# FY 2019
# Performance Budget
# Congressional Justification


## NATIONAL SECURITY DIVISION

Protecting the Nation's citizens from threats to our national security by pursuing justice through the rule of law

# Table of Contents

# I. Overview for National Security Division

## A. Introduction

The National Security Division (NSD) works to protect the United States from threats to our national security by pursuing justice through the rule of law, the Department of Justice's (DOJ) top priority. NSD requests for FY 2019 a total of 362 positions (including 243 attorneys), 362 FTE, and $101,369,000.[1]

## B. Background

NSD has six areas of focus that will guide its operations in the coming years. NSD will:

- 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 homegrown violent extremism and cyber-enabled terrorism;
- Protect national assets from nation-state and terrorist threats, including through investigating, prosecuting, and disrupting espionage activity, proliferation, and foreign investment threats; and strengthening partnerships with potential targets of intelligence intrusions;
- Combat national security cyber-based threats and attacks through the use of all available tools, strong public-private partnerships, and by investigating and prosecuting cyber threat actors;
- Investigate and prosecute the unauthorized disclosure and improper handling of classified information; and
- Ensure that Intelligence Community (IC) agencies have the legal tools necessary to conduct intelligence operations while safeguarding privacy and civil liberties.

Division Structure

NSD strengthens the Department's core national security functions by providing strategic national security policy coordination and development. NSD combines counterterrorism, counterintelligence, export control, and cyber prosecutors with attorneys who oversee the Department'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 the Department's national security efforts by ensuring greater coordination and unity of purpose between prosecutors, law enforcement agencies, intelligence attorneys, and the IC. The NSD is comprised of the:

- Office of Intelligence (OI);
- Counterterrorism Section (CTS);
- Counterintelligence and Export Control Section (CES);
- Office of Law and Policy (L&P);
- Foreign Investment Review Staff (FIRS);
- Office of Justice for Victims of Overseas Terrorism (OVT)

[1] Within the totals outlined above, NSD has included a total of 17 positions, 17 FTE, and $15,344,000 for Information Technology (IT).

NSD Major Responsibilities

*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 Federal Bureau of Investigation (FBI) to ensure conformity with applicable laws and regulations, FISC orders, and Department procedures, including the foreign intelligence and national security investigation provisions of the Attorney General's Guidelines for Domestic FBI Operations;
- Fulfilling statutory, Congressional, and judicial reporting requirements related to intelligence, counterintelligence, and other national security activities;
- Coordinating and supervising intelligence-related litigation matters, including the evaluation and review of requests to use information collected under FISA in criminal and non-criminal proceedings and to disseminate FISA information; and
- Serving as the Department's primary liaison to the Director of National Intelligence and the IC.

*Counterterrorism*

- Promoting and overseeing a coordinated national counterterrorism enforcement program, through close collaboration with Department leadership, the National Security Branch of the FBI, the IC, and the 94 United States Attorneys' Offices (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 the Department 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 of classified evidence through the application of the Classified Information Procedures Act (CIPA);
- Sharing information with and providing advice to international prosecutors, agents, and investigating magistrates to assist in addressing international threat information and litigation initiatives; and
- Managing DOJ's work on counter-terrorist financing programs, including supporting the process for designating Foreign Terrorist Organizations and Specially Designated Global Terrorists, as well as staffing U.S. Government efforts on the Financial Action Task Force.

*Counterintelligence and Export Control*

- Developing, and supervising the investigation and prosecution of espionage and related cases through coordinated efforts and close collaboration with Department leadership, the FBI, the IC, and the 94 USAOs;
- Coordinating, developing, and supervising investigations and national strategies for combating the emerging and evolving threat of cyber-based espionage and state-sponsored cyber intrusions;
- Coordinating, developing, and supervising investigations and prosecutions into the unlawful export of military and strategic commodities and technology, including by assisting and providing guidance to USAOs in the establishment of Export Control Proliferation Task Forces;
- Coordinating, developing, and supervising cases involving the unauthorized disclosure and improper handling of classified information and supporting resulting prosecutions by providing advice and assistance with the application of 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.

*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 Division/Department leadership;
- Providing legal assistance and advice on matters arising under national security laws and policies, and overseeing the development, coordination, and implementation of Department-wide policies with regard to intelligence, counterintelligence, counterterrorism, and other national security matters;
- Developing a training curriculum for prosecutors and investigators on cutting-edge tactics, substantive law, and relevant policies and procedures; and
- Supporting the Department of Justice's participation in the National Security Council.

*Foreign Investment*

- Performing the Department's staff-level work on the Committee on Foreign Investment in the United States (CFIUS), which reviews foreign acquisitions of domestic entities that might affect national security and makes recommendations to the President on whether such transactions threaten the national security;
- Tracking and monitoring certain transactions that have been approved, including those subject to mitigation agreements, and identifying unreported transactions that might merit CFIUS review;

- Responding to Federal Communication Commission (FCC) requests for the Department's views relating to the national security implications of certain transactions relating to FCC licenses;
- Tracking and monitoring certain transactions that have been approved pursuant to this process; and
- In coordination with law enforcement and IC partners, conducting community outreach and corporate engagement relating to national security issues.

*Victims of Terrorism*

- Ensuring that the rights of victims of overseas terrorism and their families are honored and respected and victims are supported and informed during the criminal justice process.

NSD Recent Accomplishments (unclassified selections only)

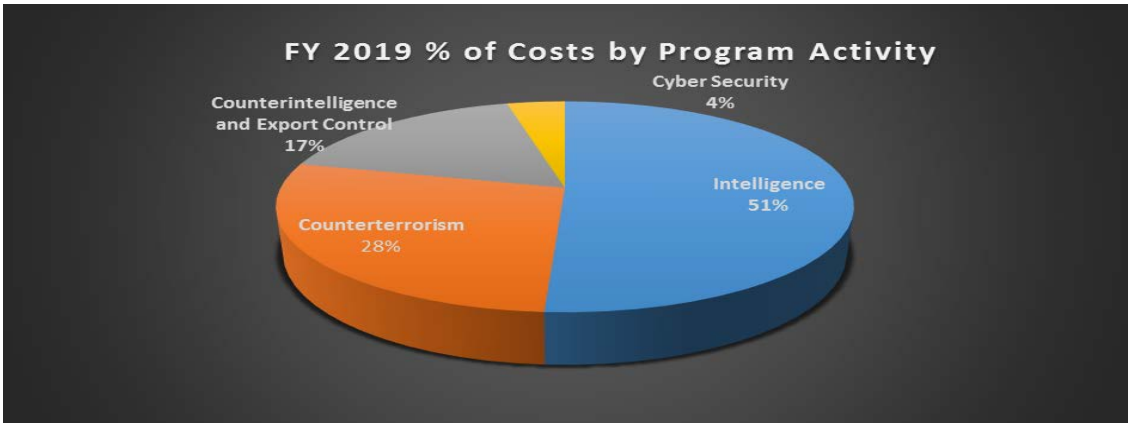
- Responding to the evolving threat of terrorism, since 2013 the Department has charged publicly more than 150 individuals, in more than 35 districts across the country, for foreign fighter, homegrown violent extremist, and ISIS-related conduct. These cases include, among others, aspiring foreign fighters who were arrested before they departed the country, and individuals who were inspired by ISIS to plot violent acts in the United States but were disrupted before they could do so.
- The Division, in partnership with U.S. Attorney's Offices, successfully brought charges in a number of complex national security cyber cases, including the indictment of officers of the Russian Federal Security Service in connection with the 2014 hack into the network of Yahoo – one of the largest data breaches in U.S. history – as well as the indictment of three Chinese nationals for computer hacking and theft of trade secrets from corporate victims in the financial, engineering, and technology industries.
- The Division reached a new high-water mark in 2017 in its efforts to enforce U.S. export control and sanctions laws: as part of a global settlement with the Departments of Justice, Commerce, and Treasury, ZTE agreed to pay a combined total fine and forfeiture amount of over $800 million for illegally shipping U.S.-origin items to Iran, obstructing justice, and making a material false statement. The criminal plea agreement resulted in the largest criminal fine ever imposed in an export control or sanctions case.
- Enforcing sanctions against Iran remains an enforcement priority for the Division, and, since 2016, the Department has charged more than 40 defendants in connection with violations of the Iranian embargo.
- In 2017, the Division received more criminal referrals involving unauthorized disclosures of classified information than it received in the last three years combined. The Department has prioritized and surged resources to resolve these matters. In 2017, the Department more than tripled the number of active investigations of unauthorized disclosures as compared to the number pending at the end of 2016.
- The Division conducted over 30 reviews at Intelligence Community component headquarter locations to assess compliance with acquisition, retention and/or dissemination requirements of Section 702 authorities during calendar year 2017, in addition to its daily activities in furtherance of overseeing implementation of Section 702 authorities. In addition, the Division conducted approximately the same number of reviews at non-headquarters locations during calendar year 2017.

- The Division continues to litigate and obtain favorable rulings upholding FISA authorities as lawful, including five such rulings in 2017.
- The Division managed a 40% jump in critical tasks relating to foreign investment review, including a 230% increase in the number of resulting national security actions. DOJ was responsible for 62% of these national security actions in 2017, an approximate 150% increase from DOJ's participation in such actions in 2016.
- The Office of Justice for Victims of Overseas Terrorism successfully assisted numerous U.S. citizen victims of overseas terrorism in exercising rights available to them in foreign criminal justice systems.

## C. Full Program Costs

The NSD has a single decision unit. Its program activities include intelligence, counterterrorism, counterintelligence and export control, and cyber security. The costs by program activity include the activity's base funding plus an allocation of management, administration, and L&P overhead costs. The overhead cost is allocated based on the percentage of the total cost comprised by each of the program activities.

The charts below represent the percentage of costs by program activity for FY 2019.




## D. Performance Challenges

Protecting the Nation's citizens against acts of terrorism and other threats to our national security through the rule of law is the top priority for the Department, and NSD's work is critical to that mission. As threats continue to grow and evolve, the challenges NSD must overcome also continue to increase and so does the need for additional resources. These challenges include:

1. The changing terrorism threat: The terrorism threat continues to become increasingly diverse and decentralized – as the world has made progress against core al Qaeda, the Islamic State in Iraq and al-Sham (ISIS) has emerged and turned to a more diverse set of tactics, calling on operatives to engage in terrorism attacks wherever the opportunity arises. Thus, NSD and its partners are

increasingly focused on this trend and disrupting smaller, faster-developing plots, rather than larger, longer-term plots like 9/11.

As part of this changing threat environment, there continues to be a rise in homegrown violent extremism, which has resulted in terrorist attacks on U.S. soil inflicting civilian casualties. In addition, there continues to be a number of U.S. persons traveling to Syria to join the ongoing conflict there. These individuals may return to the U.S. trained in the use of improvised explosive devices and other weapons, prepared to conduct attacks. The FBI has conducted investigations of such individuals in all 50 states. The U.S. also faces numerous threats as a result of domestic terrorism, including acts of terrorism by disparate groups that pose special investigative challenges.

The threat of these types of attacks is heightened by radical Islamic extremists aligned with ISIS and other terrorist organizations, such as al-Shabaab, that continue to leverage social media and online engagement to further their recruitment efforts and call for attacks against the homeland. This environment gives rise to the potential for increasing number of homegrown violent extremists (HVEs), who – although they do not necessarily have any direct ties to ISIS, al Qaeda or any other foreign terrorist organization – reside or operate in the U.S. and become inspired by ISIS, al Qaeda or similar groups through social media and English-language propaganda.

The 2017 Worldwide Threat Assessment of the US Intelligence Community notes that the "worldwide threat from terrorism will remain geographically diverse and multifaceted," and, in particular, that "US-based homegrown violent extremists (HVEs) will remain the most frequent and unpredictable Sunni violent extremist threat to the US homeland." The Department must stand ready to disrupt terrorist actors and to respond to attacks that the Intelligence Community assesses "will probably occur with little or no warning." Indeed, since 2013, the Department has charged publicly more than 150 individuals, in more than 35 districts across the country, for foreign fighter, homegrown violent extremist, and ISIS-related conduct.

The terrorism threat is also evolving, requiring NSD to confront novel threats while it continues to disrupt traditional ones. For example, over the past three years, we have seen first-of-their-kind cases in which terrorists are using the Internet and social media as part of conspiracies to steal personal identifying information and disseminate it online, for the purpose of soliciting the murder of or encouraging terrorist attacks against U.S. persons. We expect these kinds of blended threats—converging once-unrelated counterterrorism and cyber cases—to grow in number. Similarly, terrorists and other criminals increasingly use technology, including encryption, to conceal their crimes and hide from 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.

The distributed nature of these types of threats makes investigation of them incredibly complex – as terrorist groups have turned to inspiring individuals across the globe to commit independent and more easily executed acts of terror, identifying and disrupting the threat has become increasingly resource-intensive both in terms of time and personnel. Unlike the small, organized cells that NSD has traditionally seen, the new face of terrorism is everywhere, and the potential population of would-be attackers is not easily knowable.

2. <u>The recent recognition of increasing and changing threats to our national assets, including significant growth of cyber threats to the national security</u>: A top priority for NSD is the protection of national assets through counterintelligence investigations and prosecutions, enforcement of export controls and sanctions, and cyber-related investigations and prosecutions. The theft of trade secrets and other intellectual property by or for the benefit of foreign entities is an increasingly acute and costly threat to U.S. national and economic security. Foreign governments and other non-state adversaries of the United States are also engaged in an aggressive campaign to acquire superior technologies and commodities that are developed in the United States, in contravention of our export control and sanctions laws. The threat our nation confronts increasingly consists not only of unlawful shipments and deliveries of physical commodities and equipment, but also the theft of proprietary information and export-controlled technology through cyber attacks and intrusions in their computer networks, as well as through insider threats. The most sophisticated of our adversaries employ multi-faceted campaigns to acquire valuable proprietary technologies through a combination of traditional and asymmetric approaches. For example, our nation-states adversaries increasingly rely on commercial and other non-state entities to conduct economic espionage, creating a new threat vector that is especially difficult to investigate. Adequately addressing these threats requires a comprehensive, "all-tools" approach that leverages the full array of our options under existing legal authorities. NSD plays a central role in leading these efforts.

   Likewise, NSD's foreign investment review work—including its review of filings before the Committee on Foreign Investment in the United States (CFIUS) and its review of foreign entities' license applications for provision of communications services before the Federal Communications Commission (through the so-called Team Telecom working group)—has also expanded to address the asymmetric threat. With respect to Team Telecom in particular, complex transactions and differences in evaluative priorities among agencies have prompted the Administration's desire to formalize this process with stricter timelines, an administrative chair, and other indicia of a structured interagency process. NSD is prepared to meet the challenge required by these increased responsibilities in effectuating this change.

   Also among the most significant challenges that NSD continues to face is the rapid expansion and evolution of cyber threats to the national security. Representatives from the IC have assessed that the cyber threat may soon surpass that of traditional terrorism, and NSD must be prepared to continue to take lessons learned over the past decade and adapt them to this new threat. Cyber threats, which are highly technical in nature, require time-intensive and complex investigative and prosecutorial work, particularly given their novelty, the difficulties of attribution, challenges presented by electronic evidence, the speed and global span of cyber activity, and the balance between prosecutorial and intelligence-related interests in any given case. To meet this growing threat head on, NSD must continue to equip its personnel with cyber-related skills through additional training while recruiting and hiring individuals with cyber skills who can dedicate themselves full-time to these issues immediately. The window of opportunity for getting ahead of this threat is narrow; closing the gap between our present capabilities and our anticipated needs in the near future will require steadfast commitment.

3. <u>An increasing workload in intelligence oversight, operations, and litigation, especially as relates to the 2015 USA Freedom Act and the reauthorization of Section 702 of the Foreign Intelligence Surveillance Act</u>: NSD's intelligence-related work supports the U.S. Government's national

security mission fully, including combating the threats posed by terrorists, threats to our nation's cybersecurity, and other threats. NSD's Intelligence Operations attorneys work closely with the intelligence community to ensure that they have the legal authorities required to conduct electronic surveillance and physical search of agents of foreign powers, including agents of international terrorist groups, in fast-paced national security investigations. Due to ISIS's prolific use of social media to spread propaganda and recruit followers on-line, NSD has seen an increase in the domestic HVE threat over the last few years, with more U.S. persons being recruited and radicalized on-line. This threat is likely to continue for some time. NSD's oversight work is a critical (and often required) component of NSD's implementation of national security initiatives and authorities, including combating cyber-attacks, terrorism, espionage and the proliferation and use of weapons of mass destruction.

Historical trends in NSD's Oversight work related to the IC's implementation of Section 702, as well as new DOJ obligations under the USA Freedom Act, indicate that the work in this area will grow in the coming years.

As a part of Section 702 oversight, NSD has reviewed an increasing number of (1) National Security Agency (NSA) and FBI targeting decisions and (2) queries concerning a known U.S. person (USP) of unminimized noncontents information obtained under Section 702. While the number of targeting decisions remains classified, the government reported in the 15th Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, "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 from 89,138 in calendar year (CY) 2013 to 106,469 in CY 2016, equating to an increase of approximately 19%. In addition, for multiple agencies involved in Section 702 collection, the estimated number of USP queries increased from 9,500 in CY 2013 to 30,355 in CY 2016, which was an increase of over 200%.

The passage of the USA Freedom Act in June 2015 resulted in many significant amendments to FISA. NSD is playing a leading role in fulfilling the Act's requirements, including new oversight and amicus provisions. With respect to transparency, the Act requires the declassification (or, where that is not possible, declassified summaries) of opinions by the Foreign Intelligence Surveillance Court (FISC) and Foreign Intelligence Surveillance Court of Review that involve significant or novel issues. It also increases the government's public reporting obligations regarding specific uses of FISA authorities. The Act further requires that the FISC generally appoint an amicus curiae in FISA cases involving significant or novel issues—a requirement that we expect to result in additional legal briefings.

NSD expects to see continued growth in the area of use and litigation relating to Section 702 information. There have been several high-profile litigation matters during the past year, including some involving individuals indicted for terrorism-related charges. The government has successfully litigated issues relating to Section 702 information in both federal district and appellate courts, and NSD expects continued growth in these challenges and the need to dedicate significant attention to these matters to ensure successful outcomes.

4. Difficulties inherent in supporting the continued development of the Division in an ever-changing environment: NSD is building case management and document management systems that will

allow NSD employees to efficiently and effectively carry out their mission. Requirements for these systems are complicated given the evolving nature of the work NSD performs and the ever-changing threats to the nation's security that NSD works daily to address. Similarly, NSD possesses a significant amount of classified and sensitive information, information technology systems and procedures must protect this information and guard against the threats posed by insiders who misuse information or improperly disclose it without authorization. This creates unique challenges both in terms of information technology infrastructure and support, as well as document management.

Because of the nature of its work and the critical role it plays in protecting the nation against terrorism and threats to national security, NSD also faces particular challenges relating to emergency preparedness. The vast majority of NSD's work relates to classified material, and more than 80% of its workforce is housed in sensitive compartmented information facilities. NSD provides operational and policy support to the intelligence community, law enforcement, the Department, and other government agencies in the event of a local or national emergency. Continuity of operations and continuity of government plans, therefore, must account for the circumstances in which NSD must be able to operate.

5. Challenges associated with victims outreach: NSD also maintains the Office of Justice for Victims of Overseas Terrorism (OVT) to assist U.S. citizen victims when the terrorist attack and criminal proceedings occur overseas. OVT faces challenges in obtaining foreign litigation information, which includes security challenges; lack of political will by the foreign government; unpredictable foreign justice mechanisms; sovereignty concerns of the foreign government; and bureaucratic issues within the United States Government.

   This caseload is defined as cases involving U.S. citizens that are in a foreign litigation process, and this caseload number is fluid as cases are resolved. This type of monitoring and advocacy requires additional time and effort on behalf of staff. U.S. citizens who are injured by terrorists abroad deserve the best advocacy and information services that can be provided. It is the goal of OVT to do exactly that, and resources and access to this information are necessary for OVT to fully achieve its mission.

## E. Environmental Accountability

NSD continues to be committed to environmental wellness and, to that end, is involved in a variety of programs and activities that promote environmental responsibility. Examples include:

- Developing and implementing automated systems in an effort to become as paperless as possible. This effort has also significantly decreased daily toner and paper usage as well as other various costs associated with printers and copier machines.
- Administering a comprehensive recycling program. NSD distributes individual recycling containers to each employee and contractor and provides larger recycling containers in common areas such as breakrooms. The Division also recycles all toner cartridges.
- Participating in DOJ environmental initiatives, including the Transit Subsidy and Bicycle Commuter Fringe Benefits programs.

## II. Summary of Program Changes

No program changes

# 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, $101,369,000, 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 505 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 substantive changes proposed.

# IV. Program Activity Justification

**National Security Division**

| *National Security Division* | Direct Pos. | Estimate FTE | Amount |
|---|---|---|---|
| 2017 Enacted | 362 | 370 | $96,000,000 |
| 2018 Continuing Resolution | 362 | 362 | $95,348,000 |
| Adjustments to Base and Technical Adjustments | 0 | 0 | $6,021,000 |
| 2019 Current Services | 362 | 362 | $101,369,000 |
| 2019 Program Increases | 0 | 0 | $0 |
| 2019 Request | 362 | 362 | $101,369,000 |
| **Total Change 2018-2019** | **0** | **0** | **$6,021,000** |

| *National Security Division*-Information Technology Breakout | Direct Pos. | Estimate FTE | Amount |
|---|---|---|---|
| 2017 Enacted | 18 | 18 | $16,583,000 |
| 2018 Continuing Resolution | 17 | 17 | $16,545,000 |
| Adjustments to Base and Technical Adjustments | 0 | 0 | -$1,201,000 |
| 2019 Current Services | 17 | 17 | $15,344,000 |
| 2019 Program Increases | 0 | 0 | $0 |
| 2019 Program Offsets | 0 | 0 | $0 |
| 2019 Request | 17 | 17 | $15,344,000 |
| **Total Change 2018-2019** | 0 | 0 | -$1,201,000 |

## 1. Program Description

The National Security Division (NSD) is responsible for:

- Overseeing terrorism investigations and prosecutions;
- Protecting critical national assets from national security threats, including through handling counterespionage, counterproliferation, and national security cyber cases and matters, as well as through investigations and prosecutions relating to the unauthorized disclosure and improper handling of classified information;
- Serving as the Department's liaison to the Director of National Intelligence;
- Administering the U.S. Government's national security program for conducting electronic surveillance and physical search of foreign powers and agents of foreign powers pursuant to FISA;
- Conducting oversight of certain activities of the IC components and the FBI's foreign intelligence and counterintelligence investigations pursuant to the Attorney General's guidelines for such investigations; and
- Assisting the Attorney General and other senior Department and Executive Branch officials in ensuring that the national security-related activities of the U.S. are consistent with relevant law.

In coordination with the FBI, the IC, and the USAOs, NSD's primary operational function is to prevent, deter, and disrupt terrorist and other acts that threaten the U.S., including counterintelligence threats and cyber threats to the national security  The NSD also serves as the Department's liaison to the Director of National Intelligence, advises the Attorney General on all matters relating to the national security activities of the U.S., and develops strategies for emerging national security threats – including cyber threats to the national security.

NSD administers the U.S. Government's national security program for conducting electronic surveillance and physical search of foreign powers and agents of foreign powers pursuant to FISA, and conducts oversight of certain activities of the IC components and the FBI's foreign intelligence and counterintelligence investigations pursuant to the Attorney General's guidelines for such investigations. NSD prepares and files all applications for electronic surveillance and physical search under FISA, represents the government before the FISC, and – when evidence obtained or derived under FISA is proposed to be used in a criminal proceeding –obtains the necessary authorization for the Attorney General to take appropriate actions to safeguard national security.  NSD also works closely with the Congressional Intelligence and Judiciary Committees to ensure they are apprised of Departmental views on national security and intelligence policy and are appropriately informed regarding operational intelligence and counterintelligence issues.

In addition, 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 National Security Council-led policy committees and the Deputies' Committee processes, and represents the DOJ on a variety of interagency committees such as the Director of National Intelligence's FISA Working Group and 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, the FBI, and the Defense and State Departments concerning questions of law, regulations, and guidelines as well as the legality of domestic and overseas intelligence operations.

NSD also serves as the staff-level DOJ representative on the 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 resulting from transactions, and ultimately the national security risks, if any, of allowing a transaction to proceed as proposed or subject to conditions.  In addition, NSD tracks and monitors transactions that have been approved subject to mitigation agreements and seeks to identify unreported transactions that may require CFIUS review.  On behalf of the Department, NSD also responds 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 transaction.

Finally, NSD, through its OVT, ensures that  American citizens overseas who are victims of terrorist attacks receive the services and support they need as they navigate foreign judicial systems.  Among other things, OVT is responsible for monitoring the investigation and prosecution of terrorist attacks against Americans abroad, working with other Justice Department components to ensure that the rights of victims

of such attacks are honored and respected, establishing a Joint Task Force with the Department of State to be activated in the event of a terrorist incident against American citizens overseas, responding to Congressional and citizen inquires on the Department's response to such attacks, compiling pertinent data and statistics, and filing any necessary reports with Congress.

## 2. Performance Tables

Performance materials will be provided at a later date.

## 3. Performance, Resources, and Strategies

Performance materials will be provided at a later date.

## V. Program Increases by Item

The FY 2019 requested budget does not request program increases.

## VI. Program Offsets by Item

The FY 2019 requested budget does not request program offsets.

# VII. Exhibits