FY 2027
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) 2027 a total of 325 positions (including 231 attorneys), 356 full-time equivalents (FTE), and $123,000,000.

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

- Pursuing the criminal investigation and prosecution (1) of those responsible for the Hamas attack on and kidnapping of over 50 U.S. citizens on October 7, 2023, and (2) of those responsible for any U.S.-based financing of Hamas as it relates to this attack, including through the new Joint Task Force October 7 established by the Attorney General;
- Helping to apply maximum pressure on the Islamic Republic of Iran and its terror proxies, as called for by National Security Presidential Memorandum 2. This includes (1) investigating, prosecuting, and otherwise disrupting financial and logistical networks, operatives, and front groups; (2) targeting related foreign-based hacking operations; (3) targeting the leaders and members of terrorist groups and terror proxies responsible for capturing, harming, or killing American citizens, and (4) seizing illicit Iranian oil exports;
- Combatting international drug trafficking by foreign terrorist cartels and other international criminal organizations, which is critical to helping secure the U.S. border and protecting the American people from the import of illicit drugs;
- Conducting oversight of the Intelligence Community's (IC) foreign intelligence collection activities, including compliance with the bipartisan Reforming Intelligence and Securing America Act of 2024;
- Continuing to remediate the infiltration of U.S. telecommunications networks and preventing further intrusions by the Chinese Government, other nation-states, and their proxies, including by chairing Team Telecom;
- Deploying all tools at NSD's disposal to conduct disruptions of and other operations against state-sponsored cyber hackers, particularly to protect U.S. critical infrastructure and sensitive data;
- Enforcing sanctions and export controls to disrupt the unlawful transfer of world-class American technology and defense products to unauthorized or sanctioned end-users;

- Combating foreign governments' exploitation of the U.S. open-market, including through the Department's review of foreign investments, including real-estate purchases, as a member of the Committee on Foreign Investment in the United States;
- Implementing the President's America First Trade Policy by leading the government's effort to secure technology supply chains to protect national security; and
- Pursuing the prosecutions of individuals charged in connection with attempted political assassinations, terrorist attacks on U.S. military members, and other crimes of significance related to national security.

2. Division Structure

NSD combines counterterrorism, counterintelligence, export control, and cyber prosecutors with attorneys who oversee DOJ's foreign intelligence/counterintelligence operations, as well as attorneys who provide policy and legal advice on a wide range of national security issues. This organizational structure strengthens the effectiveness of DOJ's national security efforts by ensuring greater coordination and unity of purpose between prosecutors, law enforcement agencies, intelligence attorneys, and the Intelligence Community (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); and
- Office of Law and Policy (L&P)

C. NSD Major Responsibilities

1. Counterintelligence and Export Control

- Supervising the investigation and prosecution of cases affecting national security, foreign relations, violations of sanctions, and the export of military and strategic commodities and technology, some of the department's most complex, high profile, and sensitive cases.

- Authorizing the prosecution of cases under criminal statutes relating to espionage, sabotage, neutrality, and atomic energy; coordinating, developing, and supervising investigations and prosecutions involving the unauthorized disclosure of classified information.

- Developing and leading counter-threat finance investigations and prosecutions, using all available tools (e.g., civil forfeitures) to aggressively and offensively advance the nation's national security priorities.

- Providing legal advice to U.S. Attorney's Offices and investigative agencies on all matters within its area of responsibility, which includes 88 Federal statutes affecting national security.

- Providing advice and assistance to prosecutors nationwide regarding the application of the Classified Information Procedures Act (CIPA).

- Administering and enforcing the Foreign Agents Registration Act of 1938 (FARA) and related disclosure statutes.

- Accomplishing its mission through coordinated efforts and close collaboration with DOJ leadership, the Federal Bureau of Investigation (FBI), the IC, and the 94 United States Attorney's Offices (USAOs). CES also coordinates the use of all tools to protect our national assets, including use of law enforcement tools, and economic and diplomatic solutions, with interagency partners.

- Conducting corporate and community outreach for 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:

    - Collaborating with prosecutors nationwide on terrorism matters, cases, and threat information;

    - Maintaining an essential communication network between DOJ and USAOs for the rapid transmission of information on terrorism threats and investigative activity; and

    - 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, Data Security, Telecommunications, Foreign Adversary Apps, and Technology Supply Chains

- **CFIUS.** 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 mitigates any national security risks arising from those transactions, including making appropriate recommendations to the President to prohibit a transaction, and identifying non-notified transactions that were not filed with CFIUS (including bankruptcy proceedings) that might merit CFIUS review;

- **Outbound Investment.** Providing advice and contributing to the interagency development of the Department of Treasury's (TREAS) implementation of the outbound-investment program which regulates U.S. investments in certain technology sectors in countries of concern;

- **Team Telecom.** 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. Team Telecom is the interagency group through which the Executive Branch responds to Federal Communications Commission (FCC) requests for views on the national security and law enforcement implications of certain transactions involving foreign ownership, control, or investment that relates 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)[1];

- **Civil and Administrative Compliance and Enforcement.** Negotiating measures to mitigate national-security and law-enforcement risks for transactions reviewed by CFIUS and Team Telecom, monitoring private-sector compliance with any mitigation agreements, and investigating and undertaking enforcement actions, when appropriate, for breaches of agreements and other violations.

- **Foreign Adversary Apps.** Enforcing the Protecting Against Foreign Adversary Controlled Apps (PAFACA) Act, which generally makes it unlawful for U.S. companies to provide services to distribute, maintain, or update any foreign-adversary-controlled application, unless the application executes a qualified divestiture that the President determines (1) eliminates the foreign-adversary control and (2) "precludes the establishment or maintenance of any operational relationship" between the application's U.S. operations and foreign-adversary-affiliated entities.

[1] Executive Order 10530 "Providing for the Performance of Certain Functions Vested in or Subject to the Approval of the President".

- **Technology Supply Chain Threats.** Investigating, referring, and participating in interagency adjudication of national security threats posed by foreign-sourced technology, software, services, and equipment through the use of various supply-chain authorities, including the Department of Commerce's Information and Communications Technology and Services (ICTS) program under Executive Order 13873,[2] the Federal Acquisition Security Council (FASC), the Federal Communications Commission's Covered List, and the Department of War's (DOW) authorities under section 889 of the FY 2019 National Defense Authorization Act and section 1260H of the FY 2021 National Defense Authorization Act.

- **Other Legal, Litigation, and Policy Support.** Providing legal and litigation advice and policy support on broader legislative and policy matters involving issues at the intersection of national security, technology, 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, theft, intelligence-gathering, and malign influence;

- Providing advice and assistance to prosecutors nationwide regarding the leveraging and protecting of classified intelligence in cyber-related investigations, including through the application of CIPA;

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

- Sharing threat intelligence developed through national security investigations with private sector network defenders, with the aim of encouraging victim reporting and cooperation, empowering network defenders, and otherwise educating the American public about cyber threats; and

- Conducting corporate and community outreach relating to cybersecurity.

5. Intelligence Operations, Oversight, and Litigation

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

[2] Executive Order 13873 "Securing the Information and Communications Technology and Services Supply Chain".

- Representing the United States before the Foreign Intelligence Surveillance Court (FISC) to obtain authorization under 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, applicable laws and regulations, FISC orders, DOJ procedures, and Executive Branch policies, including the protection of individual privacy and civil liberties;

- Assessing FBI national security investigations to ensure conformity with the Constitution, applicable laws and regulations, and DOJ procedures, including the foreign intelligence and national security investigation provisions of the Attorney General's Guidelines for Domestic FBI Operations;

- Executing specific oversight functions directed by Congress designed to ensure compliance with FSA restrictions of particular concern;

- 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 Office of the Director of National Intelligence (ODNI) and the IC.

6. Victims of Overseas Terrorism

- Supporting U.S. 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 U.S. 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 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, 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;

- Providing advice and support on the development and implementation of watch listing programs related to national security threat actors and providing legal advice and guidance on Federal screening and vetting programs; and

- Supporting DOJ's participation in the NSC.

D. Recent Accomplishments (UNCLASSIFIED only)

- **Evolving Threat of Terrorism.** In FY 2025, DOJ charged over 230 individuals for terrorism-related conduct, including providing material support to Foreign Terrorist Organizations, ideologically driven violent threats and attacks, plots against critical infrastructure, and attacks against Americans around the world. 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.

- Protecting the American people from terrorists is one of the Administration's highest priorities. NSD leads the Department's efforts to coordinate the investigation, disruption, and prosecution of terrorist threats against American interests and people. In 2025, NSD, working with U.S. Attorney's Offices and law enforcement across the country, brought terrorism-

related charges against over 230 individuals, and secured convictions against over 150 defendants. Among those successes, the following are a few notable convictions:

- ***United States v. Routh:*** On September 23, 2025, after a two-week trial, a Federal jury found Ryan Wesley Routh guilty on all counts related to his attempted assassination of President Trump at the Trump International Golf Club on September 15, 2024, and on February 5, 2026, Routh was sentenced to life plus 84 months in Federal prison.

- ***United States v. Naser:*** On March 4, 2025, in the Eastern District of Michigan, the district court denied Aws Mohammed Naser's motion to suppress and/or disclose Foreign Intelligence Surveillance Act (FISA) materials. Naser had been given notice of the government's intent to use or disclose FISA information, and the Litigation Section of the Office of Intelligence drafted and prepared the brief and related filings protecting the FISA materials. On June 3, 2025, after a five-week trial, a Federal jury found Naser guilty of attempting to provide material support to ISIS and being a felon in possession of a destructive device. In 2016 and 2017, Naser attempted to build a destructive device after pledging loyalty to ISIS.

- ***United States v. Pahlawan:*** On June 5, 2025, a Federal jury found Muhammad Pahlawan guilty on all counts for smuggling Iranian advanced weapons from Iran to the Houthis to use against civilian and military shipping in the Red Sea. During a U.S. operation in January 2024 to interdict the shipment of weapons, two Navy Seals tragically lost their lives.

- **Espionage Enforcement.** NSD (through CES) continues its enforcement of the Espionage Act and Economic Espionage Act by successfully prosecuting defendants for violations of these laws. For instance, in August 2025, former U.S. Navy sailor Jinchao Wei was convicted of espionage for selling national defense information to an intelligence officer working for the People's Republic of China (PRC). Wei was also convicted of conspiracy and the unlawful export of technical data related to defense articles in violation of the Arms Export Control Act and the International Traffic in Arms Regulations. He was sentenced to 200 months imprisonment in January 2026. Similarly, in November 2025, defendant Ji Wang was convicted of economic espionage and the theft of trade secrets for stealing fiber laser technology with military applications from his employer for the benefit of the PRC.

- **Export Controls and Sanctions Enforcement.** In the face of increased efforts by our adversaries to acquire highly valuable and sensitive U.S. technologies, NSD's CES continues to prioritize export control and sanctions enforcement. Through criminal investigations and prosecutions, NSD has punished and deterred efforts by China, Iran, North Korea, and Russia to secure military technology, advanced microchips with AI applications, firearms, and aircraft from the United States. In addition to investigating and prosecuting individual wrongdoers, NSD sent a powerful message to corporations—setting both the floor and ceiling for enforcement in this space. On one hand, a powerful deterrent to corporate violators was created by securing a parent-level guilty plea from Cadence Design Systems, Inc. ("Cadence"), for exporting semiconductor design tools to a restricted PRC military university, resulting in nearly $118 million in criminal penalties. On the other hand, in the first ever application of the DOJ's M&A Policy, NSD declined the prosecution of private equity firm White Deer—which

discovered and voluntarily self-disclosed criminal violations of U.S. Sanctions laws committed by a company it acquired, Unicat Catalyst Technologies LLC (Unicat). It is worth noting that as part of the resolution, Unicat obtained a non-prosecution agreement, while the former Unicat CEO, Mani Erfan, pleaded guilty to conspiring to violate U.S. sanctions against Iran.

- **Counter-Threat Finance Actions.** NSD (through CES) has also applied its civil enforcement tools to seize assets and funds used by hostile regimes, thereby limiting their ability to operate.

- **Mishandling of Classified Information.** NSD also continues to prioritize cases involving the mishandling and unlawful retention of classified information related to the national defense. For example, in October 2025, former U.S. Department of State employee and Department of War contractor Ashley Tellis was charged with unlawfully retaining national defense information in his residence after a court-authorized search of his residence revealed over 1,000 pages of documents with classification markings, including materials labeled SECRET and TOP SECRET. The same month, former National Security Advisor John Bolton was charged with unlawfully retaining national defense information in his home and unlawfully transmitting national defense information using personal email and messaging application accounts.

- **Economic Espionage and Theft of Trade Secrets**. NSD (and CES in particular) defends American innovation against actions by its competitors which undermine our national security. A recent example is the case of Ji Wang, who stole critical data generated while he was working on a research project for Corning, funded by the Defense Advanced Research Projects Agency (DARPA). The project aimed at developing optical fibers for high-powered lasers with military and commercial applications. Wang attempted to use these stolen trade secrets to start a specialty fiber business in China, which included potential military users, using a grant from China's Thousand Talents Plan Award. Ultimately, law enforcement disrupted Wang's efforts. In November 2025, CES attorneys tried and convicted Ji Wang of two counts of economic espionage, one count of theft of trade secrets, one count of attempted economic espionage, and one count of attempted theft of trade secrets.

- **National Security Cyber Investigations.** NSD, through NatSec Cyber, continues to focus resources on disrupting and deterring adversaries' cyber-enabled efforts to harm U.S. national security through cyber intrusions and attacks, foreign malign influence, and sanctions evasion. NSD has utilized traditional law enforcement tools to investigate and disrupt state-sponsored malicious cyber and cyber-enabled activity, including through the seizure of funds or infrastructure and targeted sharing of threat intelligence from its criminal investigations with the private sector, United States Government, and foreign partners.

- Threat intelligence obtained through criminal investigations has provided the basis for NSD court-authorized disruption operations, such as the approximately 22 malware network and botnet takedowns and large-scale seizures seizure of digital assets and fiat currency (totaling approximately $15 billion in value) since 2018. Notable examples of recent NatSec Cyber accomplishments in this regard include:

    - **Disrupting Overseas Cyber Scam Centers**. In October 2025, NatSec Cyber initiated forfeiture proceedings against virtual currency valued at approximately $15 billion that

NatSec Cyber and FBI had seized in relation to human trafficking-powered cyber scam compounds operated by Cambodian national Chen Zhi and his Prince Group conglomerate. Concurrent with the forfeiture proceedings, NatSec Cyber indicted Chen Zhi for wire fraud and money laundering associated with such scam compounds. The forfeiture action, in which Chen Zhi and other claimants are actively litigating claims, represents the world's largest ever cryptocurrency seizure.

- **Interdicting Proceeds of DPRK Virtual Currency Heists.** By the end of 2025, NSD had seized virtual currency valued at approximately $72.6 million that Democratic People's Republic of Korea (DPRK) hackers stole from digital assets technology providers, developers, and users. Additionally, reflecting a victim-centric approach, NSD and the FBI regularly leveraged intelligence developed through their investigations to alert compromised victims before such heists can occur, and to issue multiple cybersecurity advisories containing actionable threat intelligence that empowers the digital assets sector's network defenders in their own efforts to counter the DPRK's attempted heists.

- **Thwarting Hamas Financing Schemes**. In 2025, NatSec Cyber disrupted an ongoing terrorist financing scheme through the seizure of more than $200,000 in cryptocurrency held in wallets and accounts intended to benefit Hamas. The seized funds were traced from fundraising addresses that Hamas used to launder more than $1.5 million in virtual currency since October 2024.

- **Removing PRC Malware from More Than 4,200 Infected U.S. Computers.** In January 2025, NatSec Cyber announced a multi-month, court-authorized law enforcement operation that deleted "PlugX" malware from thousands of infected victim computers worldwide, including approximately 4,258 U.S.-based computers. These computers were part of a malware network that a People's Republic of China (PRC) sponsored group, known to the private sector as "Mustang Panda" and "Twill Typhoon," had used to infect, control, and steal information from other victim computers worldwide.

- In parallel to these disruption efforts, NSD works to develop prosecutable cases against cyber threat actors, including approximately 60 *public* prosecutions since the inception of NSD's cyber program in 2014. Notable examples of recent NatSec Cyber accomplishments in this regard include:

  - ***United States. v. Xu, et al.*:** In July 2025, NatSec Cyber obtained the arrest of a PRC Ministry of State Security (MSS) hacker in Milan, Italy, for his involvement in 2020-2021 computer intrusions. These included the targeting of U.S. COVID-19 research and the indiscriminate "Hafnium" campaign that compromised thousands of computers in the United States and worldwide. (The Hafnium campaign was the subject of a 2021 NSD-led botnet takedown operation). Xu's extradition to the United States is pending in Italian courts.

  - ***United States v. Williams*:** In October 2025, NatSec Cyber obtained the guilty plea of Peter Williams, an Australian national and former Australian intelligence community

employee, to two counts of theft of trade secrets. Williams stole national-security focused software from his cleared defense contractor employer and sold it to a Russian cyber-tools broker in exchange for the promise of millions in cryptocurrency. The stolen software included at least eight sensitive and protected cyber-exploit components that Williams's employer marketed and sold exclusively to the U.S. government and select allies.

- **United States v. Ahmad 'Umar Agha:** In November 2025, NatSec Cyber obtained the arrest of Syrian Electronic Army hacker Ahmad 'Umar Agha for his involvement in hacking the White House, universities, technology companies, and numerous press entities on behalf of the Bashar Al Assad regime between August 24, 2011, and January 31, 2014. In one such instance, the Syrian Electronic Army commandeered the Associated Press' Twitter account and announced an explosion at the White House, which led to an immediate $136 billion stock market sell off.

- **Prosecution of the DPRK's U.S.-Based Facilitators:** The DPRK raises substantial revenue for its weapons programs and other regime priorities through remote information technology (IT) worker schemes. Teams of IT workers can generate as much as $3 million annually. From May 2024 through FY 2025, NatSec Cyber charged 10 U.S.-based individuals who helped various IT worker teams generate approximately $25 million in income for fraudulent DPRK IT workers. In connection with these and other DPRK IT worker investigations, NatSec Cyber seized approximately 525 laptop computers provided by victim employers that were hosted at the residences of the U.S.-based facilitators and accessed remotely by the DPRK IT workers to carry out their schemes.

- **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 U.S. assets and technology.

  - NSD reviewed approximately 13% more merger, acquisition, and investment submissions in FY 2025 than in FY 2024.

  - NSD led approximately 20% of the matters in which a Joint Voluntary Notice (JVN) was filed with CFIUS in FY 2025, a 19% decline from the prior five-year averages.

  - In approximately 14% of DOJ co-lead cases closed, the transaction was prohibited, abandoned, or mitigated, based on national security risks identified by NSD, down from a high of 59% in FY 2023 and an average of 32% for FY 2020 to FY 2024. Out of all CFIUS cases mitigated, NSD co-led 20% of such cases in 2025 and 28% of cases annually in FY 2020 through FY 2024. Further:

    - NSD co-led several particularly challenging cases in FY 2025. In one case, NSD was able to resolve national security risks that arose when a sovereign wealth fund purchased a gaming company which collected and stored highly sensitive data of its users. NSD articulated a risk and crafted a mitigation which

ensured the foreign entity would not gain access to the player data. NSD also served an invaluable role in reviewing Nippon's acquisition of U.S. Steel. NSD worked extensively with the co-leads to develop a risk-based assessment that met statutory requirements. NSD also spent significant time ensuring that any decision to block the transaction was legally supported and afforded the transaction parties due process.

- NSD has continued to expand its international outreach efforts with allied nations to promote and strengthen those countries' investment screening processes.

- In 2025, CFIUS met with several companies that frequently appear before CFIUS. NSD represented DOJ at those meetings which focused on making the CFIUS process more efficient and effective when reviewing transactions from countries such as the United Arab Emirates, Saudi Arabia, Japan, Taiwan, Canada, and Australia. NSD is the DOJ designee for Treasury's Outbound Investment Security Program. NSD regularly attends update meetings with interagency counterparts and has provided feedback to Treasury in particular cases where DOJ's expertise is required.

- **Protecting U.S. Telecommunications.** NSD represents the Attorney General in her formal role as the chair of Team Telecom as required under Executive Order 13913[3], 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. In addition to the substantive work associated with a Team Telecom review, NSD manages the operation and administration of this multi-agency committee, assuming responsibilities that include communicating directly with outside parties, managing the case review docket, and interacting with the FCC.

    - Team Telecom closed out many long-running cases in FY 2025, resulting in 102% more cases concluded in FY 2025 than in FY 2024 and 7% higher than in FY 2020 through FY 2024.

    - In addition, the complexity of the reviews increased substantially during the same period, with approximately 58% of referrals requiring mitigation in FY 2025. As the Chair, NSD led or co-led all the reviews for FCC referrals to Team Telecom for applications of licenses.

    - During FY 2025, Team Telecom initiated one review of existing FCC licenses that either presents new or additional national security or law enforcement risks or involves material noncompliance by the license holder with the mitigation agreement. Team Telecom continues to review 11 other potential matters involving existing licenses.

    - In FY 2025, Team Telecom concluded 400% more submarine cable landing license applications from hyperscaler operators, such as Google and Meta, than in FY 2024 and

[3] Executive Order 13913 "Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector".

166% more submarine cable cases than in FY 2020 through FY 2024. Leveraging the success of complex negotiations with those hyperscalers in FY 2024, Team Telecom was able to review and close 20 cases involving new submarine cables (18 FCC referrals), without resorting to more complex and time intensive secondary assessments. This allowed for faster license approvals and the quicker deployment of critical communications infrastructure.

- Team Telecom continued to undertake measures in FY 2025, as part of a years-long project, to streamline its process and simplify information requirements, consistent with the America First Investment Policy. These measures have decreased the timelines for the FCC licensing approvals referred to Team Telecom and have appropriately triaged referrals using a risk-based approach to use existing resources more effectively and in a targeted fashion.

- FIRS continues to work with the FCC's Enforcement Bureau to police companies' adherence to mitigation agreements and address issues of non-compliance. These efforts led to a recent landmark FCC enforcement action that resulted in a consent decree and a monetary penalty, the first-ever for breaching a Team Telecom mitigation agreement. Team Telecom anticipates more compliance enforcement activities along these lines in the next fiscal year.

- **Protecting Technology and Software Supply Chains.** NSD is the leading source of referrals and assistance—as well as participating as a member agency—to various interagency committees charged with addressing national-security risks posed by foreign-adversary participation in supply chains for technology and software used in the United States. The Department of Commerce's Office of Information and Communications Technology and Services (ITCS), which is responsible for implementing several ITCS authorities, is one of the primary interagency partners in this space.

  NSD continues to provide assistance to the Department of Commerce in administering and implementing Executive Order 13873, "Securing the Information and Communications Technology and Services (ICTS) Supply Chain" authority, the OMB-led Federal Acquisition Security Council (FASC) in administering its SECURE Technology Act authority, and the Federal Communications Commission in administering its "Covered List" pursuant to the Secure and Trusted Networks Communications Act. These regulatory regimes were established to address the Government's and the private sector's exposure to national security risk through the U.S. ICTS supply chain. Since 2021, NSD submitted 11 referrals to the Secretary of Commerce which identified 16 companies of concern for investigation, as well as two referrals to the FASC that identified four companies of concern for investigation. To date, NSD remains one of two U.S. Government entities to make a referral pursuant to these new authorities.

- **Monitoring and Enforcing Compliance with National Security Agreements.** In FY 2025, NSD led and completed high priority national security reviews in two new CFIUS and 23 new Team Telecom national security agreements that NSD negotiated and entered with companies and will monitor for compliance going forward.

- NSD spearheaded, along with colleagues in the Civil Division, a statement of interest filed on behalf of the United States in the bankruptcy proceeding for the genomic testing company 23andMe – action that was praised by Members of Congress. The statement outlined potential national security processes that could develop if certain foreign acquirers attempted to buy the company or its assets. The bankruptcy court ultimately identified a U.S. buyer following the statement of interest, which substantially reduced many of the potential negative outcomes of the sale that could have put the sensitive genetic data of millions of Americans at risk.

- NSD conducted nine in-person mitigation compliance site visits in the first quarter of FY 2025 and two site visits during the remainder of FY 2025.

- The total number of national security agreements monitored by NSD continues to increase, up to 209 active agreements at the end of FY 2025. This reflects approximately 14% more complex mitigation matters from FY 2020 to FY 2025 and annual average increases in agreements of 12% from FY 2020 to FY 2025.

- This significant rise in complex mitigation matters reflects the growth of new mitigation agreements, ongoing agreement terminations, and a 66% annual average increase in mitigation matters negotiated and supported for CFIUS and Team Telecom.

- FIRS terminated a total of 13 agreements in FY 2025.

- In FY 2025, NSD referred to the FCC an enforcement matter that the FCC took up and concluded action on in 2026, a first-of-its-kind partnership to increase the accountability of parties who execute national security commitments to reduce national security risk.

- **Implementation of FISA Authorities to Foil National Security Threats and Advance Administration Priorities.** Although the details are classified, NSD continued to make appropriate use of FISA authorities to gather foreign intelligence information of critical importance to the IC and to foil a number of severe national security threats, including some that involved threat to life. In addition, one particular achievement this past year has been the new narcotics Section 702 certification to permit the government to better address the scourge of drugs and international cartels, a high Administration priority.

- **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. 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 CY 2025, NSD completed 37 such reviews of 109 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 – the National Security Agency (NSA), the Central Intelligence Agency (CIA), FBI, and the National Counterterrorism Center (NCTC). The most recent publicly available numbers show that the FBI conducted 5,518 U.S. person queries of raw Section 702-acquired information in CY 2024. The query oversight program significantly increased in CY 2024 and CY 2025,and we anticipate its continued growth through CY 2026 and 2027 due to the requirements in the Reforming Intelligence and Securing America Act (RISAA) to audit 100% of FBI's U.S. person queries of unminimized Section 702-acquired information, along with increasing taskings pursuant to Section 702.

- **Implementing RISAA**. RISAA imposed multiple new obligations on NSD. As a part of its response to the new obligations, OI established several new oversight programs that have consumed a significant amount of attorney resources. Included in these, OI:

    - Implemented a process to audit every U.S. person query conducted by FBI within one week of it being conducted.

    - Implemented a process to pre-review all non-emergency Section 702 queries conducted only to retrieve evidence of a crime to ensure all proposed queries fall within the limited statutory exceptions to the RISAA imposed prohibition on queries to retrieve evidence of a crime.

    - Initiated a review of FBI technical systems in which FBI personnel can conduct Section 702 FISA queries to ensure these legacy FBI systems have been appropriately updated to account for new legal requirements. Due to the age and complexity of these systems, this project has required a significant amount of attorney resources. NSD has identified and worked with FBI to remediate one legacy system sub-feature that could have allowed FBI users to conduct U.S. person queries without meeting the relevant RISAA requirements.

- **FBI Minimization.** OI collaborated with the FBI in its development of several new programs and innovations to ensure the Bureau was satisfying its obligations to manage and store information collected under Section 702 within the boundaries of FISC ordered procedures, particularly information pertaining to U.S. persons. The FBI minimization team worked over many months with FBI to investigate FBI's partnership with another government agency's electronic information storage system and to provide a full accounting to the FISC. This partnership has allowed the FBI to leverage more efficiencies in viewing and receiving information about a particularly sensitive national security investigation.

- **National Security Reviews (NSRs).** In January 2026, the U.S. Government Accountability Office (GAO) issued a Report to Congressional Requestors on FBI Investigative Activities entitled "Oversight Efforts of Opening and Conducting Assessments Should be Strengthened" (**GAO-26-106994SU**). The results of GAO's report emphasized the importance and value of the NSRs conducted by NSD. GAO had no recommendations for the NSD about its review of FBI national security assessments but did recommend that FBI share NSD's NSR findings across the Bureau.

- **CLOUD.** The team of attorneys working on issues related to the Clarifying Lawful Overseas Use of Data (CLOUD) Act conducted 80 reviews over FY 2025. These reviews help ensure compliance with procedures governing the acquisition and use of data by American law enforcement under the CLOUD Act. Specifically, the CLOUD team reviews orders obtained under the CLOUD Act before they are served on providers overseas and works with law enforcement to ensure that CLOUD Act data, once acquired, is used consistently with the governing agreements and procedures. The results of these reviews are compiled by the CLOUD team into annual reports that OI is required to provide to the Office of International Affairs (OIA) at DOJ. OIA then incorporates these inputs into broader reports provided to the governments of Australia and the United Kingdom. The CLOUD team also continued its coordination with OIA to respond to questions from Australia and the United Kingdom regarding the interpretation of procedures governing their acquisition of data from U.S.-based providers under the CLOUD Act.

- **Assisting IC Agencies with Compliant Use of Artificial Intelligence Tools**. As IC agencies expand their use of AI, those tools raise new compliance issues and questions. The Oversight Section has worked closely with IC agencies to discuss new AI tools that are involved in processing or analyzing FISA-acquired information, answer their questions, and help them use this powerful new technology in ways that comply with agency procedures, statutes, and the Constitution.

- **Assisting Victims of Overseas Terrorism.** In FY 2025 and into FY 2026, OVT continued to support U.S. victims of international terrorism by providing them with foreign legal system information and communicating with foreign counterparts around the world, such as Algeria, France, Germany, Indonesia, Israel, Kenya, Sri Lanka, and the United Kingdom. OVT provided travel and participation assistance to ISIS hostage-taking victims in an FY 2025 French trial and provided similar assistance to the next of kin and a support person to travel to London for the FY 2024 conclusions of a Coroner's Inquest. OVT also assisted with the submission of written victim impact statements in trials in Kenya and France. Foreign criminal justice attendance and participation can be an important element of the victims' journey, help the victims seek accountability, help them understand what happened, and that they are part of a larger community. At their request, OVT also facilitated a meeting between a victim's family and other members of NSD so that the victims might share their concerns regarding prisoner releases and seek insights on U.S.-based prosecutions.

- **Providing Training to Domestic and International Partners.** OVT provided in-person training and information about its mission and subject matter to the European Commission's Network of EU single contact points for victims of terrorism in FYs 2024 and 2025 and the European Network for Victims' Rights in FY 2026. OVT also provided programmatic training to DOJ's Office of Prosecutorial Development, Assistance, and Training (OPDAT) staff to foster internal DOJ collaboration.

- **Supporting International Cooperation on Victims of Terrorism.** OVT has cooperated with the U.S. Department of State's (DOS) Bureau of Counterterrorism through its participation in the Council of Europe's 24/7 Network of Contact Points on Victims of Terrorism and their efforts in creating best practices and guidelines, and with the U.S. Mission to the United Nations regarding their continuing efforts to support and assist victims of terrorism.

- **Defending U.S. Law. *Latombe v. European Commission*:** On September 3, 2025, the General Court of the European Union (E.U.) dismissed a French parliamentarian's action for annulment of the E.U.'s "adequacy decision" that underlies the U.S./E.U. Data Privacy Framework. E.U. law requires a valid adequacy decision to permit the flow of personal data from the E.U. to a destination country, and thousands of U.S. companies rely on the E.U. adequacy decision, which sustains $7 trillion in commercial transactions with European customers, vendors, and partners. E.U. courts had invalidated similar adequacy decisions twice on prior occasions (in 2015 and 2020). The *Latombe* judgment means that the current adequacy decision remains intact and will continue to serve as the basis in E.U. law for E.U.-U.S. commercial transfers of personal data. NSD's Law & Policy Section drafted litigation briefs in this matter, advised and prepared foreign counsel on the legal issues at play, and provided in-person advice and assistance at the E.U. court hearing in Luxembourg to defend the adequacy of U.S. law.

- **Success Before the U.S. Court of Appeals.** NSD's Appellate Section handled several successful appeals, drafted the government's brief, and presented oral arguments to the U.S. Court of Appeals, including:

    - ***United States v. Arthur*:** On December 3, 2025, the Fourth Circuit rejected a facial First Amendment challenge to the constitutionality of 18 U.S.C. § 842(p)(2)(B), which prohibits providing bombmaking instruction knowing that the recipient intends to use the information in a Federal crime of violence. This is first court of appeals decision to address the constitutionality of the statute, and the panel concluded that it complies with the First Amendment because it criminalizes speech integral to criminal conduct. As a result, the panel affirmed the conviction of Christopher Arthur for teaching an FBI confidential informant bombmaking techniques that he believed would be used against ATF agents that were going to return to the informant's home.

    - ***United States v. Carpenter*:** On October 31, 2025, the Sixth Circuit affirmed the convictions and sentence of Benjamin Carpenter for attempting to provide material support to ISIS. Carpenter was sentenced to 20 years of imprisonment after a jury convicted him of attempting to provide material support in the form of translation services that he performed for an FBI undercover agent. The Sixth Circuit unanimously rejected Carpenter's arguments that his conduct fell outside the material support statute, as well as numerous evidentiary challenges and claims that the government violated the Classified Information Procedures Act in his case. The court also rejected his claims that his 20-year sentence was procedurally or substantively unreasonable.

    - ***United States v. Abouammo*:** On December 4, 2024, the Ninth Circuit affirmed the convictions of Ahmad Abouammo, including for acting as an agent of a foreign government within the United States without prior notification to the Attorney General, wire fraud, and money laundering. Abouammo used his position at the social media company then known as Twitter to access nonpublic information about pseudonymous accounts, which he then provided to a foreign government official seeking to identify dissidents. In return he was paid hundreds of thousands of dollars and given an expensive watch.

E. Performance Challenges

Increasing and Changing Threats to the United States

Protection of National Assets and Enforcement of Export Controls and Sanctions

Protecting national assets (both public and private) through the criminal investigation and prosecution of counterintelligence, export control, and sanctions offenses remains a top priority for CES. CES has continued to see increased investigations and charges across portfolios, taxing already limited resources. Against the backdrop of an increasing case load, CES is facing unprecedented personnel constraints. In mid-2024, CES was staffed by 45 criminal prosecutors; currently, CES has only 27 criminal prosecutors. In other words, CES has 40% fewer prosecutors than it did a year and a half ago, but the section has seen no reduction in total matters—which has been hovering at approximately 1,500 for several fiscal years. CES's FARA Unit is also short-staffed, having lost 60% of its attorneys and 40% of its analysts since mid-2024. Replenishing CES's human resources is necessary to ensure that the section can continue to perform its vital national security function.

Despite its staffing challenges, many enforcement-related indicators have continued to rise. One such example is voluntary self-disclosures (VSDs). In 2024, there was a 50% increase in the number of VSDs submitted to NSD, as compared to 2023. In 2025, there was a 67% increase in VSDs submitted to NSD, as compared to 2024. In FY 2025, NSD began to formally distinguish (for the first time) between partnership and consultation cases. In FY 2025, the number of charged partnership cases was 67, compared to 139 charged cases (of all kinds) in FY 2024, 163 in FY 2023, and 114 in FY 2019. During that same period, the number of defendants charged was 67 in FY 2025, 139 in FY 2024, 163 in FY 2023, and 114 in FY 2019. Moreover, in FY 2024, CES negotiated its own grand jury access with the District Court for the District of Columbia, and CES continued to lead investigations pursuant to that authority in FY 2025. In those matters, CES is working without a U.S. Attorney's Office as a partner, and CES attorneys and support staff must issue, track, and process returns for all grand jury processes issued. Similarly, CES attorneys are prosecuting certain charged criminal cases without a U.S. Attorney's Office partner, and in those matters, CES attorneys and staff are responsible for conducting the prosecution, including administering discovery and preparing for trial.

The unlawful export of sensitive technologies and the theft of trade secrets and intellectual property by nation-state actors represent a critical and growing threat to U.S. national and economic security interests. U.S. adversaries continue to pursue a sustained campaign of stealing U.S. innovations and acquiring superior U.S. technologies. These adversaries employ sophisticated strategies to obtain export-controlled and proprietary technologies, including through a combination of legitimate commercial channels and illicit procurement networks. Increasingly, nation-state adversaries rely on complex commercial networks to export sophisticated technologies such as AI chips to third countries, and then unlawfully divert them to prohibited countries and end users, in violation of export control and sanctions laws. 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.

CES continues to pursue the most complex national security investigations, including those involving sophisticated international networks and corporate defendants. However, these cases pose unique challenges. International investigations are resource-intensive and often require extensive coordination with other government agencies, and sometimes with U.S. government components located overseas. Many of CES's ongoing and recent cases have involved the collection and review of voluminous

documents, sometimes numbering in the millions. Discovery in such cases is painstaking, time-intensive, and aggressively litigated by sophisticated, well-resourced defense counsel. CES's white-collar cases often require reviews to filter out documents protected by attorney-client privilege. These issues have combined to make complex national security cases involving international networks or corporate defendants particularly challenging – both legally and logistically.

National Security Cyber-Related Investigations and Disruptions

Cyber and cyber-enabled threats continue to expand and evolve rapidly. 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 U.S. critical infrastructure at risk to destructive or disruptive attacks. In addition, nation-states and criminal actors are forming a "blended threat" of alliances that enable malicious cyber activity to proliferate in ways that have profound national security implications. This blended 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 nation-states' intelligence services.

To counter these growing and sophisticated threats, NSD must recruit and hire personnel with preexisting cyber experience who can be dedicated to focus on these issues. Both new and veteran personnel must also receive training to stay abreast of new technologies that can be used by, and against, our cyber adversaries. In this decisive decade for cybersecurity, the window of opportunity for getting ahead of this threat is narrow. Closing the gap between NSD's present capabilities, as described below, and NSD's anticipated needs to meet President Trump's Cyber Strategy for America's (National Cyber Strategy) ambitions (Pillars 1 and 4 in particular), will require steadfast and sustained commitment.

The creation of NatSec Cyber in 2023 allowed NSD to focus resources on countering expanding and sophisticated cyber and cyber-enabled threats. Because they are often highly technical, investigating and prosecuting cyber threats requires substantial investigative and prosecutorial 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 appropriately balance various law enforcement, intelligence, and diplomatic interests. For example, NatSec Cyber's unique expertise in analysis and coordination is often required for issues relating to: (a) how to protect classified information pursuant to CIPA; (b) the appropriate use of FISA authorities and other classified information in furtherance of investigations and whether notice to a defendant is required; (c) how investigations can leverage or support the actions of the United States Intelligence Community (USIC) and DOW partners; and (d) how prosecutions can proceed without otherwise unduly impacting USIC and other national security interests.

Additionally, outside the context of traditional nation-state threats, recent ransomware attacks underscore the growing threat that ransomware and digital extortion pose to the United States, and the destructive and devastating consequences those attacks can have on national and economic security. For these reasons, the U.S. Government now considers ransomware as a national security priority. Accordingly, 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 USIC, DOW, and other relevant agencies, to disrupt and dismantle the infrastructure, networks, and foreign safe havens used to carry out these attacks. These developments have vastly expanded the number of cyber-related investigations and the

policymaking processes for which NSD must coordinate with the National Security Council, USIC, DOW, and other inter-agency partners as part of NSD's role as the Department's lead in NSC's National Security Memorandum 2 on processes and liaison activities with the USIC. *See* (*e.g.,* 28 C.F.R. § 0.72 and Justice Manual 9-90.010 *et seq.).* Consequently, NSD will be expected to adequately resource the Department's counter ransomware efforts, and to bring to bear its unique authorities and expertise.

Further, with the increasing use, types, and value of virtual currency and digital assets over the past several years, some adversary governments use hacking, ransomware, and other forms of theft and cyber-enabled sanctions evasion to obtain funding to support the government's malign 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 and IT workers fraudulently posing as Western programmers 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.

Similarly, our adversary governments are increasingly leveraging artificial intelligence ("AI") to amplify the scale, speed, and sophistication of cyberattacks. AI-driven tools can automate vulnerability discovery, enabling attackers to identify and exploit weaknesses far faster than traditional manual methods. Through machine learning, adversaries can craft highly convincing phishing messages, deepfake audio, and synthetic video that erode trust and deceive even well-trained users. AI also allows malware to adapt in real time, altering its behavior to evade detection by security systems. The widespread availability of powerful AI models lowers the barrier to entry, empowering adversaries with less resources and skills to conduct malicious activities mirroring the sophistication of more mature cyber adversaries. These developments strain investigative and prosecutorial resources, as NatSec Cyber must now counter complex and dangerous threats to U.S. national security that learn, evolve, and operate autonomously. Adversary use of AI demands proactive efforts to ensure NatSec Cyber's prosecutors stay abreast of the latest AI technologies so that they can identify and disrupt their use by our adversaries at the "speed of cyber."

Foreign Investment Review

Increasing Workload. FIRS's work has been consistently increasing in volume and complexity since its last baseline personnel increase in FY 2020. Work streams that were previously performed by other DOJ components (such as the Civil Division and FBI) have been shifted to FIRS over the course of FY 2025. Every year since the last baseline personnel increase in FY 2020, FIRS has accumulated a higher workload.

FIRS's workload has also continued to increase in complexity across all its portfolios. For example, in FY 2025, FIRS completed reviews and investigations of 20% more CFIUS transactions than the prior year, and 45% of the declarations co-led by DOJ have resulted in full filings and reviews before CFIUS (compared to 26% of declarations led by other CFIUS agencies). Likewise, FIRS's Team Telecom completed 102% more cases in FY 2025 than the prior year. These complex Team Telecom cases resulted in 23 new DOJ-monitored mitigation agreements in FY 2025 alone, 35% more than the annual average for the prior five years – adding the responsibility to monitor those new agreements to FIRS's

Compliance & Enforcement Unit. In addition, the number of active mitigation agreements monitored by FIRS hit an all-time high in FY 2025 at 209 agreements (13% higher than prior five-year averages case load), in addition to a record number of open enforcement investigations and actions.

Finally, in FY 2025, FIRS's workload increased further as it became responsible for the Department's implementation of additional Presidential and Department priorities, including implementing the America First Investment Policy, facilitating and securing the deployment of the necessary data, telecom, and other infrastructure and services (such as submarine cables and data centers) needed to power American leadership in AI under the 2025 Executive Order on Removing Barriers to American Leadership in AI, assisting the Department of Commerce, the Department of War, the FCC, and other agencies in "expand[ing]" controls on secure technology supply chains under the America First Trade Policy, and others.

Significant Workforce Attrition Impacting NSD's Ability to Handle Intelligence Operations, Oversight and Litigation Responsibilities.

OI, which takes the lead in handling intelligence operations, oversight and litigation responsibilities, particularly as they pertain to FISA, experienced significant staffing attrition in CY 2025. As of January 2026, OI is 27 positions below the authorized level (15 positions under for OI's Operations Section, 11 positions under for the Oversight Section and one position under for OI's Litigation Section). Similarly, as of January 2026, OI is understaffed by 14 authorized non-attorney positions. Due to the hiring freeze, OI has not been able to replace these significant losses.

Increasing Workload in Intelligence Oversight, Operations, and Litigation

NSD's intelligence oversight work is an essential component of its 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 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 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. The number of targets grew approximately 215% from CY 2014 through CY 2024. 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%[4] increase in the number of matters handled by OI, from FY 2014 through FY 2025. 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 risen. 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. The yearly increases from CY 2022 through CY 2025 were over 60%, and OI expects the increase in such compliance investigations by OI will continue in CY 2026 and CY 2027. In addition, as part of its

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

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.

Further adding to the Section 702 growth, in April 2024, Congress reauthorized Section 702 of FISA through RISAA. Through RISAA, Congress has levied new auditing requirements on NSD's oversight of the IC's queries of raw Section 702 information and the IC's compliance with its targeting procedures and statutory requirements under Section 702. In particular, RISAA requires NSD to audit 100% of FBI's U.S. person queries. From CY 2023 through CY 2025, NSD reviewed well over 100,000 FBI U.S. person queries of Section 702 information. This new requirement will continue to necessitate additional oversight reviews and significant additional resources. Meanwhile, NSD will still audit U.S. person queries of Section 702 information conducted by other IC agencies. NSD will also continue to conduct oversight of the IC's implementation of non-Section 702 FISA authorities. In short, the bill provisions include auditing and congressional reporting requirements that substantially increase the workload of OI.

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 OIG's December 2019 Report, *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* (OIG Report). 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. These resource-intensive reviews require multiple attorneys to complete and may 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 but will require complementary training and the development of additional oversight programs to ensure compliance with these procedures.

Terrorism Threats Continue to Flourish.

In recent years, the threat of terrorist attacks has continued to increase. Whether driven by animus against the United States and western culture from abroad or by extremist ideology domestically, the depth and breadth of the terrorist threats we face grows year over year. To stay ahead of myriad threat actors, to thwart terrorist plots, and to stymy the steady stream of new threat trends requires ensuring NSD has adequate resources.

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, nihilist violent extremists, 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 engaging with foreign partners to counter the threat. These threats will continue to pose unique challenges for the foreseeable future.

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 and in other engagements, DOW has received and collected significant amounts of material that must be reviewed for both intelligence and evidence to potentially be used in foreign or U.S. prosecutions. NSD continues to provide advice and support on the dissemination and potential use of such materials to the FBI and DOW as part of efforts to encourage partner nations to repatriate and, where appropriate, prosecute their citizens. NSD also provides critical training to foreign partners to build their capacity to prosecute terrorism offenses, including those committed by repatriated foreign fighters.

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 U.S. citizens and high-level ISIS fighters who have been repatriated from the custody of the Syrian Democratic Forces. In addition, recent terrorist designations of branches of the Muslim Brotherhood will likely result in additional investigations and prosecutions in the coming years.

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. On February 5, 2025, the Attorney General announced the formation of Joint Task Force 10-7 – a vigorous effort to investigate and prosecute those responsible for the attack on and kidnapping of over 50 U.S. victims as part of the invasion into Israel. In October 2025, an individual in Louisiana was charged with offenses related to his participation in the 10-7 attack. The prosecution is being led by members of Joint Task Force 10-7.

In National Security Presidential Memorandum 2 (NSPM-2), issued on February 4, 2025, the President directed the Attorney General, in collaboration with partners across the government, to address the threats posed by Iran and its terror proxies by investigating, prosecuting, and otherwise disrupting financial and logistical networks, operatives, and front groups inside the United States; their foreign-based hacking corps; and the leaders and members of terrorist groups and terror proxies responsible for capturing, harming, or killing American citizens and seizing illicit Iranian oil exports. NSD supports this effort through the work of multiple attorneys and support staff working on related investigations and prosecutions, including prosecutions of plots by Iranian-linked actors to assassinate the President, Iranian dissidents in the United States, and former U.S. government officials.

NSD assists USAOs with managing voluminous classified and unclassified discovery in terrorism-related cases. In addition, NSD is responsible for protecting classified information in all terrorism-related cases as well as a variety of other criminal matters where classified information is involved. These efforts start with working with IC partners through the Prudential Search Request (PSR) process, to identify classified information related to a particular case, and end with litigation under the Classified Information Procedures Act (CIPA), to protect vital national security information during a prosecution. After the

designation of cartels and TCOs as FTOs, NSD saw a sharp increase in the number of PSRs in 2025. As cases related to these PSRs work through the system, NSD anticipates a significant increase in litigation under CIPA to protect critical intelligence information.

Continuing Need for Assistance to U.S. Citizen Victims of Overseas Terrorist Attacks and Support for Foreign Terrorism Prosecutions

Americans have fallen victim to 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, foreign attacks harming U.S. victims continue. 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 U.S. 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 U.S. 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 and helps U.S. 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 U.S. Government and throughout the world.

In addition to its direct victim services and international training and technical assistance, OVT also plays a role in U.S. Government financial support programs for U.S. victims of overseas terrorism. For example, OVT administers the attack designation process for the International Terrorism Expense Reimbursement Program (ITVERP), which provides reimbursement for some victims' expenses related to overseas terror attacks. Further, OVT operates the Criminal Justice Participation Assistance Fund (CJPAF), a victim foreign travel funding program, which can be administratively burdensome.

OVT supports U.S. citizen terrorism victims over the long term, no matter how long the search for justice and accountability takes. Its caseload is cumulative with new attacks that occur. 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 U.S. citizen victims requires sustained and intensive efforts to research and understand foreign laws and directly engage in foreign justice systems despite barriers of unfamiliarity, distance, and language. OVT continues innovative engagement with foreign governments to encourage good practices that will benefit U.S. citizen terrorism victims involved with those systems. OVT seeks to support U.S. citizen victims who live both at home and abroad with comprehensive, efficient, and compassionate services. OVT provides 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 U.S. Government's commitment to its citizens who suffer great losses and profound and life-altering trauma at the hands of terrorists.

II. Summary of Program Changes

Not applicable

III. Appropriations Language and Analysis of Appropriations Language

Appropriations Language

SALARIES AND EXPENSES, NATIONAL SECURITY DIVISION

For expenses necessary to carry out the activities of the National Security Division, $123,000,000, 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
2025 Enacted	359	364	$128,000,000
2026 Enacted	321	342	$117,200,000
Adjustments to Base and Technical Adjustments	4	14	$5,800,000
2027 Current Services	325	356	$123,000,000
2027 Request	325	356	$123,000,000
Total Change 2026-2027	**4**	**14**	**$5,800,000**

National Security Division - Information Technology Breakout (of Decision Unit Total)	Direct Pos.	Estimate FTE	Amount
2025 Enacted	26	26	$15,822,000
2026 Enacted	26	26	$25,286,000
Adjustments to Base and Technical Adjustments	-26	-26	($514,000)
2027 Current Services	0	0	$24,772,000
2027 Request	0	0	$24,772,000
Total Change 2026-2027	**-26**	**-26**	**($514,000)**

1. Program Description

NSD is responsible for:

- Overseeing terrorism investigations and prosecutions;

- Protecting critical national assets from national security threats, including through handling counterintelligence, counterproliferation, and national security cyber cases and matters; reviewing, investigating, and assessing foreign investment in U.S. business assets; countering malign foreign influence activities; 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, prevent, deter, and disrupt terrorist and other acts that threaten the United States, including counterintelligence threats and cyber threats to the national security;

- Serving as DOJ's liaison to the DNI, advising the Attorney General on all matters relating to the national security activities of the United States, and developing strategies for emerging national security threats – including cyber threats;

- Administering the U.S. Government's national security program for conducting electronic surveillance and physical search of foreign powers and their agents pursuant to FISA;

- Conducting oversight of certain activities of the IC components and the FBI's foreign intelligence and counterintelligence investigations pursuant to the Attorney General's guidelines for such investigations. NSD in this regard, prepares and files all applications for electronic surveillance and physical search under FISA, represents the U.S. 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;

- Working 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;

- Advising government agencies on a range of matters of national security law and policy, while also participating in the development of national security and intelligence policy through NSC-led policy committees and the Deputies' Committee processes. NSD 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 CIA, the FBI, DOW, and the State Department concerning questions of law, regulations, and guidelines as well as the legality of domestic and overseas intelligence operations;

- Serving as the staff-level DOJ representative on CFIUS, which reviews foreign acquisitions of domestic entities affecting national security. In this role, NSD evaluates information relating to the structure of transactions, foreign government ownership or control, threat assessments provided by the IC, vulnerabilities associated with transactions, and ultimately the national security risks, if any, of allowing a transaction to proceed as proposed or subject to conditions. NSD tracks and monitors transactions that were approved subject to mitigation agreements and seeks to identify unreported transactions that may require CFIUS review. To help fulfill the Attorney General's new role as Chair of Team Telecom, NSD also leads the interagency process to respond to FCC requests for Executive Branch determinations relating to the national security implications of certain transactions that involve FCC licenses. NSD reviews such license applications to determine if a proposed communication provider's foreign ownership, control, or influence poses a risk to national security, infrastructure protection, law enforcement interests, or other public safety concerns sufficient to merit mitigating measures or opposition to the license; and

- Finally, NSD, through its OVT, provides American victims of overseas terrorist attacks the services and support needed to navigate foreign judicial systems. Services include providing foreign system information and case notification, assistance for victim attendance and participation in foreign criminal justice systems as permitted by foreign law, and referrals to U.S. and foreign government and non-governmental services providers. OVT further provides expertise and guidance within DOJ and to U.S. Government partners on issues important to U.S. victims of overseas terrorism. OVT also works with government and international organizations to deliver international training and technical assistance to encourage recognition of rights for victims of terrorism around the world. Grounded in U.S. victims' rights and international best practices, OVT supports a role for terrorism victims in foreign partners' justice systems.

V. Program Increases by Item

Not applicable

VI. Program Offsets by Item

Not applicable

VII. EXHIBITS