Department of Justice National Security Division Priorities 2021-2025

The Justice Department has no higher priority than keeping the American people safe. The National Security Division leads the Justice Department's mission to protect the United States from threats to our national security by pursuing justice through law.

Today, our nation faces a wide range of complex and evolving threats – including international and domestic terrorism, nation-state sponsored lethal targeting of American civilians and officials, transnational repression of dissidents, foreign malign influence, national security cyber threats, and the illicit procurement of sensitive American data and technology. Working closely with U.S. Attorneys' Offices and our law enforcement and intelligence community partners, the National Security Division is committed to deploying all available tools to arrest, prosecute, and otherwise disrupt adversaries and threat actors around the world.

I. Counterterrorism

The National Security Division leads the Department's efforts to combat all forms of terrorism. NSD's counterterrorism strategy has evolved to address the array of threats facing the country – from foreign terrorist organizations (FTOs) plotting from abroad and at home, to FTO-inspired homegrown violent extremists plotting within the homeland, to domestic violent extremists inside the United States, including those motivated by racial animus and anti-government ideologies. Working in partnership with U.S. Attorney's Offices, NSD executes its well-established playbook to investigate, disrupt, deter, and prosecute terrorism crimes.

International Terrorism. NSD has led the Department's counterterrorism strategy by implementing a whole-of-government approach based upon strong partnerships with the law enforcement and intelligence communities and close coordination with federal, state, local, and foreign partners. Together, NSD and our partners use all available legal tools to disrupt and prevent terrorist attacks and to hold accountable those who engage in terrorist activity.

In cases exemplifying NSD's counterterrorism strategy, the Department has:

- Thwarted an ISIS-inspired plot to conduct a terrorist attack in the U.S. on Election Day.
- Charged Hamas senior leadership with terrorism crimes and murder conspiracy for the October 7, 2023, terrorist attacks on Israel and the kidnapping and killing of scores of innocent civilians, including Americans.
- Prosecuted the highest-ranking ISIS fighter to ever face jury trial in the United States for his participation in a brutal hostage-taking scheme that resulted in the deaths of four Americans, as well as the deaths of British and Japanese nationals, in Syria.

- Obtained U.S. custody of a Libyan intelligence operative charged for his involvement in the 1988 Lockerbie bombing of a civilian aircraft that killed 270 people, including 190 Americans.

Domestic Terrorism. The National Security Division has strengthened and expanded the Department's capacity to respond to heightened threats from domestic violent extremists and domestic terrorists.

- Established a new Domestic Terrorism Unit within the NSD's Counterterrorism Section to better coordinate with U.S. Attorney's Offices, the FBI, and other partners to prosecute domestic violent extremism and terrorism offenders. Since its inception, the DT Unit has assisted with hundreds of domestic terrorism matters.

- Adopted new Justice Manual requirements to ensure effective coordination and a consistent approach to matters with a domestic terrorism nexus throughout the country.

- Worked closely with the Civil Rights Division to enhance coordination and ensure all appropriate criminal charges are brought to bear against domestic extremist violence, given the frequent overlap between domestic terrorism and hate crimes incidents.

- Increased the partnerships and coordination with other DOJ components, including through the Domestic Terrorism Executive Committee, to ensure the Department has an effective and consistent approach to combatting domestic terrorism-related threats.

II. Preserving Intelligence Authorities: FISA Section 702

The National Security Division is responsible for helping to ensure that the intelligence community has the legal authorities necessary to fulfill its national security mission and that the government exercises those authorities in a manner that safeguards civil liberties and upholds the trust of the American people. The public's trust and confidence are essential to the operation and legitimacy of U.S. national security programs.

NSD was at the forefront of the government's efforts to ensure reauthorization of Section 702 of the Foreign Intelligence Surveillance Act (FISA), leading other DOJ components and working with interagency partners to secure the passage of the Reforming Intelligence and Securing America Act. Section 702 has proven to be indispensable to protect the American people from terrorist, nation-state, cyber, and other threats.

By securing 702 reauthorization in April 2024, the government preserved the authority to continue to collect vital foreign intelligence information about non-U.S. persons located outside the United States, while codifying important reforms the Justice Department has adopted to ensure the protection of Americans' privacy and civil liberties.

III. Sanctions and Export Control Enforcement

The national security of the United States is inextricably linked to the strength, security, and resilience of the U.S. economy. Our adversaries seek to undermine our economic and national security by stealing or illicitly obtaining cutting-edge technology and intellectual property to gain competitive advantages in areas of transformative technologies, spanning from artificial intelligence to semiconductors to quantum computing.

The National Security Division has prioritized the effort to leverage intergovernmental resources and international law enforcement partners to target illicit actors, protect supply chains, and prevent critical technology falling into dangerous hands. In addition, NSD has bolstered sanctions enforcement efforts to expose criminal actors seeking to evade national security restrictions and unlawfully do business in the United States. The Department is committed to imposing accountability for both the sanctioned entities and their U.S.-based facilitators.

NSD has enhanced its capacity to enforce sanctions and export controls, including by adding more than 25 prosecutors dedicated to investigating and prosecuting sanctions evasion, export control violations, and other economic crimes.

- Launched and led the Disruptive Technology Strike Force (DTSF), together with the Commerce Department, to bring together experts across the government to stop hostile nation-states trying to illicitly acquire and abuse sensitive U.S. technology.
    - The DTSF has brought numerous complex, high-impact cases charging more than 30 individuals and corporate entities with export control violations and other crimes related to the unlawful transfer of technology to Russia, China or Iran, and other adversaries. And it has worked with foreign partners, including to issue denial orders against dozens of businesses facilitating such illicit acquisitions.
- Reaffirmed the Department's support of Ukraine and its commitment to curbing the illegal flow of advanced technology to Russia through delegation visit to Kyiv, Ukraine.
- Co-led Task Force KleptoCapture, an interagency law enforcement task force announced by the Attorney General in 2022 to impose costs and accountability for Russia's unprovoked invasion of Ukraine. The Task Force has seized or obtained forfeiture judgments against hundreds of millions of dollars belonging to Russian oligarchs and enablers of the Putin regime and charged and arrested dozens of defendants worldwide.

IV. The Intersection of Corporate Enforcement and National Security

In today's complex and uncertain geopolitical environment, corporate crime and national security intersect to an unprecedented degree. The Department's increased focus on corporate investigations reflects the reality that corporations are on the front lines when it comes to critical

national security tools designed to deter Russia, Iran, China, and other adversaries from stealing sensitive American technology and data.

The Department's enforcement tools cut off Iran's access to the financial markets and technologies it needs to support its weapons systems and aggression. They prevent China from stealing cutting-edge technology that enables their military advances and human rights abuses. They block North Korea from funding its nuclear ambitions. And DOJ enforcement efforts impose costs on Russia for its invasion of Ukraine.

For NSD, finding and prosecuting corporate and individual wrongdoers is a core responsibility, but this work extends beyond criminal investigations. The Department has adopted policies to drive corporate responsibility – encouraging companies to prevent the evasion of sanctions and export controls in the first place and incentivizing business entities to build strong compliance programs to prevent, detect, and report violations.

- Invested in NSD sanctions and export control corporate enforcement, including increasing the number of prosecutors working on these cases and naming the National Security Division's first-ever Chief Counsel for Corporate Enforcement.

- Issued the first NSD Enforcement Policy for Business Organizations, designed to address national security-related white-collar crime and associated considerations.

- Secured groundbreaking convictions and dispositions in significant national security-related corporate enforcement matters, working in partnership with U.S. Attorney's Offices, including the first-ever prosecution and conviction of a company for providing material support to a terrorist organization (ISIS), and the first corporate declination – which was accompanied by charges against individual employees – under the NSD Corporate Enforcement Policy, as a result of the company's voluntarily self-disclosure, cooperation, and remediation.

- Obtained a guilty plea from the subsidiary of a British tobacco company for violating sanctions against North Korea along with a $629 million penalty – the largest ever criminal penalty for a violation of sanctions on North Korea.

- Secured a guilty plea by Binance, the world's largest cryptocurrency exchange, for violating Iranian sanctions. That case, brought in partnership with the Criminal Division, involved a $4.3 billion financial penalty – one of the largest criminal penalties in history – as well as a guilty plea by the company's founder and former CEO.

V. Transnational Repression and Lethal Targeting

NSD has prioritized the work, in partnership with the FBI and U.S. Attorneys' Offices, to combat the actions of adversary nation-states to harm, intimidate, and threaten people inside the

United States. Authoritarian governments increasingly have turned to violence, threats of violence, and repressive tactics to target government officials, as well as perceived critics of their regimes. The Department launched the Strategy for Countering Nation-State Threats, in part, in response to this alarming rise in illegal activity from hostile nations, including their efforts to punish dissidents, target perceived critics, and undermine the rule of law.

In the past few years, the Department and its law enforcement partners successfully disrupted foreign-directed schemes ranging from surveillance and harassment to kidnapping and attempted assassinations.

- Secured the arrests and successful prosecutions of, among other threat actors, an array of PRC-affiliated subjects carrying out the repressive tactics of the Chinese government in violation of U.S. laws.

- Detected and disrupted multiple dangerous Iranian plots to target individuals inside the United States, including lethal targeting of current and former U.S. government officials:

    - Charges unsealed in August of 2022 in connection with Iran's effort to assassinate the former National Security Advisor John Bolton.

    - Charges unsealed in January 2024 against three defendants – including an Iranian national living in Iran – for a plot to carry out a contract killing of two individuals, including an Iranian defector.

    - Charges brought in September 2024 against a Pakistani national with ties to Iran in connection with a foiled plot to assassinate a politician or U.S. government official on U.S. soil.

    - Charges unsealed in September 2024 against an IRGC-asset in Iran, who allegedly plotted with other defendants to murder a prominent critic of the Iranian regime and who had been tasked by the Iranian regime to plot the assassination of President Trump.

- Detected and disrupted the Iranian government's lethal targeting of current and former U.S. Government officials as retribution for the 2020 death of former Iranian Revolutionary Guard Corps leader Qassem Soleimani. Brought multiple prosecutions against Iranian officials and assets for their roles in orchestrating such plots.

- Pursued charges related to an India-linked assassination plot in the United States, charging an Indian government employee in connection with his role in directing a foiled plot to assassinate a U.S. citizen and activist in New York.

VI. Foreign Malign Influence and Election Security

NSD leads the Department's efforts to counter foreign malign and covert influence and to protect the integrity of our democratic process from the actions of foreign adversaries. Our laws demand that U.S. citizens are informed of the foreign nature of political messages when they originate from foreign sources. That transparency empowers citizens to evaluate information and make informed decisions for themselves, as the American people decide how to exercise their fundamental right to vote in free and fair elections.

Our adversaries seek to covertly influence our elections and undermine our democracy. Authoritarian regimes – including Russia, Iran and China – are determined to impact the views of the electorate in ways that they believe will serve their own interests and weaken the United States by sowing discord and undermining confidence in our democratic institutions.

In taking on this threat, the Justice Department has demonstrated its commitment to defend the integrity of our democratic institutions and public discourse against those who would seek to illegally exert influence, no matter the country and regardless of viewpoint.

- Charged two employees of a Russian state-controlled media outlet, RT, in a $10 million scheme to create and distribute content to U.S. audiences with hidden Russian government messaging and propaganda.
- Seized 32 internet domains used in Russian government-directed foreign malign influence campaigns, colloquially referred to as "Doppelganger," which operated at the direction of the Russian Presidential Administration to covertly spread Russian government propaganda to reduce international support for Ukraine, bolster pro-Russian interests, and influence voters in U.S. and foreign elections.
- Indicted members of the Islamic Revolutionary Guard Corps (IRGC) with a conspiracy to hack into accounts of current and former U.S. officials, members of the media, and individuals associated with U.S. political campaigns as part of Iran's efforts to stoke discord, erode confidence in the U.S. electoral process, and unlawfully acquire information relating to current and former U.S. officials.
- Issued a new rule updating, clarifying, and modernizing key regulations establishing the scope of liability and exemptions under the Foreign Agents Registration Act, amending those regulations for the first time in more than a decade.

VII. Countering Espionage

The Department, through NSD's Counterintelligence and Export Control Section, has continued to prioritize the investigation and prosecution of traditional espionage cases. Nation-state actors, particularly China, have demonstrated that they remain committed to illegally

obtaining sensitive and classified U.S. government information to benefit their interests and to harm the United States.

In partnership with investigators in the FBI's Counterintelligence Division, prosecutors in CES prosecutors and in U.S. Attorneys' Offices have worked aggressively to hold spies and leakers accountable and to deter future espionage activity. This includes charging active-duty members of the U.S. Navy for sharing sensitive military information with China; charging a U.S. government contractor with espionage related offenses; securing a guilty plea from a U.S. Air National Guardsman who publicly disclosed classified information; and convicting a former U.S. Ambassador and NSC official for secretly acting as an agent of Cuba for decades.

VIII. Foreign Investment Review and Data Protection

Over the past several years, the Department has increasingly focused on countering the risks that foreign investment in the United States may pose to our national security. NSD's Foreign Investment Review Section is at the forefront of the effort to proactively prevent China, Russia, Iran, and other foreign adversaries from exploiting American technology, business, data, and communications.

FIRS reviews and regulates commercial activities – including through DOJ's role in the Committee on Foreign Investment in the United States (CFIUS) – to address national security risks and to monitor and enforce compliance obligations.

- Prioritized the Department's participation on CFIUS, the Treasury Department-chaired interagency body that reviews certain transactions involving foreign investment in the United States to assess potential national security risks.
    - The National Security Division secured the resolution of an enforcement action involving the first-ever public naming of the transaction party and the imposition of the largest monetary penalty in CFIUS history.
- Protected Americans' sensitive and personal data from Russia, Iran, China, and other adversaries by creating a new comprehensive national security regulatory program in coordination with interagency partners, to be implemented by FIRS.

IX. National Security Cyber Threats

Against a rapidly evolving landscape of sophisticated cyber threats, the Department has deployed a strategy of proactive disruptions and dedicated prosecutorial resources to increase the U.S. government's capacity to protect national security and advance cybersecurity.

In 2023, the Department created the new National Security Cyber Section in NSD to lead, along with its partners in U.S. Attorney's Offices and the FBI, our comprehensive efforts to

investigate, disrupt, and deter nation-state threat actors, state-sponsored cybercriminals, and other cyber-enabled threats to national security.

NatSec Cyber has significantly increased the number, scale, and speed of DOJ's campaigns to disrupt the cyber crimes of nation-state threat actors and their proxies – carrying out numerous significant public actions to counter cyber and cyber-enabled threats to national security.

- Identified PRC Hackers' Infiltration of U.S. Telecommunications Networks and launched the investigation of "Salt Typhoon."
- Exposed an Iranian "hack-and-leak" operation targeting President Trump's campaign by the Islamic Revolutionary Guard Corps.
- Executed a court-authorized takedown of a global network of computers compromised by the sophisticated "Snake" malware used by the Russian FBS to conduct espionage against the US and NATO allies for almost two decades
- Carried out court-authorized proactive disruption operations using innovative legal process, including disrupting:
    - spear-phishing efforts by Russian intelligence;
    - a worldwide botnet used by PRC state-sponsored hackers;
    - a Russian government-operated, artificial intelligence-enhanced social media bot farm spreading disinformation in the United States and abroad;
    - a North Korea IT workers scheme to generate illicit revenue for the DPRK;
    - a Russian GRU botnet used as intelligence gathering platform to target the U.S., Ukraine, and other allies; and
    - a PRC botnet used to conceal hacking of critical infrastructure.