on the trial team for the two multi-week trials of Oath Keeper defendants that featured charges of seditious conspiracy, as well as for the trial of other Oath Keeper defendants charged with related felonies and assisted at the sentencing phase, providing strategic advice on potential sentencing enhancements and drafting portions of the government's sentencing memoranda that argued successfully for the application of an upward departure for "terrorism" under U.S.S.G. § 3A1.4, Note 4.

On May 25, 2023, and May 26, 2023, in the District of Columbia, Elmer Stewart Rhodes III (Rhodes), Kelly Meggs (Meggs), Jessica Watkins (Watkins), and Kenneth Harrelson (Harrelson) were sentenced in connection with their convictions for seditious conspiracy and/or other charges involving the breach of the Capitol on January 6, 2021. On June 1, 2023, and June 2, 2023, in the District of Columbia, Roberto Minuta (Minuta), Ed Vallejo (Vallejo), David Moerschel (Moerschel), and Joseph Hackett (Hackett) were also sentenced in connection with their convictions for seditious conspiracy and other charges. The defendants were sentenced to the following terms:

Defendant	Sentencing Date	Imprisonment	Supervised Release	U.S.S.G. § 3A1.4, Note 4 Upward Departure
Rhodes	May 25, 2023	18 years	3 years	6 offense levels
Meggs	May 25, 2023	12 years	3 years	3 offense levels
Watkins	May 26, 2023	8.5 years	3 years	3 offense levels
Harrelson	May 26, 2023	4 years	2 years	1 offense level
Minuta	June 1, 2023	4.5 years	3 years	1 offense level
Vallejo	June 1, 2023	3 years	3 years (with first year on home confinement)	2 offense levels
Moerschel	June 2, 2023	3 years	3 years	1 offense level
Hackett	June 2, 2023	3.5 years	3 years	1 offense level

On November 29, 2022, Thomas Caldwell was found guilty of seditious conspiracy; he has not yet been sentenced.

On March 2, 2022, Joshua James pled guilty to seditious conspiracy and obstruction of an official proceeding. On April 29, 2022, Briam Ulrich pled guilty to seditious conspiracy and obstruction of an official proceeding.

On May 4, 2022, in the District of Columbia, William Todd Wilson pled guilty to seditious conspiracy and obstruction of an official proceeding. Wilson's guilty plea is part of a cooperation plea agreement.

CTS Integral to the Successful Prosecution of Two Members of The Front Sentenced for Conspiring to Attack Power Grids

On April 21, 2023, in the Southern District of Ohio, Christopher Brenner Cook (Cook) was sentenced to 92 months in prison followed by 30 years of supervised released, and Jonathan Allen Frost (Frost) was sentenced to 60 months in prison followed by 30 years of supervised release. The defendants, both of whom are founding members of The Front, were sentenced for conspiring to provide material support and resources in the form of training, weapons, explosives, and personnel, intending for the material support to be used in preparation for and in carrying out the destruction of an energy facility. The third founding member of the Front, Jackson Matthew Sawall (Sawall), will be sentenced at a later date. On February 23, 2022, Cook, Frost, and Sawall were arraigned on an Information, and each defendant pled guilty to the Information. The defendants each agreed that the terrorism sentencing enhancement applied at sentencing and agreed to recommend a term of 30 years of supervised release to begin after completing their terms of imprisonment.

CTS played a critical role in the investigation and prosecution of the defendants. The CTS trial attorney participated at the earliest stages of the investigation by assisting law enforcement with legal process, participating in proffers, negotiating with defense counsel on

plea and cooperation agreements, and successfully securing guilty pleas to providing material support to terrorists. The CTS trial attorney served on the trial team and presented the sentencing argument for one of the defendants. The CTS trial attorney also provided strategic advice on potential sentencing enhancements and drafted portions of the government's sentencing memoranda that argued successfully for the application of an upward departure for "terrorism" under U.S.S.G. § 3A1.4, Note 4.

In Fall 2019, Frost and Cook began planning an attack on the power grid, and, within weeks, they began recruiting others to join in their plan. Part of the recruiting process involved circulating a reading list that promoted white supremacy and Neo-Nazism. By late 2019, Sawall—a friend of Cook's—joined the conspiracy and assisted Cook with online recruitment efforts, operational security, and organization.

As part of the conspiracy, each defendant was assigned a substation in a different region of the United States. The plan was to attack the substations and power grids with powerful rifles. The defendants believed their plan would cost the government millions of dollars and cause unrest in the region. They planned for the attack to cause power outages and hoped the outages would be for many months, which might cause war and induce the next Great Depression. Frost provided Cook with an AR-47 and went to a shooting range to train for their attack on the power grid. Frost also provided Cook and Sawall with suicide necklaces. The necklaces were filled with fentanyl and were to be ingested if caught by law enforcement. Both Cook and Sawall expressed their commitment to dying in furtherance of the mission.

CTS Supports Successful Prosecution of Individual Who Joined ISIS with His Teenage Children

On March 28, 2023, in the Southern District of Florida, Emraan Ali (Ali) was sentenced to 20 years in prison, to be followed by lifetime supervised release, for conspiring to provide material support to ISIS. Ali entered a guilty plea on November 22, 2022.

Ali, a United States citizen, moved back to his birthplace, Trinidad, where he joined the Rio Claro Mosque (RCM), run by a Saudi imam. More than 250 Trinidadians were recruited into ISIS's ranks, mostly from RCM. Ali married the Saudi-born daughter of RCM's imam. Ali's close relationship to the Imam gave him tremendous influence over RCM's largely uneducated members. Between 2010 and 2015, Trinidad supplied more ISIS fighters per capita than any other nation, and Ali was instrumental in assisting this massive recruiting scheme. CTS completed extensive research into Ali's recruiting efforts in Trinidad. This involved meeting and interviewing an expert witness.

Shortly before leaving for Syria, Ali liquidated many of his assets and set up a means of transferring much of his wealth into Syria. Ali and his family crossed into Syria via Gaziantep, Turkey. Ali was a man of means, so CTS was heavily involved in the substantial review of his financials.

Once in ISIS-controlled territory, Ali attended ISIS' mandatory military training, bringing his then 15-year-old son, Jihad, with him. Soon thereafter, Ali arranged for his 15-year-old daughter to marry an older ISIS fighter, with whom Ali's daughter had a child less than 10 months later. Ali's 11-year-old son also was forced to fight for ISIS as ISIS began losing

territory. Much work was done by CTS to ensure FBI's victim witness team was involved related to the daughter's mental health and potential testimony given the trauma she sustained.

Claiming he was too ill to fight himself, Ali became a weapons trafficker, specializing in American-made scopes and firearms that he resold to ISIS fighters for profit. Ali also ran a general store, a money transfer business, a well-digging crew, and multiple construction companies. Ali's businesses supported ISIS' economy and assisted it in occupying and controlling territory it seized from Syrian civilians. The wells allowed ISIS members to occupy parts of Syria that had lost infrastructure in the war, and the construction business allowed ISIS members to restore damaged homes of Syrians so ISIS fighters and families could live in these and help ISIS hold towns under its control. CTS worked diligently to research ISIS' economics and was able to file motions explaining why Ali's position as a construction boss directly assisted ISIS in establishing a Caliphate. Over the years that followed, Ali's teenaged sons continued to serve in ISIS' military wing.

As the territory controlled by ISIS shrank, Ali had to move throughout Syria to avoid capture. In the last throes of battle, Ali called upon his fellow Trinidadian fighters not to surrender so that he would not go to jail. Ali continued to fight in Baghuz until he was fully surrounded by coalition forces and had no other choice than to surrender in March of 2019. In his statements to the FBI, Ali expressed no regret for his actions, and described his son, Jihad, as having lacked personal discipline. Ali claimed that what prevented the successful establishment of an ISIS "caliphate" was poor management by ISIS' bureaucracy.

In addition, CTS helped facilitate the discovery and later, admission at trial, of collected exploitable material (CEM), also referred to as "battlefield evidence." CTS also worked closely with Trinidad on numerous Mutual Legal Assistance Treaties (MLATs) to obtain all necessary evidence.

<u>CTS Supports Successful Prosecution of Michigan Man Who Fought with ISIS in Iraq and Syria, Assisting in Successful Interlocutory Appeal Allowing for Admissibility of "Battlefield Evidence"</u>

CTS attorneys played a significant role in the successful prosecution of Ibraheem Musaibli (Musaibli), a Michigan-born man who served in an ISIS armed fighting battalion while in Iraq and Syria in 2015-2018. Following the inception of the government's investigation with an anonymous tip received by the FBI, a CTS trial attorney provided input and advice in the early stages of the investigation, consulting with AUSAs at the Eastern District of Michigan (EDMI) as well as investigators and attorneys at the FBI to coordinate Musaibli's repatriation and to allow for a successful law enforcement interview while he was in transit. Musaibli's admissions during this interview were later admitted at trial, over Musaibli's objection.

In addition, CTS attorneys helped facilitate the discovery and later, admission at trial, of CEM obtained by Coalition Forces operating in Iraq and Syria as part of Operation Inherent Resolve (OIR) and collected by the Operation Gallant Phoenix intelligence sharing platform as well as the United Nations Investigative Team to Promote Accountability for Crimes Committed by Da'esh (UNITAD). This CEM provided crucial trial evidence linking Musaibli to ISIS during

his time in Syria and Iraq, and to ISIS's Tariq bin Ziyad foreign fighter battalion, in particular. CTS Trial Attorneys worked with AUSAs to move for the admission of this CEM prior to trial, while protecting classified and sensitive equities. Specifically, a CTS Trial Attorney coordinated with expert witnesses and a cooperating defendant facing terrorism charges in another district to develop a pre-trial evidentiary record that the CEM was reliable and related to Musaibli's role within ISIS. Although the trial court held that the ISIS documents at issue were authentic, it ruled *in limine* that they should be excluded based on its finding that no hearsay exceptions applied. CTS Trial Attorneys and CTS supervisors ultimately worked in tandem with EDMI to raise a successful appeal of this ruling in front of the United States Court of Appeals for the Sixth Circuit, where a panel issued a favorable, unanimous opinion that will serve as useful precedent for the admission of CEM in future cases.

A CTS trial attorney also provided significant assistance in the drafting and editing of other various case-related motions and motion responses prior to trial.

Finally, a CTS Trial attorney helped EDMI prepare the government's sentencing memorandum, with a focus on the application of the "terrorism" sentencing enhancement under U.S.S.G. § 3A1.4(a) & (b), which was contested by Musaibli. The court later applied the terrorism enhancement when calculating Musaibli's guidelines range at sentencing.

On, June 15, 2023, Musaibli was sentenced to fourteen years in prison and ten years of supervised release in connection to his conviction of providing and attempting to provide material support to ISIS and conspiring to provide material support to ISIS.

<u>CTS Supports Successful Filing of Forfeiture Action Against Over Nine Thousand Rifles and Over 700,000 Rounds of Ammunition Enroute from Iran to Yemen</u>

On July 6, 2023, the DOJ announced the filing of a forfeiture complaint against over 9,000 rifles, 284 machine guns, approximately 194 rocket launchers, over 70 anti-tank guided missiles and over 700,000 rounds of ammunition that the United States Navy seized in transit from Iran's Islamic Revolutionary Guard Corps (IRGC) to militant groups in Yemen.

According to court documents, the noted weapons came from four interdictions of stateless dhow vessels: two from 2021 and two from 2023. These interdictions led to the discovery and seizure of four large caches of conventional weapons, including long arms and anti-tank missiles, and related munitions – all of which were determined to be primarily of either Iranian, Chinese or Russian origin.

This action follows the Government's March 2023 forfeiture action against over one million rounds of ammunition enroute from Iran to Yemen. The network for both actions was involved in the illicit trafficking of advanced conventional weapons systems and components by sanctioned Iranian entities that directly support military action by the Houthi movement in Yemen and the Iranian regime's campaign of terrorist activities throughout the region. The forfeiture complaint alleges a sophisticated scheme by the IRGC to clandestinely ship weapons to entities that pose grave threats to United States national security. This forfeiture action is a product of the United States Government's coordinated effort to enforce United States sanctions against the IRGC and the Iranian regime.

In this case, CTS played three main roles. First, CTS coordinated with relevant components of the Department of Defense and other government agencies to make sure that the timing of the forfeiture action, any subsequent litigation, and public statements coincided with partners' operational needs. Second, CTS developed and reviewed legal process and public statements in a way that demonstrated the legal sufficiency and public safety/international security implications of the allegations, but coordinated extensively with inter-agency partners to ensure that doing so would not put at risk intelligence information, sources, or methods. Third, CTS drafted legal process in a way that accurately applied the underlying counterterrorism legal authorities and did not create undue litigation risk.

CTS Supports Successful Prosecution of ISIS Member Sentenced to Life in Prison

On July 14, 2023, in the Eastern District of New York, Mirsad Kandic (Kandic) was sentenced to life in prison. On May 24, 2022, Kandic was convicted, after a three-week jury trial, of one count of conspiring to provide material support and resources to a designated foreign terrorist organization resulting in death and five counts of attempting to provide and providing material support and resources to a designated foreign terrorist organization, including one count resulting in death. Kandic faces life imprisonment for the two counts of 18 U.S.C. § 2339B(a)(1) resulting in death, and 20 years imprisonment for the other four counts of 18 U.S.C. § 2339B(a)(1).

Between approximately May 2003 and November 2013, Kandic resided in the Bronx and Brooklyn, New York. After his attempts to leave the United States by air were thwarted, Kandic successfully flew from Mexico to Turkey in approximately December 2013. There he joined ISIS. Kandic worked to further ISIS's media operations, as well as to recruit foreign fighters and facilitate their travel into ISIS-claimed territory. He also participated in obtaining night vision equipment for ISIS and in fabricating and distributing false identification documents for persons wishing to travel in and out of ISIS-controlled territory.

Kandic later relocated to Sarajevo, where he continued to support ISIS. Kandic is believed to have been one of the principal ISIS facilitators for persons attempting to enter or exit ISIS-claimed territory. One such person was an Australian national named Jake Bilardi. Kandic facilitated Bilardi's travel into ISIS-claimed territory, encouraged Bilardi to follow through with his plan to commit a suicide bombing, and, after Bilardi successfully carried out such a bombing, publicized the attack via social media.

A CTS trial attorney was initially assigned to this case in late 2015. CTS trial attorneys reviewed and approved numerous draft search warrants submitted by the USAO and continued to do so well into 2017. In April 2016, CTS attorneys reviewed and recommended approval of a proposed complaint against Kandic, charging him with a violation of 18 U.S.C. 2339B, after Kandic was located overseas. The assigned CTS attorneys facilitated the transmission of prudential search requests to relevant agencies in 2016, 2017 and 2018 and conducted a lengthy review over several months of material produced in response to these search requests. CTS attorneys reviewed the prosecution memorandum and proposed indictment of Kandic, recommending approval in August 2018.

The assigned CTS trial attorney was actively involved in pretrial classified litigation pursuant to the Classified Information Procedures Act (CIPA) in a number of ways. The CTS

trial attorney reviewed and analyzed for NSD leadership whether particular evidence could be considered in the context of the independent source and inevitable discovery doctrines. The CTS trial attorney reviewed draft declarations of stakeholder affiants to be included in a CIPA Section 4 filing relating to the discovery of certain classified material. The CTS trial attorney prepared the highly classified package for consideration by The State Secrets Review Committee in mid-2018, recommending that the Attorney General assert the state secrets privilege as to certain material and approve the assertion of the state secrets privilege by several other stakeholders to protect classified information from disclosure, as required in Second Circuit cases. Thereafter, the CTS trial attorney reviewed and edited the draft CIPA Section 4 submission before it was filed with the court. In early 2019, the Court granted the relief requested by the government in the CIPA Section 4 submission.

Throughout the pretrial and trial timeframe, the assigned CTS attorney reviewed and approved recommendations seeking the renewal of Special Administrative Measures of Kandic in prison. In March 2022, when the Court issued a pretrial ruling suppressing certain evidence, the CTS attorney reviewed the ruling and joined in appellate counsel's recommendation against appeal.

CTS Integral to the Successful Prosecution of Texas Man Sentenced on Weapon of Mass Destruction Charge

On July 18, 2023, in the Northern District of Texas, Erfan Salmanzadeh (Salmanzadeh) was sentenced to 135 months in prison, followed by a lifetime of supervised release, following his guilty plea to one count of use and attempted use of a weapon of mass destruction and three counts of possession of an unregistered explosive device. Salmandzadeh has been in federal custody since July 30, 2021, when he was charged by complaint with the possession of unregistered explosive devices.

As alleged in the complaint filed shortly after the incident, on July 26, 2021, the Amarillo Police Department (APD) responded to Salmanzadeh's residence following reports of an explosion. Salmanzadeh retreated inside the house upon arrival of APD officers and poured triacetone triperoxide (TATP, a highly unstable explosive) down the toilet. Upon further investigation, APD officers and the FBI found three separate destructive devices in the residence, including a suicide vest with explosives and an improvised explosive device (IED) comprised of a cylinder wrapped in BBs, nails, and other shrapnel. Within the plea agreement, Salmanzadeh admitted to detonating an IED prior to APD's arrival. A review of Salmanzadeh's digital devices revealed multiple videos that displayed the explosive devices he created and his stated plans to use them to conduct a terrorist-type attack at Tascosa High School on or about July 27, 2021.

CTS played a significant role in the initial stages of the incident, charging decisions, and disposition. For example, CTS attorneys were assigned the evening of the explosions and worked with the AUSAs on drafting search warrants and charging documents. After review of the evidence, CTS identified a potential weakness related to the defendant's intended use of the destructive device and helped craft the indictment to avoid this weakness. As a result, the defendant's proffered mental defect defense was not applicable to the charges based on the language proposed by CTS. His mental defense vitiated; the defendant pled guilty.

CTS Supports Successful Prosecution of Proud Boys Sentenced for Seditious Conspiracy Related to United States Capitol Breach

On September 5, 2023, Enrique Tarrio (Tarrio) was sentenced to 22 years of imprisonment, followed by 36 months of supervised release. On September 1, 2023, co-defendant Ethan Nordean (Nordean) was sentenced to 18 years of imprisonment, followed by 36 months of supervised release and Dominic Pezzola (Pezzola) was sentenced to 10 years of imprisonment, followed by 36 months of supervised release. On August 31, 2023, co-defendant Joseph Biggs (Biggs) was sentenced to 17 years of imprisonment and 3 years of supervised release and Zachary Rehl (Rehl) was sentenced to 15 years of imprisonment and 3 years of supervised release.

On May 4, 2023, the jury returned a verdict of guilty on numerous counts against these defendants, members of the Proud Boys who are charged for their conduct related to the breach of the United States Capitol on January 6, 2021. Since the inception of the investigation beginning on January 6, 2021, CTS was partnered with the D.C. USAO to identify and prosecute the offenders. CTS prosecutors sat side by side with members of law enforcement and the USAO to pour through countless hours of videos, photographs, search warrant returns, chat logs, and other evidence in the days and months after the attack, to scrutinize actions and relationships between members of this conspiracy and others. This partnership was instrumental in bringing Tarrio and the other Proud Boys involved on January 6, to justice.

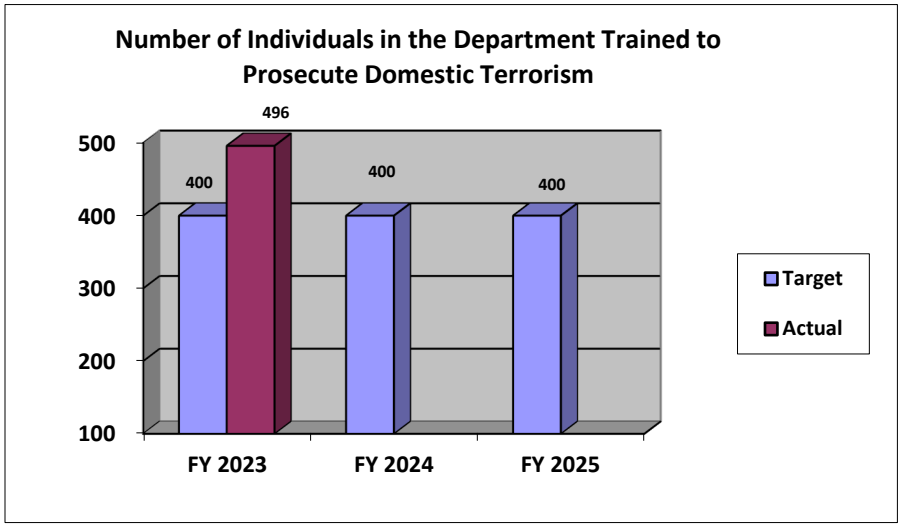
Defendants Nordean, Tarrio, Biggs, and Rehl were found guilty of seditious conspiracy, The charge of seditious conspiracy was significant in this case and in another January 6 conspiracy case involving the Oath Keepers. Due to the rarity of this charge, its heavy penalty, and likelihood of public scrutiny – the decision to charge involved heavy contemplation and review by both the D.C. USAO and CTS. This review occupied many weeks of discussion at all levels of prosecutors and supervisors, and ultimately concluded with the approval to charge seditious conspiracy in both the Oath Keepers and Proud Boys conspiracy cases, detailed here.

As early as November 4, 2020, Nordean, Tarrio, Biggs, Rehl and other leaders of the Proud Boys began to voice their opinion that the results of the election were corrupt. On December 19, 2020, plans were announced for a "Stop the Steal" protest event in Washington, D.C. to occur on January 6, 2021, coinciding with Congress's certification of the Electoral College vote. The next day Tarrio created a Telegram group called "Ministry of Self Defense" (MOSD). As alleged in the indictment, from in or around December 2020, Tarrio and his co-defendants, all of whom were leaders or members of the MOSD, conspired to prevent, hinder, and delay the certification of the Electoral College vote, and to oppose by force the authority of the government of the United States. Almost immediately after Tarrio initiated the MOSD leadership messaging group, Biggs told the group that he had booked his ticket to Washington, D.C. for January 5-7. Tarrio also created an MOSD recruitment chat to identify potential MOSD participants. The messages from Tarrio and other MOSD leadership emphasized the top-down control of the chapter. The MOSD chat log was key to understanding the Proud Boys conspiracy. A significant amount of legal process was required to obtain the social media accounts, phone records and devices needed to construct the pieces of the chat. CTS was instrumental in drafting, reviewing, and obtaining those search warrants. CTS prosecutors also substantially aided in reviewing, categorizing, and linking relationships inside the chat log and other digital evidence, to identify the culpable parties and understand the details of the

conspiracy. When it came time to charge the Proud Boys conspiracy, CTS was partnered with the USAO in those decisions to ensure the senior leaders of the group were held accountable.

Measure:	**Number of individuals in the Department trained to prosecute domestic terrorism and domestic violent extremism**
FY 2023 Target:	**400**
FY 2023 Actual:	**496**
FY 2024 Target:	**400**
FY 2025 Target:	**400**

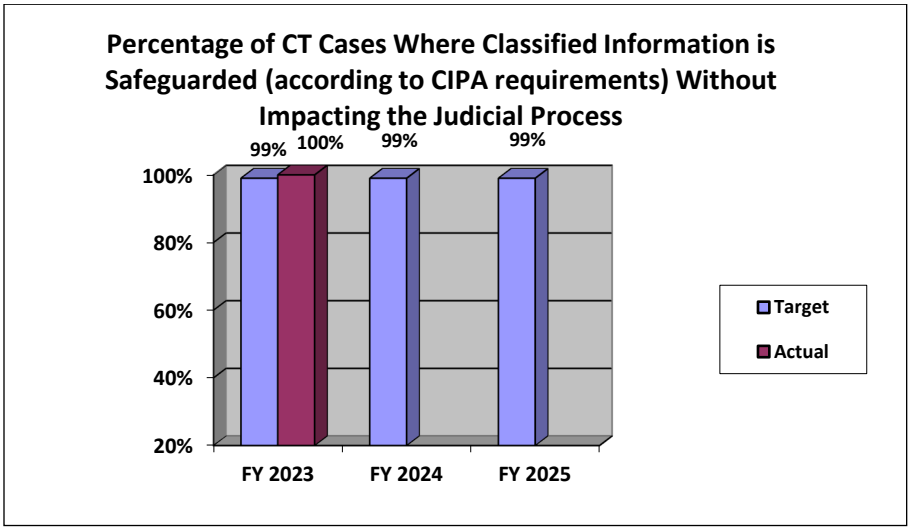
Discussion: The FY 2025 target is consistent with previous fiscal years.



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 2025 will continue to depend on the ability to conduct in-person trainings although currently there are no COVID restrictions, and in-person training is planned. For the few national security sessions that can be conducted in an unclassified environment, NSD will continue to conduct some webinars to reach a larger audience of prosecutors and agents. NSD has set FY 2025 targets assuming that most trainings will be conducted in person. In FY 2025, there are four courses tentatively scheduled that include topics regarding Domestic Terrorism. If all those courses can be conducted in-person without facility limitations, it is anticipated that more than 400 individuals will be trained.

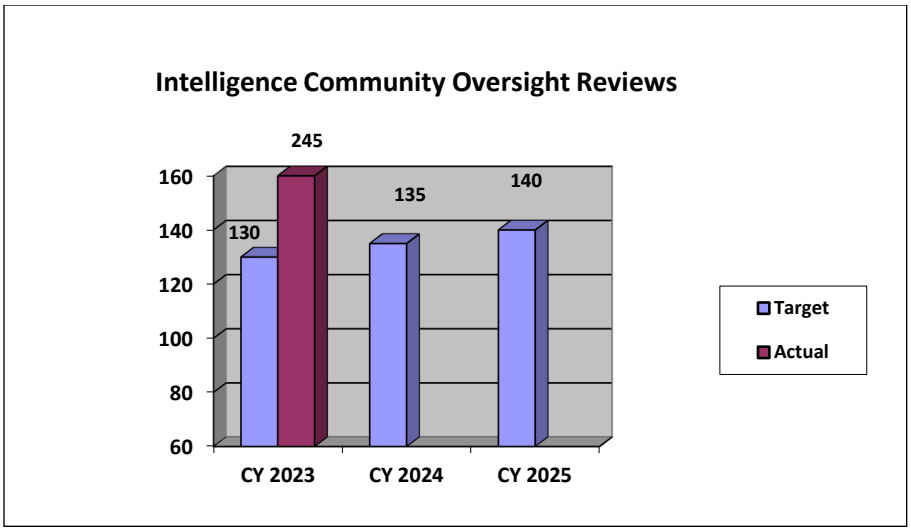
Measure:	**Percentage of CT Cases Where Classified Information is Safeguarded (according to CIPA requirements) Without Impacting the Judicial Process**
FY 2023 Target:	**99%**
FY 2023 Actual:	**100%**
FY 2024 Target:	**99%**
FY 2025 Target:	**99%**

Discussion: The FY 2025 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.

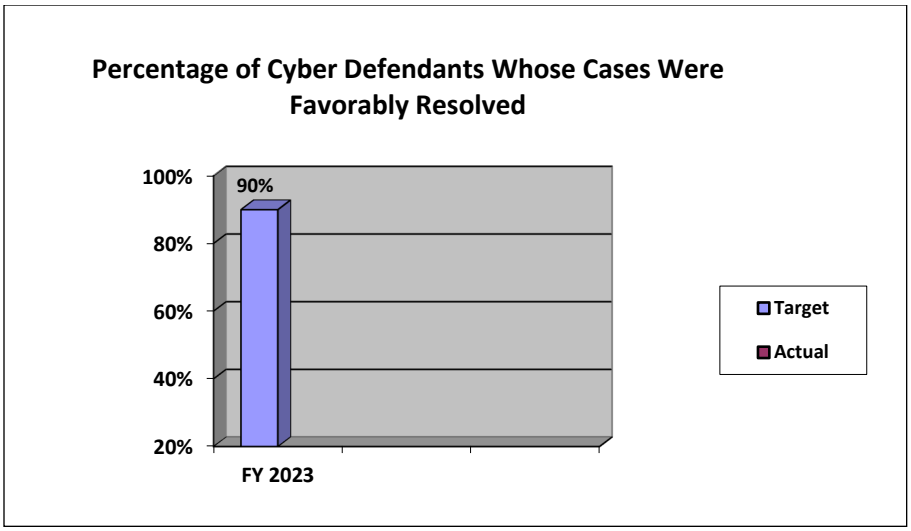
Measure: **Intelligence Community Oversight Reviews**
CY 2023 Target: **130**
CY 2023 Actual: **245**
CY 2024 Target: **135**
CY 2025 Target: **140**
Discussion: The CY 2025 target is slightly increased but consistent with prior fiscal years. The overall work of NSD assessing and ensuring compliance 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 2023 Target: 90%
FY 2023 Actual: N/A - No cyber defendants' cases were closed in FY 2023
FY 2024 Target: N/A
FY 2025 Target: N/A
Discussion: This performance measure has been discontinued starting in FY 2024 and replaced with an internal measure.



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 NatSec Cyber management.
Data Limitations: There are no identified data limitations at this time.

Highlights from Recent National Security Cyber Cases

NSD Leads Disruption of GRU's "Cyclops Blink" Malware Network: In April 2022, the Department announced the completion of a court-authorized operation to disrupt a two-tiered global botnet of thousands of infected network hardware devices under the control of a threat-actor known to security researchers as Sandworm, which the United States Government has attributed to the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (the GRU). The operation copied and removed malware (dubbed "Cyclops Blink" by security researchers) from vulnerable internet-connected firewall devices that Sandworm used for command and control (C2) of the underlying botnet. Although the operation did not involve access to the Sandworm malware on the thousands of underlying victim devices worldwide, referred to as "bots," the disabling of the C2 mechanism severed those bots from the Sandworm C2 devices' control. The FBI provided notice to owners of infected devices in the United States and – through foreign law enforcement partners – abroad. This removal of malware deployed by the GRU demonstrated the Department's commitment to disrupt nation-state hacking, using all legal tools available.

CES trial attorneys led this technical operation from its inception. The initial concept for the operation (CONOP) was proposed by FBI agents working with CES and the USAO for the Western District of Pennsylvania on the Department's enterprise investigation into Sandworm (a/k/a GRU Unit 74455). From that initial stage, CES took the lead role in: (i) further refining the CONOP; (ii) coordinating with legal counsel for Watchguard, the United States-based

manufacturer of the firewall devices; (iii) arranging, through counsel, for Watchguard's assistance in evaluating the feasibility of, and later testing the code used in, the operation; (iv) developing the legal theory that the Department would use to obtain the necessary judicial authorizations; (vi) ensuring that the operation complied with relevant Department policies; (v) coordinating with the Department's Office of International Affairs and foreign partners; (vi) drafting the search warrant application; and (vii) preparing the USAO partners to brief the assigned judge. The USAO then presented the search warrant application to the judge, who quickly provided the requested authorization. NatSec Cyber continues to be the Department's lead for the ongoing investigation into Sandworm's malicious cyber activities, setting investigative strategies and drafting the vast majority of related legal process.5

NSD Leads Effort to Seize DPRK Ransomware Proceeds: In July 2022, in the District of Kansas, the Department filed a complaint to civilly forfeit two cryptocurrency accounts containing victims' money from DPRK ransom attacks. In May 2021, DPRK hackers used a ransomware strain called "Maui" to encrypt the files and servers of a hospital in Kansas. After more than a week of being unable to access encrypted servers, the Kansas hospital paid approximately $100,000 in Bitcoin to regain the use of their computers and equipment. Because the Kansas hospital notified the FBI and cooperated with law enforcement, the FBI was able to identify the never-before-seen DPRK ransomware and trace the cryptocurrency to China-based money launderers. As a result, in April 2022, the FBI observed an approximately $120,000 Bitcoin payment into one of the seized cryptocurrency accounts identified due to the cooperation of the Kansas hospital. The FBI's investigation confirmed that a medical provider in Colorado had just paid a ransom after being hacked by actors using the same Maui ransomware strain. In May 2022, the FBI seized the contents of two cryptocurrency accounts that had received funds from the Kansas and Colorado healthcare providers. The District of Kansas then began civil proceedings to forfeit the hackers' funds and return the stolen money to the victims. In July 2023, the Department publicly announced the DPRK's hospital ransomware scheme, alongside a Cybersecurity and Infrastructure Security Agency (CISA) Cyber Security Announcement and the unsealed civil forfeiture complaint in order to publicize the threat, the United States Government's response, and to encourage other victims to come forward.

CES trial attorneys led this investigation from its inception. After the FBI identified that the ransomware note came from DPRK state-sponsored hackers, CES contacted the USAO of the District of Kansas. Throughout 2022 and 2023, CES trial attorneys drafted, and the USAO presented, numerous applications for search warrants and other legal authorities that allowed the FBI to identify multiple other Maui ransomware victims and to trace the trail of Bitcoin paid by these victims. It was the early portion of these efforts that saw CES draft a seizure affidavit for $500,000 from the cryptocurrency accounts of two Hong Kong-based money launderers who received funds from healthcare provider ransomware victims. NSD then worked with the FBI and CISA to in July 2023 to publicly attribute the DPRK's hospital ransomware scheme, issue a related joint cybersecurity advisory, and encourage additional victims to come forward. CES's efforts, however, did not end there. Trial attorneys continued to draft legal process related to this activity, which resulted in the identification of a cyberespionage (versus ransomware) scheme by the same actors, which became the subject of a second CISA Cyber Security Announcement in

5 When NatSec Cyber was created in August 2023, eight trial attorneys and the portfolio of national security-related cyber investigations from CES to the new section. All pre-August 2023 events listed herein were handled by current NatSec Cyber prosecutors and the underlying investigations are now being handled by NatSec Cyber.

2023. NatSec Cyber continues to lead this investigation and planning for future disruption operations.

NSD Provides Substantial Support to Disruption of FSB's "Snake" Malware: In May 2023, in the Eastern District of New York, the Department announced the completion of a court-authorized operation, code-named Medusa, to disrupt a global peer-to-peer network of computers compromised by sophisticated malware, called "Snake," which the United States Government attributes to a unit within Center 16 of the FSB of the Russian Federation. For nearly 20 years, this unit, referred to in court documents as "Turla," used versions of the Snake malware to steal sensitive documents from hundreds of computer systems. Victims came from at least 50 countries, including North Atlantic Treaty Organization (NATO) member governments, journalists, and other targets of interest to the Russian Federation. After stealing these documents, Turla exfiltrated them through a covert network of unwitting Snake-compromised computers in the United States and around the world. Operation Medusa disabled Turla's Snake malware on compromised computers through the use of an FBI-created tool named PERSEUS, which issued commands that caused the Snake malware to overwrite its own vital components. Within the United States, the operation was executed by the FBI pursuant to a federal search warrant that authorized remote access to the compromised computers. For victims outside the United States, the FBI engaged with foreign authorities to provide both notice of Snake infections within those authorities' countries and remediation guidance. Additionally, the FBI, NSA Cyber Command, CISA, and agencies from all "Five Eyes" partners issued a cybersecurity advisory with detailed technical information about the Snake malware that will allow cybersecurity professionals to detect and remediate Snake malware infections on their networks.

The USAO for the Eastern District of New York and the FBI's New York field office developed the CONOP for this operation during the early months of 2023. Approximately two weeks prior to the proposed execution date, as required by Department policy, they sought CES's input and expertise regarding the CONOP and the underlying legal authorities. CES trial attorneys quickly reviewed the CONOP and related proposed legal filings. The technical aspects of the CONOP were sound (e.g., there was a legal capability to send the desired commands to disrupt the malware, the commands did not interfere with the legitimate operation of victim devices, and the FBI conducted adequate testing). However, the proposed search warrant application required substantial revisions, including to comport with the Department's legal theories, policies, and best practices that had been developed for such operations. The following week, CES trial attorneys took the lead on: (i) refining the legal theory that the Department would use to obtain the necessary judicial authorizations; (ii) ensuring that the operation complied with relevant Department policies; (iii) coordinating with the Department's Office of International Affairs and foreign partners; (iv) substantially revising the search warrant application; and (v) preparing the USAO to brief the assigned judge. The USAO then presented the search warrant application to the judge by the CONOP's original deadline. The judge immediately provided the necessary authorization. NatSec Cyber continues to provide program management for several investigations into Center 16's malicious cyber activities and is setting investigative strategies and drafting the vast majority of related legal process for several of those investigations.

NatSec Cyber leads Disruption of Illicit Revenue Generation Efforts of DPRK Information Technology (IT) Workers: In October 2023, in the Eastern District of Missouri, the Department announced a three-pronged effort to disrupt the DPRK government's illicit revenue generation efforts that rely on thousands of skilled DPRK IT workers living abroad, primarily in China and

Russia, who obtained work for unwitting United States and foreign companies. The DPRK uses the illicit funds generated by these IT workers to advance the DPRK's weapons of mass destruction and missile programs and, in some instances, to further computer intrusion activities. First, the Department conducted a court-authorized seizure of 17 website domains that the IT workers used to mimic United States-based IT services companies, thereby helping the IT workers hide their true identities and location when doing remote work for the United States and other businesses worldwide. Second, the Department conducted court-authorized seizures totaling $1.5 million of the revenue that the IT workers received from unwitting victim companies for their IT work. Third, the Department, other United States government partners, and the Republic of Korea (ROK) government shared IT worker-related threat intelligence with nine United States-based online freelance work and payment service platforms used by the IT workers to pose as non-DPRK IT workers, which resulted in the services' improvement of their fraud detection mechanisms and their termination of thousands of fraudulent IT worker accounts. The announcement of the Department's long-running disruption operations coincided with both the United States and ROK governments' release of a public service advisory, containing threat intelligence gleaned from the Department's investigation, regarding the sanctions evasion and cybersecurity threat posed by such IT workers, which contained indicators that would-be employers of DPRK IT workers can use to protect themselves from the scheme. This advisory updated an earlier advisory that the United States Government released in May 2022.

NatSec Cyber trial attorneys conceived of and led all three aspects of this disruption. First, upon being briefed by the FBI regarding the then recent identification of the DPRK IT worker websites, NatSec Cyber saw an opportunity to eliminate the bona fides of the fake IT services companies by drafting an application for a court-authorized seizure warrant to take control over the domains and redirect them to an FBI "splash page" website that would provide the public with further information about the DPRK IT worker threat and tactics. The USAO for the Eastern District of Missouri then submitted that application to a judge, who ultimately approved it.

Second, NSD-drafted search warrants for IT worker communication accounts revealed the identity of United States-based payment services companies used by the DPRK, including their account identifiers. NSD contacted the fraud detection teams of two major online payment providers, who in 2022 and 2023 froze millions of dollars of DPRK IT worker funds. NatSec Cyber drafted, and the USAO for the Eastern District of Missouri submitted, multiple seizure applications that resulted in the seizure of approximately $2 million of this money.

The third and final aspect of this disruption, the sharing of threat intelligence with United States-based online freelance work and payment service platforms began in 2022 was a result of NSD's focus on: (i) ensuring that information gained from NSD's cyber investigations is quicky shared with the private sector (in this case, platform compliance personal and network defenders who could identify and root out abuse of their platforms); and (ii) building domestic and international coalitions to disrupt malicious cyber threats. NatSec Cyber trial attorneys worked with DOS's Bureau of Intelligence and Research (State INR) to develop the additional contacts with ROK government officials who were also seeking to disrupt the DPRK IT worker threat. That, in turn, led to NatSec Cyber, State INR, and the ROK to pool their threat intelligence into a dataset of information that the private sector could utilize to identify fraudulent DPRK IT worker accounts on their platforms and improve their threat detection algorithms to prevent the future creation of similar fraudulent accounts. NatSec Cyber was responsible for reaching out to all the private

sector companies to establish the initial contacts, liaise with their compliance personnel and counsel, and to ultimately pass the threat intelligence that enabled the companies' success in substantially limiting the IT workers' access to their platforms. As a result of these efforts, these companies now know and care about the threat, have hired specific fraud detection personnel to search for it, and are now independently and constantly searching for and closing thousands of DPRK accounts, and then mutually sharing the data with other private-sector companies. This new private-sector coalition has resulted in two conferences focused on this information, one in 2023 organized by the DOS, and the second in 2024 organized by the private sector themselves. NatSec Cyber continues to lead this investigation and planning for future disruption operations.

NatSec Cyber Leads Disruption of Russian Intelligence Service's Cyber-Enabled Malign Influence Operation: In December 2023, DOJ obtained an indictment of two Russian nationals, an officer "Center 18" of the FSB and an associated cybercriminal, with a campaign to hack into computer networks in the United States, the United Kingdom, other North Atlantic Treaty Organization members countries, and Ukraine, in some instances in furtherance of foreign malign influence efforts designed to undermine democratic processes. The indictment alleges the conspiracy targeted current and former employees of the IC, DOD, DOS, defense contractors, and Department of Energy facilities between at least October 2016 and October 2022. In addition, the indictment alleges the conspirators – known publicly by the name "Callisto Group" – targeted military and government officials, think tank researchers and staff, and journalists in the United Kingdom and elsewhere, and that information from certain of these targeted accounts was leaked to the press in Russia and the United Kingdom in advance of United Kingdom elections in 2019. Separately, OFAC and the United Kingdom government each announced sanctions against the two charged individuals and the DOS announced rewards of up to $10 million for information leading to the identification or location of the individuals and their conspirators.

NatSec Cyber trial attorneys participated in the enterprise investigation of this particular unit of Center 18 since its inception several years earlier, serving as co-counsel with the USAO for the Northern District of California. Their work primarily consisted of drafting legal process and coordinating with United Kingdom authorities who were also investigating the same activity. However, once the investigation identified the two charged individuals, NatSec Cyber was responsible for coordinating with the FBI, the TREAS, the DOS, and United Kingdom authorities to develop a coordinated disruption and messaging plan that focused on Russian Intelligence's hack-and-leak operation targeting the 2019 election. NatSec Cyber continues to co-counsel with the USAO for the Northern District of California in the ongoing investigation into Center 18 malicious cyber activities, setting investigative strategies and drafting the related legal process.

NatSec Cyber Leads Online Operation to Disrupt Botnet Used by Chinese Intelligence Services to Target United States and Allied Critical Infrastructure: On January 31, 2024, the Department announced a court-authorized online operation, commenced in December 2023, that disrupted a botnet that state-sponsored actors working for the People's Republic of China (PRC) had been using to conceal the hacking of United States and allied critical infrastructure. The PRC actors, known to the private sector as "Volt Typhoon," used hundreds of "end of life" Cisco and NetGear small office/home office (SOHO) routers and formed them into the botnet, known as the "KV botnet." They used the botnet to obfuscate their hacking of, and to maintain surreptitious access to, the critical infrastructure networks. United States government has assessed that this activity was part of the PRC's efforts to pre-position itself on such networks

and then lie low until a future crisis or conflict requires destructive or disruptive attacks. To carry out the operation, the Department obtained multiple court authorizations to delete and cut off certain of the actors' malware and other tools, as well as taking non-persistent/reversible steps to prevent the actors from reinfecting the devices. Additionally, the FBI, CISA, and the NSA issued several cybersecurity advisories with detailed technical information about the PRC hackers' tactics and techniques, which will allow cybersecurity professionals to detect and prevent similar intrusions into their networks.

NatSec Cyber trial attorneys led this technical operation from its inception. After receiving relevant intelligence about the threat posed by this botnet, NatSec Cyber proposed to the FBI that the botnet be targeted through a technical operation. From that initial proposal, NatSec Cyber took the lead role in: (i) creating a CONOP; (ii) developing the legal theory that the Department would use to obtain the necessary judicial authorizations; (iii) ensuring that the operation complied with relevant Department policies; (iv) coordinating with the Department's Office of International Affairs and foreign partners; (v) drafting the warrant applications; and (vi) preparing the USAO for the Southern District of Texas to brief the assigned judges. In the case of one warrant application, the judge asked for more legal support for the proposed authorization and NatSec Cyber promptly researched the relevant issues and provided responsive information to the judge, who ultimately provided the necessary authorization. In the case of other applications, NatSec Cyber directly briefed the judges on important context for the proposed authorization. NatSec Cyber continues to be the Department's lead for the ongoing investigation into Volt Typhoon's malicious cyber activities, setting investigative strategies and drafting the key legal process.

NatSec Cyber Leads Online Operation to Disrupt Botnet Used By Russian Military Intelligence as a Global Intelligence Collection Platform, Including Against Targets in Ukraine: On February 19, 2024, the Department announced an online operation to disrupt a botnet operated by Unit 26165 of Russia's military intelligence agency, the GRU (a/k/a "APT 28" and "Fancy Bear"). The GRU created this botnet of thousands of compromised Ubiquiti SOHO routers by co-opting criminal hackers' earlier compromise of SOHO routers with "Moobot" malware. The GRU turned that criminal botnet into its own global intelligence collection platform, primarily in support of spearphishing and similar credential harvesting campaigns, including operations targeting Ukraine. As with prior operations, the Department obtained a court's authorization to delete and cut off certain of the actors' malware and other tools, as well as taking non-persistent or otherwise easily reversible steps to prevent the actors from reinfecting the devices (e.g., modifying victim router firewall rules). This takedown was the third time since Russia's unjustified invasion of Ukraine that the Department has stripped the Russian intelligence services of a key tool used to further Russia's acts of aggression and other malicious activities.

NatSec Cyber trial attorneys led this technical operation from its inception, when FBI first proposed a disruption CONOP. Specifically, NatSec Cyber took the lead role in: (i) refining the FBI's original CONOP; (ii) coordinating with legal counsel for Ubiquiti; (iii) developing the legal theory that the Department would use to obtain the necessary judicial authorizations; (iv) ensuring that the operation complied with relevant Department policies; (v) coordinating with the Department's Office of International Affairs and foreign partners; (vi) drafting the search warrant application; and (vii) preparing the USAO for the Eastern District of Pennsylvania to brief the assigned judge. The USAO then presented the search warrant application to the judge, who immediately provided the proposed authorization. NatSec Cyber continues to be the

Department's lead for the ongoing investigation into Unit 26165's malicious cyber activities, setting investigative strategies and drafting the vast majority of related legal process.

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.

Cyber Threats to National Security

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, prosecution, and disruption of national security-related cyber threats 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 added a domestic terrorism unit within the CTS using base resources.

C. Priority Goals

The Department's FYs 2024 – 2025 Agency Priority Goals (APGs) are being finalized. If the Department continues with an APG related to combating ransomware attacks, NSD will assist with DOJ's efforts to achieve the FYs 2024 – 2025 goal. 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. Countering National Security Cyber Threat

Budget Decision Unit(s): National Security Division

Organizational Program: National Security Cyber Section

Program Increase: Positions: 22 Atty: 20 FTE: 11 Dollars: $5,000,000

Description of Items

The National Security Cyber Section (NatSec Cyber) requests 22 positions, including 20 attorneys, one intelligence analyst, and one administrative officer.

Justification

As detailed in the Performance Challenges section, cyber threats with national security implications are evolving and growing at an intensifying rate. In order to meet this threat, as well as the strategic objectives set out in the President's National Cybersecurity Strategy and associated Implementation Plan, NSD has changed its organizational structure to add the National Security Cyber Section (NatSec Cyber).

NatSec Cyber will address national security cyber threats across the spectrum, including disruptive activities targeting United States critical infrastructure, ransomware, and cyber-enabled foreign malign influence, sanctions evasion, illicit revenue generation, economic espionage, and intelligence gathering. However, NSD's ability to respond to significant incidents and develop disruption options and threat intelligence depends on attorney and staff resources. Creating a stand-alone section focused on cyber-threat matters allows the Division to expand cyber subject matter experts within its workforce and enhance the recruitment of the high-quality attorneys and staff who perform this complex and technical work by demonstrating the Division's focus on this emerging area of law, policy, and operations. In order to adequately staff this new section, NSD is seeking 20 full-time attorney positions, as well as one staff position and one analyst.

NSD has already been an integral part of a larger transformation in the Federal Government's response to significant cyber incidents by using traditional law enforcement tools to investigate and disrupt state-sponsored actors, arresting and prosecuting them where possible. Because arrest is often unlikely in the near term, NSD works to disrupt state-sponsored malicious cyber activity by using legal tools such as seizure of infrastructure and funds, as well as targeted sharing with private sector and United States Government and foreign partners of threat intelligence gathered through NSD's criminal investigations. This threat intelligence provided the basis for NSD court-authorized disruption operations such as botnet takedowns, and enabled other government agencies to deploy their respective tools and authorities through technical operations, intelligence operations, sanctions, trade remedies, and diplomatic efforts. Sharing threat intelligence developed through national security investigations also empowers private sector network defenders, encourages victim reporting and cooperation, and serves to educate the American

public about cyber threats, thereby enhancing the nation's collective cybersecurity. NSD plays a critical role in driving a whole-of-government response and supporting private sector partnerships. Such efforts demand considerable resources but are essential to an effective response.

By creating NatSec Cyber, NSD and the Department have shown their commitment to precisely such a robust response. Funding for a full complement of dedicated attorneys and staff for the new Section is necessary to address the 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 similar disruptive actions. Given other pressing criminal justice priorities, USAOs can lack resources to devote to these investigations, especially when their offices are facing pressure to tackle other pressing crime issues in their districts. 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, prioritized proactive disruptive actions, and placed other significant resource demands on NSD. This is because disruption efforts invariably require threat intelligence obtained as part of the Department's criminal investigations, especially when such efforts occur on cyber infrastructure in the United States and therefore often require a court's authorization based on unclassified information. To better address the increasing caseload of significant cyber matters, NatSec Cyber attorneys will work almost exclusively on cyber investigations, prosecutions, and other disruption operations. Responsibilities will include:

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

• working with foreign partners to develop global operational capacity to obtain evidence/threat intelligence and collectively disrupt the most sophisticated national security threats.

NatSec Cyber is also core to the Department's ability to implement other Strategic Objectives of the National Cybersecurity Strategy: 2.1 (Integrate Federal Disruption Activities), 2.2 (Enhance Public-Private Operational Collaboration to Disrupt Adversaries), 2.3 (Increase the Speed and Scale of Intelligence Sharing and Victim Notification), 2.5 (Counter Cybercrime, Defeat Ransomware), 5.1 (Build coalitions to Counter Threats to Our Digital Ecosystem), 5.2 (Strengthen International Partner Capacity), and 5.4 (Build Coalitions to Reinforce Global Norms of Responsible State Behavior).

Impact on Performance

The above request will allow NSD to appropriately staff NatSec Cyber so that it is positioned to better address the increasing caseload of significant cyber matters affecting national security and cybersecurity. These resources directly relate to DOJ Strategic Objective 2.1, (Protect National Security), as well as the National Cybersecurity Strategy's Strategic Objective 2.1 (Integrate Federal Disruption Activities), 2.2 (Enhance Public-Private Operational Collaboration to Disrupt Adversaries), 2.3 (Increase the Speed and Scale of Intelligence Sharing and Victim Notification), 2.5 (Counter Cybercrime, Defeat Ransomware), 5.1 (Build coalitions to Counter Threats to Our Digital Ecosystem), 5.2 (Strengthen International Partner Capacity), and Build Coalitions to Reinforce Global Norms of Responsible State Behavior.

Funding

1. Base Funding

FY 2023 Enacted				FY 2024 Continuing Resolution[6]				FY 2025 Current Services			
Pos	Atty	FTE	Amount ($000)	Pos	Atty	FTE	Amount ($000)	Pos	Atty	FTE	Amount ($000)
6	6	6	$1,846	10	10	10	$3,076	11	10	11	$3,325

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2025 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Intelligence (0132) – Analyst	$148	1	$241	$59	($54)	$59	($54)
Clerical and Office Svcs (0300-0399) – Administrative Officer	$135	1	$215	$67	($54)	$67	($54)
Attorneys (0905)	$4,717	20	$356	$48	$4	$9600	$80
Total Personnel	**$5,000**	**22**	**$812**	**$174**	**($104)**	**$1,086**	**($28)**

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)

6 FY 2024 Annualized Continuing Resolution reflects an internal realignment of resources, designed to help stand up NatSec Cyber and does not include program changes. Internal realignments of resources may not reflect permanent changes and are completed as needed based on leadership priorities.

	Count	Atty	FTE	Personnel	Non-Personnel	Total	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Current Services	11	10	11	$3,325	$0	$3,325	$0	$0
Increases	22	20	11	$5,000	$0	$5,000	$1,086	($28)
Grand Total	**33**	**30**	**22**	**$8,325**	**$0**	**$8,325**	**$1,086**	**($28)**

6. Affected Crosscuts

National Security, Counterterrorism, Cybersecurity, Intelligence and Information Sharing

VIII. Exhibits