STATEMENT FOR THE RECORD

Ken Wainstein
Under Secretary
Office of Intelligence and Analysis
U.S. Department of Homeland Security

BEFORE THE

U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Intelligence and Counterterrorism

AT A HEARING ENTITLED

"Examining the Operations of the Office of Intelligence and Analysis"

December 13, 2022

Chairwoman Slotkin, Ranking Member Pfluger, and members of the Subcommittee, thank you for the opportunity discuss the current activities of the Office of Intelligence and Analysis (I&A) of the Department of Homeland Security (DHS). It is an honor to be here representing I&A's dedicated and high-caliber intelligence professionals who work tirelessly to further the security of our Nation.

Today, I will provide the Committee with an overview of I&A and its operations. In crafting this overview, I have erred on the side of being comprehensive and detailed, as I know that the Committee Members are intensely interested in the organizational effectiveness and well-being of every part of I&A. This overview will focus on describing I&A's mission, detailing certain aspects of the management and oversight we are putting in place, and assessing the current threat that my I&A colleagues are confronting.

I. THE MISSION

Last month marked the 20th anniversary of the Homeland Security Act of 2002, which brought together many components of the federal government in a determined national effort to safeguard the United States against terrorism in the wake of the devastation on September 11, 2001. The creation of DHS was the largest reorganization of the federal government's national security establishment since 1947 and is a testament to the grave threat we face as a Nation from terrorism.

The Homeland Security Act provides many of the core authorities that guide I&A's intelligence activities. Acknowledging the need to enhance information sharing and provide timely, actionable intelligence to a far-reaching base of customers and partners, Congress tasked I&A to collect, analyze, and disseminate intelligence with state, local, tribal, and territorial (SLTT) governments, the private sector, the Intelligence Community, critical infrastructure owners and operators, and other DHS components to ensure that these entities are all aware of the most pressing threats to the Nation.

The Intelligence Cycle

Over the past 20 years, I&A has developed its capacity to carry out every stage of the intelligence cycle – the establishment of requirements, the collection of information, the analysis and reporting of that information, and its dissemination to our partners. I&A plans and directs its intelligence activities, performing collection, analysis, dissemination, and feedback functions, to holistically implement the full intelligence cycle.

Establishment of Intelligence Requirements. I&A oversees the formulation of the requirements that guide our intelligence collection and production efforts. Each year, I&A represents DHS in the ODNI's National Intelligence Priorities Framework process by which the President articulates the intelligence targets and topics that should be prioritized by the federal Intelligence Community elements. During that process, we advocate for the Department's intelligence interests in the ranking of priorities across the federal government.

As the Chief Intelligence Officer of the Department, I also oversee the intelligence prioritization process within DHS – called "Threat Banding" – by which we prioritize the homeland security threats within our departmental responsibility. The Department's intelligence efforts are prioritized and carried out in accordance with that ranking.

Collection. I&A then carries out collection activities in furtherance of the established requirements and in support of National and Departmental missions. It is authorized to do so through overt means and by collecting publicly available information.

A focus of our collection efforts has been on enhancing I&A's Open Source Collection Operations Office, where we have realigned our open source collection officers to threat-specific accounts, which has enhanced our ability to identify and disseminate actionable intelligence. As a recent example, our collectors were one of the first in the Intelligence Community to locate the manifesto of the shooter responsible for the domestic violent extremist attack in Buffalo, New York, providing it within minutes of the attack to stakeholders including the FBI and SLTT partners. In the coming year, we plan to make additional investments in the capabilities of our open source collection program consistent with DHS policy and legal authorities that protect privacy, civil rights, and civil liberties. We are also engaging with fusion centers and the intelligence community to share best practices for open source collection and analysis.

Intelligence Production. I&A conducts analysis and issues products on the full range of threats that are currently facing the homeland. I&A's analyst cadre is organized in mission centers – e.g., the Transnational Organized Crime Mission Center and the Cyber Mission Center – allowing analysts to develop specific subject-matter expertise and to develop the network of contacts within the agencies that operate within their mission space.

Since 2020, I&A has recommitted to improving the quality and timeliness of its analysis to provide decision advantage to homeland security stakeholders in responding to threats. As part of these efforts, I&A has centralized its planning, review, and dissemination of finished intelligence production under its Research Director – a senior, analytic subject matter expert who recently came to I&A from the Defense Intelligence Agency. The Research Director has focused on establishing effective processes and procedures for producing analysis and instituting multi-layered review of finished intelligence products and improving training tailored to analytic expertise.

These efforts have resulted in greater utility of I&A's analysis by homeland security customers and positive feedback on its timeliness and relevance to protecting the Homeland. In FY 2022, I&A received significant positive feedback on its finished intelligence products.[1]

Dissemination. I&A has one of the broadest customer sets within the Intelligence Community – from the President and cabinet-level officials like Secretary Mayorkas to state government leaders, local law enforcement, critical infrastructure owners and operators, and even the public. In fiscal year 2022 (FY 2022), more than 60 percent of I&A's finished

[1] This feedback indicated that 86% of the respondents were very satisfied or satisfied with the timeliness, and 89% were very satisfied or satisfied with the relevance of the products.

intelligence products were produced at the unclassified level to ensure the widest dissemination with those who have a need to know. At the same time, I&A's production – including regular products in the President's Daily Brief last year -- helped inform the Intelligence Community and policymakers on the unique threats the Nation faces internally and at its borders.

With such a broad customer set, I&A has worked to modernize our methods for delivering intelligence to our full range of customers. In 2020, I&A stood up a team to manage the delivery of intelligence to customers within DHS. This team curates a daily read book with DHS and Intelligence Community products that have a Homeland nexus and provides a daily classified briefing to all I&A personnel deployed across the country, including those assigned to the 80 state and major urban area fusion centers. Each month, that team also provides a secret-level threat briefing to our SLTT customers.

The primary mechanism for dissemination of unclassified products is the Homeland Security Intelligence Network, which provides on-line access to over 50,000 unclassified intelligence products for our SLTT partners. To facilitate more convenient access to these products, this year I&A rolled out its HSIN-Intel mobile application that allows HSIN members to access those products on their smartphones.

As another effort to facilitate SLTT access to our intelligence products, we are currently piloting a project that distributes laptops to cleared SLTT partners that will allow them access to SECRET-level products without having to travel to one of the few locations scattered around the country with a SECRET, Homeland Security Data Network or to a Sensitive Compartmented Information Facility.

The above efforts are going a long way to expand access to DHS and Intelligence Community products and enhance coordination with our state, local, tribal, territorial, and private sector partners against the threats to our homeland security.

Intelligence Partnerships

As Secretary Mayorkas often says, DHS is fundamentally a Department of partnerships. This is at the core of why Congress established I&A and why the I&A workforce is dedicated to building close and lasting coordination with all levels of government and the private sector, including critical infrastructure owners and operators, academia, faith communities, and non-profit organizations. We are taking numerous steps to further energize that coordination.

First, we recently established a Deputy Under Secretary for Intelligence Partnerships to elevate I&A's partner engagement efforts. This new position and structure elevate our engagement, liaison, and outreach efforts under a single position, ensuring our senior leadership maintains close connectivity with our partners, and providing those partners with a single senior-level touch point within I&A.

Second, we are hosting national, bi-weekly meetings with our SLTT and private sector partners to discuss the threat environment. These meetings allow I&A to routinely share relevant threat information and discuss emerging threats at both the local and national levels, while also

providing an opportunity for I&A to hear and incorporate our partners' perspectives into our analysis.

Third, we hosted a national Intelligence Summit in August 2022 in partnership with the International Association of Chiefs of Police, which convened over a hundred partners from agencies and associations at all levels of government. The summit started with the premise that the information-sharing architecture that was largely built after and in response to the 9/11 attacks had failed to evolve with the emerging threats of the past 20 years and that we need to re-energize the process and urgency of building and maintaining information-sharing processes among all levels of government. Over two days of issue-specific workshops, the summit participants came up with – and mutually committed to – a slate of initiatives to guide our information-sharing efforts in the future. As a follow-up to the Summit, Secretary Mayorkas asked the Homeland Security Advisory Council (HSAC) to further evaluate and make recommendations for reform of the current practices and processes for sharing information and intelligence with our federal, SLTT and private sector partners, and we are supporting the HSAC as it develops its recommendations.

The DHS Intelligence Enterprise

In my role as CINT, I&A is working closely with our DHS components through the Homeland Security Intelligence Council (HSIC) to coordinate the development of intelligence processes and intelligence oversight across the Department. In March of 2022, Secretary Mayorkas directed that I&A lead the effort to expand and apply uniform standards and consistent oversight to all intelligence products across the Homeland Security Intelligence Enterprise (IE), providing unity and standardization to the Department's intelligence operations writ large. As an important part of that effort, DHS's Office for Civil Rights and Civil Liberties, Privacy Office, and Office of the General Counsel are engaging directly with DHS components to help them apply intelligence oversight principles to all DHS finished intelligence.

II. LEADERSHIP AND ORGANIZATIONAL MANAGEMENT

A leader's first priority is to support that leader's personnel. As such, supporting the I&A team is my top priority, and much of my focus during my first six months has been on the workforce.

Morale and Organizational Health

I am proud of the progress that has been made recently – both before and after my arrival – in bolstering morale and organizational health, and I am confident that our efforts will continue to yield dividends in morale and productivity.

Those efforts have included the following initiatives. First has been a focus on enhancing our diversity initiatives and representation. We live in a diverse world that requires a diverse intelligence workforce, and as such, we consider diversity a core value. In September 2020, I&A appointed a Chief Diversity, Equity, and Inclusion Officer to drive diversity and equity initiatives. I&A also established a Diversity and Inclusion Council and issued its first Inclusive

Diversity Strategic Plan for Fiscal Years 2022-2026, which is designed to spark new and creative efforts to enhance diversity, equity, inclusivity, morale, and productivity across I&A.

Second, following lessons learned during the COVID-19 pandemic, we have re-envisioned our telework program and flexible scheduling. We are finding that an appropriate level of flexibility is helping us attract and retain talented personnel.

Third, we recently implemented an advanced analytic employee feedback survey, which can be used to examine the functioning of an individual I&A center or division, diving deep into the leadership and work environment of teams and individuals. This tool has already provided actionable insight into several areas for improvement, contributing to I&A's adjustments in work unit dynamics, leadership training, and work flexibility opportunities.

Fourth, I&A implemented a multi-faceted communication strategy leveraging multiple mediums to share information and gather feedback, including – office-wide brown bags, employment of an organizational ombudsman, monthly newsletters, and virtual forums focused on employee concerns and feedback – to ensure our employees are fully engaged and informed about important workforce matters.

Finally, we have instituted several new initiatives designed to bolster employee enthusiasm and morale. These include a new speaker series, which featured conversations with recognized high-ranking national security and intelligence experts, including former CIA Director John Brennan, former Director of National Intelligence (DNI) James Clapper, and Principal Deputy Director of National Intelligence (PDDNI) Dr. Stacey Dixon.

In October 2022, we also held the first I&A Family Day in almost 10 years. Modeled after the Central Intelligence Agency's family day, this was a special celebration of I&A families and the support they give to us and our careers. We had over 300 family members participate in the event, many of whom traveled to D.C. to learn about the important work their loved ones do to protect the country. Thanks to the generosity of our partners, they were able to see a number of special capabilities from the operational missions we support, including a CBP helicopter, a Secret Service drone demonstration, the Secret Service presidential limousine known as "The Beast," and U.S. Park Police horses.

Training Enhancements

I know from my engagement with Committee Members that this Committee has placed a special focus on ensuring that I&A's training meets the high standards of both the Intelligence Community and the Department. I appreciate and share that focus. Following the reviews of I&A's activities in Portland during the summer of 2020 and leading up to the attack on the Capitol on January 6, 2021, I&A has significantly enhanced the quality and comprehensiveness of its training. I&A's training is an essential part of our workforce development and is key to ensuring that all activities are conducted in accordance with the law and the Constitution, and in a manner that appropriately protects individuals' privacy, civil rights, and civil liberties.

In partnership with the Office of the General Counsel, I&A developed a series of refresher oversight training sessions which cover I&A's authorities, the legal interpretation of the Intelligence Oversight Guidelines, whistleblower protections, and some of the discrete Constitutional and statutory considerations that were encountered by I&A collectors working on the Portland situation during the summer of 2020. This year, we also created a new mandatory training program for all new open source collection officers, which includes education about the types of information I&A can and cannot collect and the procedures for disseminating this information to appropriate stakeholders. Finally, I&A is providing training webinars on the conceptualization of finished intelligence products and I&A's Analytic Tradecraft Evaluation program to reinforce ODNI tradecraft standards.

In addition to training its own staff, I&A has expanded training opportunities for intelligence personnel in other DHS components and among our SLTT partners. In FY 2021, I&A adopted a blended learning delivery model to reach students from across DHS and our SLTT partners through a combination of virtual and classroom instructor-led classes, resulting in over 3,000 graduates from the Intelligence Training Academy – a 290% increase over FY 2020. Last year, I&A also increased the number of students from other DHS components at the National Intelligence University (NIU) by 57% and expanded their enrollment in Intelligence Community courses by 121%.

Overall, I&A's recent efforts to enhance its internal and external training have been exceptional. In fact, they recently earned recognition with two awards from the Director of National Intelligence: the "Intelligence Community Learning Innovator of the Year Team Award" for our post-pandemic pivot and success in the virtual training space and the "Intelligence Community Education/Training Support Staff Person of the Year" for the good work of one of our exceptional training staff members.

Effective Oversight

I&A has also made great strides in developing a comprehensive and effective oversight process for its intelligence activities. In direct response to the findings and recommendations of numerous reports and reviews over the past several years, I&A has significantly enhanced its oversight efforts to instill a culture that is intensely focused on analytic integrity and on the protection of the privacy, civil rights, and civil liberties of U.S. persons.

The touchstone of that oversight is found in the Attorney General-approved Intelligence Oversight Guidelines for I&A's intelligence activities. These guidelines ensure that I&A appropriately collects, retains, and disseminates information concerning U.S. persons and executes its vital mission to protect the Homeland without compromising our values or the privacy, civil rights, and civil liberties of Americans.

I&A has developed strong processes to ensure compliance with both the letter and the spirit of these guidelines. It has built a Privacy and Intelligence Oversight Branch of professionals who ensure that the constitutional and privacy rights of U.S. persons are carefully observed throughout the intelligence cycle. The branch, which doubled in size in 2021, provides intelligence oversight training for all I&A personnel, conducts compliance reviews and inquiries

into questionable intelligence activities, reviews certain finished intelligence products, and advises I&A staff and managers on privacy matters. These oversight professionals are assigned to each mission area of I&A, and one of them is embedded with the collectors in the Open Source Collection Office to advise and assist with applying intelligence oversight and privacy principles to I&A's open-source collecting and reporting activities.

I&A has also hired two career Intelligence Community professionals as full-time ombuds – an Organizational Ombuds and an Analytic Ombuds. I&A's ombuds are independent, impartial dispute resolution practitioners who provide an informal and confidential forum to hear, informally investigate, and help resolve individual and organizational concerns without fear of retaliation. I&A employees are encouraged to bring the full scope of issues to the ombuds, including concerns about collection practices and analytic tradecraft. Beyond facilitating equitable outcomes for employees with these concerns, the ombuds seek to promote better communication, foster constructive dialogue, increase collaboration, and improve transparency within the workforce.

It is important to note that DHS's Office for Civil Rights and Civil Liberties, Privacy Office, and Office of the General Counsel are all heavily involved in our internal intelligence oversight efforts. These offices help oversee and train DHS intelligence personnel, and, importantly, they review most I&A finished intelligence products before they are approved and disseminated outside the federal government, to ensure that those products are drafted in a way that fully protects the privacy and the legal rights of all U.S. persons. As mentioned above, at the Secretary's direction, we are currently extending that review process to the finished products of the other DHS components as well.

As we continue to confront the myriad threats facing the Homeland, we recognize that our activities must be conducted under strict oversight and in a manner that is consistent with the law and the Constitution and that fully protects the privacy, civil rights, and civil liberties of United States persons.

Future of I&A

I have now gone through I&A's overall mission and the way that I&A is currently deployed to further that mission. I will now describe what we are doing to position I&A to carry out that mission in the future.

Strategic Review. To ensure that our organizational decisions are aligned with a long-term strategy, I&A has hired two distinguished national security professionals to assist with strategic planning – one the former Senate-confirmed General Counsel of DHS and the other the former Acting Director and Deputy Director of the National Counterterrorism Center. These national security professionals are engaging with I&A's stakeholders, reviewing I&A's current activities and resources, and helping to ensure that I&A is adapting and aligning its resources to meet the evolving threats to the Homeland. They are a great source of advice and counsel to my team and me as we chart out the future of I&A.

Analytic Resources. We have also asked Congress for the resources that will equip I&A to meet those evolving threats. Our budget request for FY 2023 allows us to expand our analytic cadre to, among other things, enhance cybersecurity threat analysis, deepen our coverage of nation-state threat actors and their proxies, enable analysis focused on the full range of terrorism tactics, techniques, and procedures, and better assess how these threats impact our critical infrastructure. The request also includes funding to enable and sustain I&A's economic security and financial intelligence mission, including efforts related to foreign direct investment in the U.S. (CFIUS), threats to the U.S. supply chain, intellectual property theft, and strategic threats to U.S. economic security. Finally, our budget request seeks a necessary investment in modernizing our information technology tools, particularly those needed for analyzing significant unclassified data holdings, which are critical to our ability to identify and share actionable intelligence with the Intelligence Community and our SLTT and private sector partners.

III. CURRENT THREAT ASSESSMENT

With that clarification of I&A's mission and the steps we are taking to meet that mission now and in the future, I will now turn to the homeland security threats that we are confronting. Today's threat environment is a complex combination of domestic and international terrorism, transnational organized crime, malicious cyber actors, traditional counterintelligence threats, and foreign adversaries who try to undermine our national security with non-traditional collection efforts and malign foreign influence campaigns.

Nation-State Adversaries

Nation-state adversaries are becoming an increasingly complex threat with the use of both traditional and non-traditional tradecraft. These countries, including China, Iran, and Russia, engage in traditional, government-focused espionage; they engage in economic espionage targeting private sector intellectual property and technology; and they also conduct malign influence campaigns to sow divisions in our society and to undermine confidence in our democratic institutions.

The People's Republic of China (PRC), in particular, has aggressively employed a whole-of-government approach to undercut U.S. competitiveness and democracy, methodically targeting each of our industries to steal our innovations, amplifying narratives that sow doubt in U.S. institutions, and targeting messaging campaigns against U.S. politicians they deem hostile to PRC interests, including one U.S. congressional candidate who was a leader in the Tiananmen Square demonstrations in 1989. The PRC also employs trade agreements, sister-city agreements, and other seemingly benign economic and cultural outreach efforts to foster exploitable relationships to exert influence and establish a stronger foothold in the U.S. Homeland. Recently, the PRC has gone so far as to set up so called "police stations" in the U.S. to leverage police powers to target dissidents and other perceived adversaries in our country.

Terrorism

As the IC has assessed, the most significant and persistent terrorism threat we currently face is from U.S.-based lone actors and small groups who are inspired by a broad range of ideologies, including Homegrown Violent Extremists (HVEs) and Domestic Violent Extremists (DVEs). Before addressing that assessment, however, I would like to register our recognition of the significant and complex policy issues related to an intelligence agency conducting lawful activities to counter the domestic terrorism threat. The motivations that drive domestic terrorists to engage in criminal activity often overlap with lawful, constitutionally protected thought, activity, and speech. As such, we recognize that it is critical that we focus our domestic terrorism intelligence operations only on activity reasonably believed to have a nexus to violence and always in accordance with the legal and policy limitations on that conduct. As a result, I&A personnel are prohibited under all circumstances from engaging in any intelligence activities for the sole purpose of monitoring activities protected by the First Amendment.

For definitional purposes, U.S.-based terrorist actors fall into two groups. The Homegrown Violent Extremists (HVEs) are those who are radicalized to violence by the ideology of a foreign terrorist organization. The Domestic Violent Extremists (DVEs) are those who seek to further political or social goals through violence or threats of violence, without direction or inspiration from any foreign organization.

DVEs are motivated by a wide range of factors, including biases against racial and religious minorities, perceived government overreach, conspiracy theories promoting violence, and false or misleading narratives that are often spread online. Among DVEs, racially or ethnically motivated violent extremists (RMVEs) and militia violent extremists (MVEs) present the most lethal DVE threats, with RMVEs most likely to conduct mass-casualty attacks against civilians and MVEs typically targeting law enforcement and government personnel and facilities. RMVEs have been responsible for a majority of DVE-related deaths since 2010 – 92 of the 192 deaths in that period -- often directing their attacks against soft targets, such as large public gatherings, houses of worship, and retail locations.

One tragic recent example of this was the May 2022 murder and wounding of numerous innocent shoppers at a Buffalo, New York, supermarket by a shooter who was motivated by anti-Black and anti-Semitic conspiracy theories, often referred to as the "great replacement" or "white genocide" theories. Another example was the August 2019 shooting at a Walmart in El Paso, Texas, which resulted in the death of 23 individuals allegedly by a shooter who cited similar grievances and inspiration for the attack and is awaiting trial.

Among DVEs, RMVEs also possess the most persistent and concerning connections around the world. RMVEs are present throughout many western countries, they are known to frequently communicate with each other, and they routinely use the internet to inspire like-minded individuals to launch attacks in other countries. Over the past two decades, many transnational online RMVE networks have emerged, fostering a decentralized movement that encourages supporters to undertake violent action that is framed around the concept of leaderless resistance in support of global RMVE activity. For example, both the Buffalo and El Paso

attackers indicated they were inspired by Australian Brenton Tarrant's 2019 attack on two mosques in Christchurch, New Zealand, which killed 51 worshippers.

In recent years, DVEs adhering to different violent extremist ideologies have increasingly been motivated and radicalized by perceptions of government overreach and election. As a consequence, we have seen an increase in threats and acts of violence from these actors against law enforcement, judiciary, and government personnel.

While focusing on domestic terrorism, we remain vigilant against the terrorist threat from foreign terrorist organizations (FTOs) like ISIS, Al-Qaeda, and al-Shabaab. These foreign groups are committed to attacking the United States, and they continue to expand their networks, raise funds, recruit, organize, plan operations, and hone their social media-based messaging to inspire attacks in the Homeland and against our allies. They maintain a highly-visible online presence focused on inspiring HVEs to conduct attacks in the United States. ISIS media outlets, for example, routinely issue online content portraying the group as the true vanguard of resistance against the United States and its allies, calling for attacks in the United States, and sharing tactics and techniques for conducting terrorism operations without detection by law enforcement.

Iran and its partner, Lebanese Hezbollah, also continue to pose an enduring threat to the Homeland, evidenced by Iran's public statements threatening retaliation for the death of Islamic Revolutionary Guard Corps Quds Force Commander Qasem Soleimani and for the arrests of Iranian agents for plotting operations and spying on Iranian dissidents in the United States. In August, U.S. federal prosecutors unsealed charges against an IRGC member for plotting to assassinate former National Security Advisor John Bolton.

Cyber

On the cyber front, we face a sustained cyber threat from sophisticated nation-state cyber actors and from cybercriminal groups, including cyber-enabled espionage and disruptive cyber-attacks on healthcare companies and other private sector organizations.

In terms of nation-state actors, we can expect Russia to continue its targeting of the Homeland with malicious cyber operations to collect intelligence, enable influence operations, and improve its ability to disrupt critical infrastructure in a crisis. We anticipate similar efforts from Beijing with the sharpening competition between the United States and China and the potential threat of a crisis over Taiwan. Iran's growing expertise and willingness to conduct aggressive and opportunistic cyber operations make it a major threat as well. Last year, for instance, cyber actors from Iran attempted to conduct a cyberattack on Boston Children's Hospital. While the attack was successfully thwarted, it exemplifies the type of high-impact threat we face from Iran.

In terms of criminal actors, ransomware has become a serious threat in recent years. Ransomware incidents have increasingly targeted the U.S. government and critical infrastructure organizations, with ransom demands in 2021 exceeding $3 billion in the United States alone and the ransomware attacks costing an estimated $160 billion in downtime. There is also increasing criminal misuse of cryptocurrencies to facilitate illicit activity.

Transnational Criminal Organizations

Another enduring and critical national security threat is that from Transnational Criminal Organizations (TCOs) – particularly Mexico-based cartels – that continue to wreak havoc on the health and economic prosperity of our communities and profit at the expense of American lives.

These cartels are becoming more and more sophisticated, with some extending their traditional narcotics-focused trafficking operations to human smuggling, and even taking over legitimate industries in the regions they dominate in Mexico. They have also become expert at mitigating U.S. law enforcement interdiction efforts, actively employing modified commercial drones for counter-surveillance operations and skillfully using diversion tactics to facilitate drug smuggling operations at the border.

Two particular TCOs, the Sinaloa Cartel and New Generation Jalisco Cartel, dominate today's drug smuggling market. These TCOs are trafficking a range of narcotic products, to include methamphetamine, fentanyl, cocaine, and heroin. In FY 2021, CBP seized 221,000 pounds of these drugs, which was a nearly 40% increase over FY 2019.

In a very troubling development, we are increasingly seeing mass production of illicit synthetics, like fentanyl and methamphetamine, which are cheaper to produce than crop-based drugs. As a result, these drugs are becoming more and more common throughout the United States, and the deaths from these drugs are spiraling upward – approximately 108,000 last year alone. This is not surprising, given the potency of these new drugs. In the case of fentanyl, for example, just a few grains of the chemical are enough to stop a heart and kill someone. Nor is it surprising, given how many different products are now laced with fentanyl, that many of the drug's victims are youngsters who have no idea they are taking fentanyl.

The intelligence suggests that this threat will only grow in the coming years, as these cartels further concentrate on the lucrative fentanyl market, maintain and try to expand the flow of precursor chemicals from China, and shift their finishing operations from Mexico to the United States, which they are now doing to cut costs and facilitate more efficient and broader distribution. The threat from these synthetic drugs is tragic, and it is a threat that will require a whole-of-government and a whole-of-society effort to stem the tide of deaths among our people.

Conclusion

Thank you again for the opportunity to appear before you today to discuss these critical issues and for your continued support. I&A remains committed to meeting its statutory mandate by enhancing partnerships, reinvigorating our information sharing efforts, and continually improving the way we deliver intelligence to our customers. In addition, I&A is intensely focused on improving oversight, training, and morale across the organization. These efforts are vital to improving the overall health of I&A and ensuring that each and every member of the workforce feels fully supported and fully empowered to achieve our core mission of securing the Homeland with honor and integrity.

Thank you for your time today, and I look forward to answering your questions.