EXAMINING THE OPERATIONS OF THE OFFICE OF INTELLIGENCE AND ANALYSIS

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERRORISM

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

DECEMBER 13, 2022

Serial No. 117–74

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
51–412 PDF WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
DONALD M. PAYNE, JR., New Jersey
J. LUIS CORREA, California
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
ERIC SWALWELL, California
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California
JOSH GOTTHEIMER, New Jersey
ELAINE G. LURIA, Virginia
TOM MALINOWSKI, New Jersey
RITCHIE TORRES, New York, Vice Chairman
JOHN KATKO, New York
MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
JEFFERSON VAN DREW, New Jersey
MARIANNETTE MILLER-MEEKS, Iowa
DIANA HARSHBARGER, Tennessee
ANDREW S. CLYDE, Georgia
CARLOS A. GIMENEZ, Florida
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
KAT CAMMACK, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
MAYRA FLORES, Texas

HOPE GOINS, *Staff Director*
DANIEL KROESE, *Minority Staff Director*
NATALIE NIXON, *Clerk*

SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERRORISM

ELISSA SLOTKIN, Michigan, *Chairwoman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
JOSH GOTTHEIMER, New Jersey
TOM MALINOWSKI, New Jersey
BENNIE G. THOMPSON, Mississippi *(ex officio)*
AUGUST PFLUGER, Texas, *Ranking Member*
MICHAEL GUEST, Mississippi
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
JOHN KATKO, New York *(ex officio)*

BRITTANY CARR, *Subcommittee Staff Director*
ADRIENNE SPERO, *Minority Subcommittee Staff Director*
ALICE HAYES, *Subcommittee Clerk*

CONTENTS

Page

STATEMENTS

The Honorable Elissa Slotkin, a Representative in Congress From the State of Michigan, and Chairwoman, Subcommittee on Intelligence and Counterterrorism:
Oral Statement 1
Prepared Statement 2
The Honorable August Pfluger, a Representative in Congress From the State of Texas, and Ranking Member, Subcommittee on Intelligence and Counterterrorism:
Oral Statement 4
Prepared Statement 6
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Chairman, Committee on Homeland Security:
Prepared Statement 7
The Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas:
Prepared Statement 8

WITNESS

Mr. Kenneth L. Wainstein, Under Secretary, Office of Intelligence and Analysis, U.S. Department of Homeland Security:
Oral Statement 10
Prepared Statement 12

FOR THE RECORD

Statement of the National Fusion Center Association 19

APPENDIX

Questions From Chairman Bennie G. Thompson for Kenneth L. Wainstein 35
Questions From Chairwoman Elissa Slotkin for Kenneth L. Wainstein 37
Questions From Ranking Member August Pfluger for Kenneth L. Wainstein ... 40

EXAMINING THE OPERATIONS OF THE OFFICE OF INTELLIGENCE AND ANALYSIS

Tuesday, December 13, 2022

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE
AND COUNTERTERRORISM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 310, Cannon House Office Building, Hon. Elissa Slotkin [Chairwoman of the subcommittee] presiding.

Present: Representatives Slotkin, Jackson Lee, Langevin, Pfluger, Guest, Van Drew, LaTurner, and Meijer.

Ms. SLOTKIN. The Subcommittee on Intelligence and Counterterrorism will be in order.

The subcommittee is meeting today on "Examining the Operations of the Office of Intelligence and Analysis" at the Department of Homeland Security.

Without objection, the Chair is authorized to declare the subcommittee in recess at any point.

Good morning, everybody. I want to thank my colleagues from the Committee on Homeland Security for joining us, both in person and on-line, for this important hearing to discuss the current and future state of the Department of Homeland Security's Office of I&A, or Intelligence and Analysis.

I want to welcome back Mr. Kenneth Wainstein, who is testifying before us this morning. After serving as our Nation's fourth Homeland Security Advisor, Mr. Wainstein is intimately familiar with this committee. We are glad to welcome you back in your new role as the under secretary for intelligence and analysis at DHS.

As a former CIA officer, I understand the importance of the role that intelligence plays in preventing and mitigating threats to the homeland and in developing long-term expertise on issues and supporting the policy-making process.

I&A's contributions to the intelligence process are particularly important, as the office has a unique responsibility, unique among the, I think, 17 different intel agencies across the U.S. Government, to provide intelligence to our State, local, Tribal, territorial, and private-sector partners, who in many cases are on the front lines of keeping Americans safe.

I&A's mission success is dependent on effective information-sharing capabilities with local partners to address these dangerous threats. However, we know that I&A has often struggled to consistently achieve mission success.

DHS is our newest Cabinet-level agency, just born with 9/11. So we are all invested in I&A's success. We want to make sure that we understand I&A's information sharing to State and local partners, make sure it is timely, make sure our communities are getting easy access to intelligence.

We want to make sure that some of the concerns raised by the GAO, the Government Accountability Office, recently in their preliminary report that focused on some of the products right before January 6, 2021, the day that the U.S. Capitol came under attack—make sure we understand some of the sharing practices, since some of those products were not made available until days after the attack.

So we are interested in hearing from you, Mr. Wainstein, as you are in, I believe, your sixth month of taking the helm here, what are some of the issues you are focused on? How are you making sure that places like I&A are not politicized in any way, that it lives up to the intelligence community tradition of being nonpartisan and providing support to whoever is the Commander-in-Chief, whoever is in leadership? Then help us understand some of the concerns that have been brought up in these various investigations.

We are particularly—I was pleased to hear you say, under secretary, during your Senate confirmation hearing that you are committed to the production of "objective, unvarnished intelligence" and that is your first focus as under secretary. We all believe that that is the mission of I&A.

Today I hope we have an honest, robust conversation about how we address those issues, how we help, from an oversight perspective, to make sure that, for the American people, for the stakeholders invested in I&A's success, we all feel that you are able to do your best work to keep the homeland safe.

I just want to say that I believe this is the final hearing of this subcommittee's work before the end of the year. Throughout my time as Chairwoman, we have had really wonderful staff support. We have worked with the Department, with other Federal agencies. I want to thank Ranking Member Pfluger for being a good partner in this committee.

So, as we move into a new Congress, I hope that the work that you are going to put on display for us is something we can take forward into the next Congress and continue to develop that relationship for the betterment of the Department and for the people of the American public.

[The statement of Chairwoman Slotkin follows:]

STATEMENT OF CHAIRWOMAN ELISSA SLOTKIN

DECEMBER 13, 2022

The Subcommittee on Intelligence and Counterterrorism will be in order. The subcommittee is meeting today on "Examining the Operations of the Office of Intelligence and Analysis."

Without objection, the Chair is authorized to declare the subcommittee in recess at any point.

Good morning.

I want to thank my colleagues on the Committee on Homeland Security for joining me in this important hearing to discuss the current and future state of the Department of Homeland Security (DHS)'s Office of Intelligence and Analysis.

And I want to welcome back Mr. Kenneth L. Wainstein, who is testifying before us this morning.

After serving as our Nation's fourth Homeland Security Advisor, Mr. Wainstein is intimately familiar with this committee, and we are glad to welcome you back in your new role as the under secretary for intelligence and analysis—or I&A—at DHS.

As a former CIA intelligence officer, I understand the important role that intelligence plays in helping prevent and mitigate threats to the homeland and U.S. interests abroad—and in developing long-term expertise on issues and supporting the policy-making process.

I&A's contributions to the intelligence process are especially vital, as the office has the unique responsibility for delivering intelligence to our State, local, Tribal, territorial, and private-sector partners—who in many cases are on the front lines of keeping Americans safe.

I&A's mission success is dependent on effective information-sharing capabilities and processes with these local partners to address the persistent and dangerous threats facing our Nation.

However, I&A has struggled to consistently achieve mission success.

At times, information from I&A to State and local partners may not be timely enough to help them take steps to protect our communities from threats.

For example, the Government Accountability Office recently issued a preliminary report finding that although I&A developed two threat products regarding potential threats on January 6, 2021—the day the U.S. Capitol came under attack from domestic terrorists—it did not share the products with partners until 2 days after the attack, on January 8.[1]

Delays in I&A intelligence product review, approval, and dissemination are not new.

A March 2017 report by the inspectors general of DHS, the intelligence community, and the Department of Justice found that I&A officials in the field lacked, and I quote, "release authority, that is, the authority to send intelligence reports directly to the clearing offices for review and approval without first sending them to the Reporting Branch," where there were backlogs.[2]

Four years later—a DHS Administrative Review found that similar review backlogs were a factor in the improper collection and dissemination of open-source intelligence reports on journalists engaged in Constitutionally-protected activities during the Portland, Oregon protests in July 2020.[3]

Unresolved internal control deficiencies are not the only thing that has troubled I&A over the years.

Under the previous administration, I&A was repeatedly politicized, especially regarding information that could be used to justify the administration's actions.

Between March 2018 and August 2020, the senior official performing the duties of the under secretary for intelligence and analysis, Brian Murphy, made at least five whistleblower-protected disclosures regarding the politicization of information within DHS.

These concerns led the OIG to initiate investigations, during which the OIG found that—on at least one occasion—and I quote, "I&A employees during the review and clearance process changed the product's scope by making changes that appear to be based in part on political considerations, potentially impacting I&A's compliance with intelligence community policy."[4]

These serious long-standing issues amount to a decline in institutional capacity that is prone to happen when an agency lacks a permanent leader who is dedicated to the mission and leading the workforce to mission success.

This is why, Under Secretary Wainstein, I was pleased to hear you say during your Senate confirmation hearings that you are committed to the production of "ob-

---

[1] Government Accountability Office, DRAFT Report "CAPITOL ATTACK: Federal Agencies Identified Some Threats, but Did Not Fully Process and Share Information Prior to January 6, 2021," December 2022.

[2] "Review of Domestic Sharing of Counterterrorism Information," Inspectors General of the Intelligence Community, Department of Homeland Security, and Department of Justice, March 2017, *https://oig.justice.gov/sites/default/files/reports/OIG-17-49-Mar17.pdf.*

[4] "Report on DHS Administrative Review into I&A Open Source Collection and Dissemination Activities During Civil Unrest Portland, Oregon, June through July 2020," DEPARTMENT OF HOMELAND SECURITY OFFICE OF GENERAL COUNSEL, Jan. 6, 2021, *http://cdn.cnn.com/cnn/2021/images/10/01/internal.review.report.20210930.pdf.*

[4] Joseph V. Cuffari, DHS Actions Related to an I&A Intelligence Product Deviated from Standard Procedures, DEPARTMENT OF HOMELAND SECURITY OFFICE OF INSPECTOR GENERAL, Apr. 22, 2022, *https://www.oig.dhs.gov/sites/default/files/assets/2022-05/OIG-22-41-Apr22-Redacted.pdf.*

jective, unvarnished intelligence," and that your first focus as under secretary is on the workforce.

I believe in the mission of I&A—and today I look forward to having a robust, honest conversation about how we address these issues to ensure I&A is most effective, that it continues to garner support from its stakeholders and the American public, and that the men and women of I&A feel good about their efforts to keep the homeland safe.

Throughout my time as chair of the Intelligence and Counterterrorism Subcommittee, I have worked tirelessly with the Department, other Federal agencies, and Members on both sides of the aisle—including my Ranking Member, Mr. Pfluger—to find solutions to issues that came before us.

So as we move into a new Congress, I hope that we use what we learn today to work together in ensuring I&A's success.

Before I turn to the Ranking Member, without objection, I ask unanimous consent to enter into the record a statement by the National Fusion Center Association.

Ms. SLOTKIN. The Chair now recognizes the Ranking Member of the subcommittee, the gentleman from Texas, Mr. Pfluger, for an opening statement.

Mr. PFLUGER. Thank you, Madam Chair. I agree with your sentiments, and it has been a pleasure to serve on this committee with you. I appreciate your leadership, the staff's participation, and, I think, the ability to look at some of these issues in what I hope will continue to be more of an apolitical, nonpartisan view focused on security.

So, last month, at our full committee hearing, we focused on world-wide threats to the homeland, and Secretary Mayorkas testified about foreign terrorist organizations seeking new and innovative ways to target the United States—on-going cyber attacks on our critical infrastructure and emerging technology like drones being weaponized to cause harm; so many other threats. Perhaps more now than ever before, we must depend on our intelligence professionals to anticipate, to detect, to identify the countless threats that we are facing.

The Office of Intelligence and Analysis was tasked with the important role of leading the intelligence enterprise, composed of DHS components, as it navigates that complex threat environment, and it seeks to mitigate threats before they become costly or devastating to Americans or to our homeland.

Per statute, I&A also serves as the intel community's primary liaison to State, local, Tribal, territorial, private partners, as well as the conduit for information exchange within the many components of DHS that rely on timely and reliable, accurate intelligence to execute their own mission sets.

Being someone who served in the military, I know this for a fact: Intelligence can be invaluable when properly vetted and delivered to the appropriate stakeholders prior to the escalation of a threat.

However, I do believe I&A has struggled, as the Chairwoman has said, in a couple of areas, potentially identifying and disseminating pertinent intelligence. Whether we call these "failures" or some other adjective, having been investigated by DHS OIG, which has found that I&A identified pertinent specific threat information on several occasions but in some of these cases failed to produce any reports on these threats until clearly past the point of mitigation.

For example, we will go back to Portland, Oregon. Prior to your time, I&A published several intelligence reports on U.S. journalists engaged in ordinary journalism protected by the First Amendment and leading to public outcry. DHS later acknowledged, rightfully

so, that these reports were misguided and eventually recalled them.

Though a comprehensive DHS administrative review on I&A intelligence collection and dissemination activities in Portland found no evidence of politicization, it did uncover a host of other alarming issues that undoubtedly played a role in these high-profile intelligence failures.

The DHS review found I&A suffered from understaffed and overworked personnel, high turnover and decreased institutional knowledge, lack of oversight and leadership in some cases, and training gaps that left employees operating without an informed direction or knowledge of the policy.

In the Portland incident, junior collectors with less than ideal guidance and very little oversight were sent into a volatile situation with enormous pressure to produce intelligence products before they had mastered the core competencies of their own specific duties, leading to intelligence reporting on journalists rather than the real-world threats.

Conversely, in other situations, open-source collectors discovered potentially actionable threat intelligence prior to escalation but fell short in the critical mission set of sharing that information with law enforcement partners because they were, again, unclear on the Department's intelligence reporting policy and requirements.

These sorts of incidents led to public confusion, anger, and even ridicule, which only exacerbated the morale of those within I&A, many of whom had extended their working hours, covering 24/7 shifts and truly working overtime.

I look forward to hearing from you, Mr. Under Secretary, on where the morale of the rank-and-file members is today and what leadership has done to right the ship.

Like so many other members of the IC, I&A is granted the authority to collect intelligence through publicly-available sources. Having multiple agencies collect and disseminate intelligence from publicly-available internet searches and other law enforcement public releases can offer limited value and at times could be redundant, duplicative, as we mentioned before the hearing started.

A recent DHS OIG review of 9 I&A finished intelligence domestic terrorism products released over a 1-year period showed 6 of the products contained information that its partners could have easily found.

I hope that during this hearing today we will be able to talk about where we have a duplicative or overlapping gathering system and we can have that open and honest conversation to know where I&A can be most effective going forward.

In the two decades since the attacks of September 11, the intelligence apparatus has evolved greatly, and I am glad that it has, as the Chairwoman served in one of those agencies. The Office of the Director of National Intelligence, including the National Counterterrorism Center, NCTC, has been established. The FBI has refocused considerable attention and resources toward the counterterror mission and enhancing their information-sharing relationship with law enforcement partners. DHS-component intelligence branches, from CBP to CISA, have been bolstered.

It is incumbent on us to assess and review at this time the performance of the Office of Intelligence and Analysis and consider steps to update and rebalance its role and responsibilities to ensure that the value is what the American people not only deserve but what our hard-earned taxpayer money is going toward, eventually with the goal of continuing to keep the homeland protected.

So it is with that that I hope we have a great hearing, thank you for calling this, and I yield back.

[The statement of Ranking Member Pfluger follows:]

STATEMENT OF RANKING MEMBER AUGUST PFLUGER

Thank you, Madam Chairwoman. I am pleased the subcommittee is holding this important hearing today. Last month, at our full committee hearing focused on Worldwide Threats to the Homeland, Secretary Mayorkas testified about foreign terror organizations seeking new and innovative ways to target the United States, ongoing cyber attacks on our critical infrastructure, emerging technology like drones being weaponized to cause harm, and many other threats. Perhaps now more than ever, we must depend on our intelligence professionals to anticipate and detect the countless threats to our homeland so that we can defend our country from those plotting against us.

The Office of Intelligence and Analysis was tasked with the important role of leading the intelligence enterprise, composed of DHS components, as it navigates the complex threat landscape and seeks to mitigate threats before they become costly or devastating attacks to the homeland. Per statute, I&A also serves as the intelligence community's primary liaison to State, local, Tribal, territorial, and private partners, as well as the conduit for information exchange within the many components of DHS that rely on timely and reliable intelligence to execute their prescribed mission sets.

Intelligence can be invaluable when properly vetted and delivered to the appropriate stakeholders prior to escalation of a threat. However, I&A has struggled in identifying and disseminating pertinent intelligence. I&A's failures have been investigated by the DHS OIG, which has found that I&A identified pertinent specific threat information on several occasions, but failed to produce any intelligence reports on these threats until clearly past the point of mitigation.

For example, during the riots in Portland, Oregon, I&A published several intelligence reports on U.S. journalists engaged in ordinary journalism protected by the First Amendment, leading to public outcry. DHS later acknowledged the reports were misguided and recalled them. Though a comprehensive DHS administrative review on I&A intelligence collection and dissemination activities in Portland found no evidence of politicization, it did uncover a host of other alarming issues that undoubtedly played a role in these high-profile intelligence failures.

The DHS review found I&A suffered from understaffed and overworked personnel, high turnover and decreased institutional knowledge, lack of oversight and leadership, and training gaps that left employees operating without informed direction and policy. In the Portland incident junior collectors, with less-than-ideal guidance and very little oversight, were sent into a volatile situation with enormous pressure to produce intelligence products before they had mastered the core competencies of their duties, leading to intelligence reporting on journalists rather than real-world threats. Conversely, in other situations, open-source collectors discovered potentially actionable threat intelligence prior to escalation but fell short in their critical mission to share that intelligence with law enforcement partners because they were again unclear on the Department's intelligence reporting policy and requirements.

These sorts of incidents led to public confusion, anger, and even ridicule, which only exacerbated the morale of those within I&A, many of whom had worked extended hours covering 24/7 shifts during staffing shortages. I look forward to hearing from Under Secretary Wainstein on where the morale of the rank-and-file stands today and what leadership is doing to right this ship and improve the culture at I&A.

Like many other Members of the intelligence community, I&A is granted the authority to collect intelligence through publicly-available sources. Having multiple agencies collect and disseminate intelligence from publicly-available internet searches and other law enforcements' public releases can offer limited value and at times needless redundancy. A recent DHS OIG review of 9 I&A finished intelligence domestic terrorism products released over a 1-year period showed 6 of the products contained information that its partners could easily find on their own.

I hope to hear from the under secretary on efforts to address the issues that have plagued I&A and contributed to the struggles illustrated by this series of critical reviews. More specifically, I hope to hear what initiatives are under way to address the challenges in reporting timely and relevant intelligence while ensuring quality control and oversight.

Last, I hope we can discuss more broadly how I&A can be most effective going forward. In the two decades since the attacks of September 11, the intelligence apparatus has evolved greatly. The Office of the Director of National Intelligence, including the National Counterterrorism Center, has been established. The FBI has refocused considerable attention and resources toward the counterterror mission and enhancing their information-sharing relationship with law enforcement partners. And DHS component intelligence branches—from CBP to CISA—have been bolstered.

It is incumbent on us to assess and review the performance of the Office of Intelligence & Analysis and consider steps to update and rebalance its role and responsibilities to ensure it provides a distinct value add to the DHS intelligence enterprise and all the external partners and stakeholders it serves.

With that I yield back the balance of my time.

Ms. SLOTKIN. I thank the Ranking Member.

Members are also reminded that the subcommittee will operate according to the guidelines laid out by the Chairman and Ranking Member of the full committee in their February 3, 2021, colloquy regarding remote procedures.

The Chair now recognizes Mr. Wainstein—I am sorry. Just making sure we don't have Mr. Thompson or Mr. Katko? Opening statements may be submitted for the record.

[The statements of Chairman Thompson and Honorable Jackson Lee follow:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

DECEMBER 13, 2022 AT 10 O'CLOCK AM EST

Good morning.

Thank you to Subcommittee Chair Slotkin and Ranking Member Pfluger for calling today's hearing to examine the Department of Homeland Security (DHS)'s Office of Intelligence and Analysis (I&A).

And thank you, Under Secretary Wainstein, for joining us today.

At the Committee's annual Worldwide Threats to the Homeland hearing last month, we heard from the Secretary of Homeland Security, FBI director, and director of the National Counterterrorism Center that threats to the homeland have never been more complex.

We heard that threats posed by domestic violent extremists continue to rise and those posed by foreign terrorist organizations have not gone away.

We also heard that state actors continue to engage in cyber operations that threaten Americans' safety and security.

Just recently, a cyber attack on a power substation in North Carolina wiped out power for more than 45,000 people for days.

As Chairwoman Slotkin mentioned in her opening remarks, the role of intelligence is more important than ever, because it helps us detect, deter, and defend against the myriad of threats we face today.

As an intelligence community member, I&A contributes to the mission of delivering information to help protect our country.

I&A is an invaluable player, as it is the only intelligence community member that is tasked—by law—with passing intelligence information to State, local, Tribal, territorial, and private-sector partners.

Our State, local, Tribal, and territorial partners are on the ground in communities across the country, working daily to protect Americans from danger.

And in many ways, private-sector partners help support that critical effort.

To do the best job possible, it is critical that those on the ground have the most reliable intelligence available.

Unfortunately, I&A has faced challenges that have raised questions about its ability to meet its mandate.

I&A has struggled at times to identify specific analytic products and activities to best meet the needs of State and local partners.

It has also historically had trouble disseminating products in a timely manner—Chairwoman Slotkin referenced a few instances in her opening statement—and there have been issues with the mechanisms through which the information has been shared.

More recently, the Trump administration sought to use I&A as a tool to push the former President's political agenda.

Today's hearing is an opportunity for Members to hear from Under Secretary Wainstein about his plans to "right the ship."

Under his leadership, I&A already has taken important steps in the right direction—one of those being improving training for its employees.

In October, I&A changed its new-hire on-boarding and initial training program to align them in a more seamless experience.

The DHS Intelligence Training Academy (ITA) is also working diligently to ensure that before being assigned to their unit and beginning work, all new employees receive training on regulations surrounding:

- collection, retention, and dissemination of data, and
- protecting privacy, civil rights, and civil liberties.

Moreover, earlier this year the ITA developed a new, special learning module on identifying and defending against politicization.

Having properly-trained personnel is foremost in ensuring that I&A is well-positioned to meet its mission of delivering timely, useful information to State and local governments and the private sector.

I look forward to hearing from Under Secretary Wainstein on any updates regarding improving I&A's training regimen, and I stand ready to work with the under secretary on legislation to ensure the preservation of the improvements made and that we continue to build on them.

As training is just one part of investing in the workforce, I also look forward to hearing about Under Secretary Wainstein's efforts to boost morale within the office, as unfortunately, I&A once again ranked near the bottom of the 2021 Best Places to Work in the Federal Government list for subcomponents.

I've said before that an agency's most significant asset is its people.

When we properly invest in their well-being and professional development, mission success becomes more attainable.

With that, I yield back.

STATEMENT OF HONORABLE SHEILA JACKSON LEE

DECEMBER 13, 2022

Thank you, Chairwoman Slotkin and Ranking Member Pfluger, for convening this hearing and affording us, the Homeland Security Subcommittee on Intelligence and Counterterrorism, the opportunity to hear testimony on "Examining the Operations of the Office of Intelligence and Analysis."

I welcome today's witness, the Honorable Kenneth L. Wainstein, under secretary for intelligence and analysis, U.S. Department of Homeland Security and look forward to your testimony.

This hearing is the Intelligence and Counterterrorism Subcommittee's opportunity to examine the operations of the DHS Office of Intelligence and Analysis (I&A) and to hear from the recently confirmed Under Secretary for Intelligence and Analysis Kenneth L. Wainstein on his vision for the office.

During the administration of the former president, the DHS I&A faced several challenges caused by a misalignment of the aims of the former President's administration and the facts as identified by DHS I&A's intelligence products.

For example, a May 13, 2019, whistleblower complaint states that the Trump administration members at DHS I&A made inquiries requesting information indicating that the Southwest Border was being utilized by terrorists as a point of entry to the United States.

However, DHS I&A's intelligence products showed overwhelming intelligence and evidence that the Southwest Border was NOT a primary entry point for terrorists.

This attempted politicization by the former President's administration, during his tenure, of the intelligence gathering of DHS I&A is gravely concerning.

DHS I&A is the only U.S. intelligence community (IC) element that is statutorily charged with delivering intelligence to our State, local, Tribal, and territorial (SLTT) and private-sector partners, and with developing intelligence from those partners for the Department and the IC.

As such, State, local, Tribal, and territorial (SLTT) governments, the private sector, the intelligence community, and critical infrastructure owners and operators de-

pend on DHS I&A components to ensure that they are aware of the most pressing threats to the Nation.

Consequently, your leadership, Mr. Wainstein, over I&A is appreciated and critical at this time when domestic and home-grown violent extremism are on the rise.

Domestic Violent Extremists (DVEs) jeopardize Americans' safety and security, as they seek to advance political or social goals through violence or threats of violence, without direction from any foreign organization.

Home-grown Violent Extremists (HVEs) are those who are radicalized to engage in violence by the ideology of a foreign terrorist organization.

In recent years, a number of paramilitary groups within the United States have been stockpiling weapons and preparing for violence.

These characters are a subset of Domestic Violent Extremists (DVEs) called militia violent extremists or MVEs and they present the most likely threat to conduct mass-casualty attacks against civilians.

MVEs typically target law enforcement and Government personnel and facilities. In the past 2 years, some MVEs have been instigated by the former President's allegations about the 2020 election.

According to an opinion article published by the *New York Times* Editorial Board titled "How a Faction of the Republican Party Enables Political Violence," a 2022 survey found that some 18 million Americans believe that the 2020 election was stolen from Donald Trump and that force is justified to return him to power. Of those 18 million, 8 million of them own guns, and 1 million either belong to a paramilitary group or know someone who does.

Another subset of DVE's is defined by their racially or ethnically antagonistic motivations.

Your testimony states that, racially or ethically motivated violent extremists (RMVEs) are also among the most likely to conduct mass-casualty attacks against civilians.

The *New York Times* reports that of the more than 440 extremism-related murders committed in the past decade, more than 75 percent were committed by right-wing extremists, white supremacists, or anti-Government extremists.

RMVE's are a particularly pressing concern to me because the city I represent, Houston, is one of the most diverse cities in the country.

According to Rice University's Kinder Institute for Urban Research, over the past 5 decades, Houston has become a minority-majority city. The population of Harris County—that encompasses Houston—is 31 percent white, 42 percent Hispanic, 19 percent Black and 8 percent Asian.

As you noted in your testimony, RMVEs are responsible for a majority of DVE-related deaths since 2010—92 of the 192 deaths in that period.

There is no place in our democracy for racially or ethnically motivated violence whether they are based on conspiracy theories rooted in anti-Black, antisemitic, or any other bigoted ideologies. Their manufactured paranoia about the "great replacement" and "white genocide," or any other fabricated animosity threatens our Nation's social fabric.

The need for modernization and focus on DHS I&A's ability to produce tangible and impactful products from intelligence gathering is clear.

On January 6, 2021, a violent mob of rioters stormed the U.S. Capitol in an attempt to overturn the results of the 2020 Presidential election. In the midst of the chaos, House Speaker Nancy Pelosi was targeted by the mob. They broke into her office, vandalized it, and defiled the Capitol.

The threats against Members of Congress accelerated since then and are now more than 10 times as numerous as they were just 5 years ago.

As these risks continue to escalate, I welcome your leadership and look forward to learning more about the changes being implemented at DHS I&A and their results.

However, any improvements must still ensure that all intelligence development activities are conducted in accordance with the law, the Constitution, and in a manner that protects individual rights to privacy, civil rights, and civil liberties.

Your testimony reported that a realignment of I&A's open-source collection officers to threat-specific accounts, enabled I&A's intelligence collectors to be 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, and that I&A was able to provide that critical information within minutes of the attack to stakeholders in the FBI and SLTT partners.

It is essential that I&A's intelligence efforts continue to improve and ensure that a January 6th calamity never occurs again.

Again, any improvements must safeguard Constitutionally-protected rights while ensuring that dangerous people seeking to cause harm are denied opportunities to commit acts of violence.

With the rise in domestic violent extremism, cyber attacks, misinformation, and racially-motivated violent extremism, the I&A's mission is formidable and critical.

Yet, DHS I&A must continue to keep our homeland secure, preserve democratic values, and combat maliciously-disseminated falsehoods that are spread with the intent to upend democracy.

Democracy flourishes when citizens are free from harm and can receive reliable information; hence, it is ultimately the task of intelligence agencies to ensure that both occur.

The Nation depends on I&A to help safeguard our liberties and democratic traditions, as well as combat attempts by foreign interests to sow discord in our society through manipulation and misinformation.

Only in this way can we ensure that our homeland remains safe, democracy prevails, and the institutions of our republic are protected for future generations.

Thank you, and I yield back the remainder of my time.

Ms. SLOTKIN. The Chair now recognizes Mr. Wainstein for his opening statement.

STATEMENT OF KENNETH L. WAINSTEIN, UNDER SECRETARY, OFFICE OF INTELLIGENCE AND ANALYSIS, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. WAINSTEIN. Thank you, Chairwoman Slotkin, Ranking Member Pfluger. I very much appreciate the opportunity to discuss DHS's Office of Intelligence and Analysis, or I&A. It is an honor to be here, but it is really an honor to be here representing the dedicated and high-caliber intelligence professionals at I&A.

While my statement for the record includes a very comprehensive sort-of overview of what we are doing at I&A right now, over the next few minutes I would like to run through some of the key points describing I&A's mission and its management and oversight.

In terms of mission, first and very fundamentally, as an intelligence agency, I&A's primary function is to carry out each stage of the intelligence cycle on behalf of its customers: setting requirements, collecting against those requirements, reporting on that collection, and then disseminating those products to our partners.

In terms of dissemination, I&A is currently modernizing how we deliver intelligence to our partners. This year, I&A rolled out a mobile app which allows our customers, police on the beat out in their squad cars, to access products on their phones, making it a lot easier for them to get real-time access to intelligence.

We are also piloting a project that distributes laptops at the Secret level out to our cleared partners so that they don't need to be tethered to a fusion center or to an office to get intel.

The second area that I want to focus on and that is a critical part of our mission is intelligence partnerships. As Secretary Mayorkas often says, DHS is fundamentally a department of partnerships. We have taken a number of recent steps to energize our relationships.

For example, we recently established a Deputy Under Secretary for Intelligence Partnerships, which has elevated that engagement function within our organization, and that person reports directly to me. We started hosting biweekly meetings with our State, local, territorial, and Tribal partners to discuss the threat environment that we all face.

In August, as an example, we hosted a national intelligence summit with the IACP, which convened over 100 partners, police officials from agencies and associations at all levels of government, to reimagine and discuss information-sharing efforts in the future.

So, in addition to the intelligence cycle and intelligence partnerships, a third and absolutely critical mission has been building and enhancing the management and well-being of the I&A work force, something that you both very appropriately mentioned.

I am particularly encouraged by our recent progress both before and after my arrival here in bolstering morale and organizational health. This progress includes:

(A), a focus on enhancing diversity initiatives. We live in a diverse world, and it requires a diverse intelligence work force, and, as such, we consider diversity a core value.

Second, we have reenvisioned our telework program and flexible scheduling to attract and retain talented personnel.

Third, we are improving employee communication on different mechanisms therefor, including how we receive feedback from the work force, which is so critical to self-examination, which is so needed in progress.

Fourth, we have instituted initiatives to bolster employee morale. We launched a speaker series with speakers like Jim Clapper and Stacey Dixon. In October we held the first I&A Family Day in almost 10 years, patterned after what the CIA has done for many generations.

Then, finally, knowing that this committee has placed a special focus on the quality of I&A's training, we have made substantial progress in enhancing our training efforts over the past couple years, including development of oversight training that covers I&A's authorities, the Intelligence Oversight Guidelines, and whistleblower protections.

In addition to training its own staff, I&A has expanded training opportunities for intelligence personnel in other DHS components and among our State and local partners, to the tune of almost a 300 percent increase in 2021 alone in terms of the number of people who have taken that training.

These training efforts are being done in tandem with the formulation of a rigorous process of oversight. In response to the findings from the reports that you all mentioned, I&A has worked hard to instill an oversight culture that is intensely focused on analytic integrity and on the protection of privacy, civil rights, and civil liberties of U.S. persons.

In 2021, I&A doubled the size of its Intelligence Oversight Branch, which provides training and advice on the Attorney General-approved Intelligence Oversight Guidelines. It also conducts compliance inquiries and reviews all of I&A's intelligence products—finished intelligence.

We have hired two career professionals as full-time ombuds, who help resolve individual and organizational concerns in the work force without fear of retaliation.

It is also important to note that DHS's Offices for Civil Rights and Civil Liberties, Privacy, and the General Counsel are all heavily involved in our oversight efforts and review all of our finished intelligence products.

To ensure that our organizational decisions are aligned with our long-term strategy, we are also currently carrying out a 360 review of I&A's activities—and this goes to something that you said, Mr. Ranking Member—taking a look at where we stand today. We are doing that with the help of two distinguished National security professionals who are studying the organization and engaging with stakeholders to ensure that we are adapting and aligning our resources to meet the evolving threats.

Should we identify room for improvement in that process, we will work closely with Congress on the authorities and resources we may need. For instance, with our fiscal year 2023 budget, we have made particularized requests to expand our analytical cadre on a range of growing threats and to invest in technology that we need.

So, to conclude, I want to thank you for your continued support and your continued guidance. As I trust you can see from our summary, I&A remains committed to enhancing partnerships, to reinvigorating our information-sharing efforts, to improving the way we deliver intelligence to our partners, and to maintaining an intense focus on enhancing oversight, training, and morale across the organization.

Thank you for the honor of appearing before you today, and I look forward to answering your questions.

[The prepared statement of Mr. Wainstein follows:]

PREPARED STATEMENT OF KENNETH L. WAINSTEIN

DECEMBER 13, 2022

Chairwoman Slotkin, Ranking Member Pfluger, and Members of the subcommittee, thank you for the opportunity to 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 fiscal year 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, more than 60 percent of I&A's finished intelligence products were produced at the un-Classified 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 policy makers 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

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

fusion centers. Each month, that team also provides a Secret-level threat briefing to our SLTT customers.

The primary mechanism for dissemination of un-Classified products is the Homeland Security Intelligence Network, which provides on-line access to over 50,000 un-Classified 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 2 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 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 6 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 the District of Columbia 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 fiscal year 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 class-

room instructor-led classes, resulting in over 3,000 graduates from the Intelligence Training Academy—a 290 percent increase over fiscal year 2020. Last year, I&A also increased the number of students from other DHS components at the National Intelligence University (NIU) by 57 percent and expanded their enrollment in intelligence community courses by 121 percent.

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 dialog, 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 engag-

ing 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 fiscal year 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 United States (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 un-Classified 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 United States 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 Home-grown 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 on-line. 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 antisemitic 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 on-line 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 on-line presence focused on inspiring HVEs to conduct attacks in the United States. ISIS media outlets, for example, routinely issue on-line 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 cyber-criminal groups, including cyber-enabled espionage and disruptive cyber attacks on health care 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 cyber attack 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 down time. 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 fiscal year 2021, CBP seized 221,000 pounds of these drugs, which was a nearly 40 percent increase over fiscal year 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.

Ms. SLOTKIN. Without objection, I ask unanimous consent to enter into the record a statement by the National Fusion Center Association.

[The information follows:]

STATEMENT OF THE NATIONAL FUSION CENTER ASSOCIATION

TUESDAY, DECEMBER 13, 2022

Dear Chairwoman Slotkin, Ranking Member Pfluger, and Members of the subcommittee: I am pleased to submit this statement for the record on behalf of the National Fusion Center Association (NFCA). The NFCA represents the interests of 80 State and major urban area fusion centers where more than 3,000 local, State, Federal, and private-sector personnel collaborate every day to help protect America while protecting the privacy, civil rights, and civil liberties of all people. The National Network of Fusion Centers (National Network) is the hub of much of the in-

telligence and information flow between State, local, Tribal, territorial (SLTT) and private-sector partners and several components of the Federal Government.

The Office of Intelligence and Analysis (I&A) at the Department of Homeland Security is the only U.S. intelligence community element that is statutorily charged with supporting the National Network (6 USC 124h). A strong, collaborative, and fully-resourced I&A is essential to ensure effective and efficient information and intelligence sharing regarding threats to the homeland, whether the threat is related to terrorism, natural disasters, or other criminal activity.

We are operating in the most dynamic threat environment we have seen since 9/11. It is critical that I&A has steady, experienced leadership who understands the threat environment and how to break down information silos to bring together those with a mission of keeping our country safe. We were proud to support Under Secretary Wainstein's nomination given his noteworthy career in law enforcement and National security. We commend the high importance he has placed on collaboration and partnership with State and local partners. We are appreciative that this emphasis has led to the creation of a new position—the deputy under secretary for intelligence partnerships. We think this position should result in better coordination, communication, and support to all State, local, Tribal, and territorial partners. Ideally, this position should be held by a professional with significant experience in State or local law enforcement intelligence so that opportunities and challenges can be easily translated to the under secretary for I&A and throughout the Office of Intelligence and Analysis.

Enhancing analytical collaboration in the field is essential to the detection, prevention, and mitigation of threats. It is an enduring focus of the NFCA, and the support provided by I&A personnel assigned to fusion centers is critically important. We continue to encourage I&A to prioritize the deployment of well-trained and experienced I&A intelligence professionals throughout the network. We have several gaps around the Nation today, and we call on Congress to provide sufficient funding to I&A each year to enable robust presence of intelligence officers, reports officers, and analysts in the field, including at fusion centers.

We applaud Congress for passing the DHS Field Engagement Accountability Act (Pub. L. 116–116) in 2020 to ensure that I&A presence in the field is strengthened. The law requires I&A to consult with fusion center officials in developing and annually updating a strategy for I&A's fusion center engagement. In our view, deployment of I&A resources to the field to ensure best alignment with the centers' missions and needs is a central part of that strategy.

The NFCA strongly encourages Congress to increase funding for I&A to ensure it can hire, train, and deploy an adequate number of personnel across the Nation. Every State and regional fusion center should have an I&A intelligence professional with the authority to collect and share raw information. Those professionals should have release authority, they should be able to execute joint production, and they should be empowered to efficiently share timely and highly relevant information across all classification levels. Decisions regarding the appropriate type of intelligence professionals for each fusion center and their role within the center should be the result of discussions between those State and regional fusion centers and I&A.

Strengthening I&A's ability to support the National Network also requires I&A to invest in modernizing information-sharing systems and technologies, prioritizing reliable access to critical data, including Classified data, and increasing offerings of high-quality training related to intelligence analysis and privacy, civil rights, and civil liberties.

Analysts throughout the National Network are trained to monitor and contribute relevant threat-related information using the Homeland Security Information Network (HSIN). HSIN is an essential tool for the protection and security of our Nation, but it remains limited by its interface, access requirements, and capabilities. I&A should continue to support the development and enhancement of HSIN and other data and information-sharing systems it maintains.

While we have overcome certain Federal data access issues, the National Network still needs help to break down barriers that are currently keeping information from reaching analysts and decision makers at the local, regional, and State levels who work to protect communities from acts of terrorism and other homeland security threats. A handful of fusion centers still lack access or have trouble accessing critical databases, like the FBI's National Crime Information Center (NCIC) and Treasury's FinCEN systems. I&A can play a supportive role by advocating for appropriate access to Federal systems by State and local partners.

I&A provides important training opportunities for analysts in fusion centers. I&A facilitates the delivery of specialized analytic seminars focused on specific threat topics. The seminars bring together a diverse range of State and local subject-matter

experts and partner agencies from all levels of government to inform analytic efforts. These seminars provide a welcome opportunity for fusion center analysts and their Federal counterparts to discuss emerging threats, trends, and patterns and collaborate on joint products and best practices. State and local partners are eager for more training opportunities, especially in emerging threats like cybersecurity and standing priorities like civil rights and civil liberties protections. More virtual training opportunities would be very helpful since many analysts and centers have adapted to remote working environments, and since State and local budget resources for travel remain tight.

The NFCA supports a strong I&A that is relentlessly focused on strengthening its partnerships and collaboration with State, local, Tribal, and territorial agencies including fusion centers. We encourage Congress to ensure I&A has the right authorities and budget to enable those strong partnerships and to execute our shared mission to protect America from all threats, foreign and domestic.

Sincerely,

MIKE SENA,
President, National Fusion Center Association Director,
Northern California Regional Intelligence Center.

Ms. SLOTKIN. Thank you for your testimony.

I will remind the subcommittee that we will each have 5 minutes to question the witness. We have just a handful of us on, so we will likely be able to do a few rounds.

I will now recognize myself for questions.

So, you know, we are of course interested in morale and training, but could you give us and C–SPAN the meat and potatoes? How many analysts? What kind of production do you have per month? Who is your principal customer?

Then give us some illustrative examples of what you are producing so that people understand not just how your work force is faring but the value proposition for the American people.

Mr. WAINSTEIN. That is a great question. Thank you, Madam Chairwoman.

So, to step back and sort-of take a high-level view to begin with, I&A's value proposition—this goes back to its origins in 2002, when it was first stood up by statute—was to help make sure that all the players in the homeland security enterprise, be they Federal agencies like the intelligence community—DHS, DOJ, FBI—and all our partners out among the State and local law enforcement, territorial and Tribal entities, and the private sector, that we are doing our best to share relevant information across all of those partners.

That is one of the lessons, as you recall, of 9/11, which is that we didn't connect the dots. But connecting the dots was more than just not taking one data point and seeing its relevance to another data point. It was not having the intelligence channeled from one person who had the information to somebody who could act on it. You know, one of the main concerns was that our State and locals were not part of the Federal process of intelligence sharing.

That is our main job. Our main job is as a bridge to the State and locals. That is one of the reasons why my statement for the record and my comments just now focused on what we are doing to cement that relationship, expand our regular communication with State and locals, be they police forces, sheriffs, first responders.

Our analysts—you know, not only are we building those relationships, but our analysts focus on the kind of threat information that is going to be relevant to those partners.

Ms. SLOTKIN. So just help us understand. How many analysts currently work for your shop?

Mr. WAINSTEIN. All told, we have—do we have a final number now?

I thought it was a little over 300. It is somewhere in the 300 range, in terms of pure analysts. I have a work force of about 1,000, including 300 contractors, 700 Feds.

Ms. SLOTKIN. OK. How many pieces of finished intelligence, generally, would you say that that 300 analysts produce per month?

Mr. WAINSTEIN. You know, I don't have that number exactly. So——

Ms. SLOTKIN. Can you give me an example of just one or two pieces that have gone out? Understanding classification, just tell us what you can, so that the average person—my dad, who is sitting at home, who is in the hot dog business—understands what I&A does.

Mr. WAINSTEIN. Happy to. This sort-of follows on from my previous comments. Finding intelligence that is relevant to our State and local partners.

So a "for instance" is: Right in the aftermath of the abortion decision that came down from the Supreme Court—as you recall, it sort-of came out suddenly on a Friday. It was unexpectedly early. We convened a call with all the stakeholders around the country, but we also put a piece out which just raised the concerns about possible violence in reaction to that decision. It explained what we have seen in the past, from which violent actors we have seen it in the past, and what we are hearing now about whether those violent actors are going to react to the decision.

As you recall, it was relatively peaceful. But it was very well-received, because it just sort-of laid out, "These are things to look for."

Similarly, one other example: You will recall the attack on the FBI out in, I believe it was Cleveland, after the Mar-a-Lago situation, where an individual came in and tried to attack an FBI office and then was killed. We also put something out talking about threats to law enforcement around the country, calibrating whether that threat was focused only on Federal law enforcement, the FBI, because of this Mar-a-Lago situation or whether there was a broader threat to other law enforcement.

Ms. SLOTKIN. Uh-huh.

Then, just last: So Mr. Pfluger referenced some of these things in his opening statement. You know, if you are sitting at home in Michigan right now, every single person I know knows someone who has been the victim of a ransomware attack and/or a stolen identity, some sort of cyber threat.

Have you done production on cyber threats? Have you done production on counter-drone threats—or drone threats? The things that sort-of the American people think about as a potential problem, what is the level of production you have done on those things?

Mr. WAINSTEIN. Quite a bit. On the cyber front, we are embedded with and working very closely with CISA on cyber and critical infrastructure in general. But we put out a good bit on cyber.

Put out some products on ransomware, because that is the kind of issue that, you know, the average American really needs to be thinking about.

Ms. SLOTKIN. Uh-huh.

Mr. WAINSTEIN. In fact, in our fiscal year 2023 request, we have asked for more cyber resources because of the criticality of that threat.

Ms. SLOTKIN. Uh-huh.

Then, last, can you describe in as much detail as you can how I&A is handling the issue of domestic terrorism?

Mr. WAINSTEIN. Hugely important question.

We are very focused on domestic terrorism. As you know, everybody from the DNI to the FBI director to Ale Mayorkas at DHS has said that the primary terrorist threat today, the most lethal, sustained threat, is from individuals or small groups here in the United States. We still have al-Qaeda and the foreign terrorist organizations out there who are a real threat, but in terms of lethality right now that is the threat, main threat.

So we are very focused on that, and we see ourselves as playing a critical role in that effort, because domestic terrorism of that type, whether they are domestic violent extremists or home-grown violent extremists, they are the kind of targets where the State and locals are apt to be the first to find out about them. So they need our strategic intelligence to know what to look for out on the street. Then we need to get from them what they are seeing so that we can couple that with intelligence from other parts of the country to zero in on the bad guys. When I say "bad guys," I am talking about people who are engaging in violence.

Ms. SLOTKIN. Uh-huh.

Mr. WAINSTEIN. That is the key, right?

So we are heavily involved in that, including our collection process, not just our analytical process but our open-source collection, where we target a collection against people, once again, who are fomenting violence. This is not spouting political views or religious views; it is violence. So that is an area where we see an expanding role with the expanding threat.

Ms. SLOTKIN. I will come back to that, because I am interested in that collection part. The last time, you know, with your previous acting under secretary, it was more like, I think, two or three bodies had been expanded, but there wasn't any clarity on what exactly was happening, particularly on the collection side.

But I yield to the Ranking Member, Mr. Pfluger.

Mr. PFLUGER. Thank you, Madam Chair.

Secretary Wainstein, I am happy to hear you talk about how the role of I&A is to be a bridge to the State and local.

So I think I will start just with a broad question: I mean, what makes I&A unique in the IC? Where is the most value added of having I&A? What should we, as the American public, be looking at I&A as, "Nobody else does this, and here is why it is critical"?

Mr. WAINSTEIN. It is a great question, sir. I guess I would encapsulate it this way: As I said in response to the Chairwoman's questions, we have the statutory responsibility—we alone have the statutory responsibility to be the intelligence bridge to the State, local,

territorial, Tribal, and private-sector partners around the country. So that is our function.

We have other functions too, and I have listed our various facets of our mission, but that really is the key. So that is what we do. This goes back and addresses the failings, which were sort-of highlighted by 9/11, where we had insufficient coordination between the State and locals and the Federal entities.

So that is really our key mission. That is why, for example, we have created the new position, deputy under secretary for intelligence partnerships, to highlight the need to keep those relationships strong and vibrant.

That is why I mentioned earlier—and I think you actually alluded to this in your opening remarks—we are stepping back right now and doing a 360 review of I&A. What that entails is taking a look at the organization, seeing where it adds the most value to our partners, particularly the State and locals, see where maybe there are other agencies that can handle those responsibilities as well or better than us, and then, if so, consider shifting our resources to an area where we really do add more significant and unique value.

Mr. PFLUGER. I think that is fantastic. That is exactly what we are looking for, to reduce the duplicative nature that Big Government has really become, not just in this area but overall.

Keeping on that statutory mindset, when we look at the authority that you have and the two dozen responsibilities, approximately, that the office has, I personally have not seen an explicit provision for collection on open-source data.

I would like you to elaborate on the authorities and the justification drawn from the Executive Order 12333, if you will, to build out such a large collection capability and why I&A has strayed into that area of open-source collection vice focusing on the two dozen other authorities.

Mr. WAINSTEIN. Good question, sir. This sort-of goes to what we alluded to in our earlier conversation about how we should focus our resources in those areas where we add value.

So, statutorily, we are authorized to do intelligence work against the threat, the homeland security threats, and consistent with the departmental or national mission. In terms of 12333, we are allowed to do open-source collections but it is overt and it is only gaining access to publicly available information. So we have no covert means at our disposal. So that is a very important caveat.

We have an open-source collection office of about 10 people and 1 supervisor, I believe is the number now. So it is not huge, but it is consistent with our authorities. We have very heavy oversight, and part of that is an outgrowth of the situations you talked about earlier, where we had Portland and the January 6. The lessons learned from that resulted in us embedding an oversight officer in the open-source collection group to make sure that they were available to answer all questions, because that can be a dicey area. You are talking about privacy interests, even though it is publicly-available information.

So we do have the authorities. We are exercising them with strict oversight and fidelity to the oversight guidelines that were authorized by the Attorney General. We are doing so pursuant to Depart-

mental missions, in particular to, you know, terrorism and other National security threats.

Mr. PFLUGER. If we get to a second round of questioning, I will go down a path that deals with some of those last points.

Do you believe that there is a—and thank you for the answer. Thank you for the review. Because I think it is critical that we do this 360 review, that we get to a point where I&A has an area where you are focused and you are adding value to the IC where no other organization can do, at the level that you intend to, these types of jobs.

But do you believe that there is a question, a public question, or a perception problem with some of our intelligence-gathering apparatus, the IC in general, when it comes to that line and that friction point of privacy?

Mr. WAINSTEIN. I think that is inherent in intelligence collection domestically. I mean, we are a democracy. Our Government operates best when it operates transparently. By definition, some of the intelligence enterprise is conducted clandestinely, not transparently. As a result, there is always concern and there should always be intense scrutiny on the activities of the intelligence community, especially when they are focused internally here in the United States.

I will say that, be it here or before the Intelligence Committees when I have been testifying, my mantra has been: Give us the authorities, give us the resources, but give us the oversight responsibilities. Impose oversight. Because the best situation is where both Congress and the American people have the means and have comfort that the authorities they are giving to their intelligence community are being used appropriately.

Mr. PFLUGER. Thank you.

I yield back.

Ms. SLOTKIN. The Chair recognizes the gentleman from the great State of Michigan, Peter Meijer.

Mr. MEIJER. Thank you, Madam Chair.

Thank you, Mr. Under Secretary, for being here.

I just want to ask quickly, on the National Terrorism Advisory System, you know, replacing that color-coded HSAS system from the immediate post-9/11 period—but we continually state and use the phrase "heightened threat environment." Heightened and heightened.

As anyone who travels through the airport also knows, you know, we have the TSA liquids rule, that 3.4-ounce maximum. Originally in 2006, after we foiled that plot to have liquid explosives on airliners, that was initially supposed to be temporary, right?

The ratchet goes in one direction. I am just curious—from a general standpoint, if it is heightened, it is heightened relative to a baseline. Is that baseline pre-9/11? Is that baseline just some sort of fantasy of safety that we have had?

Would you ever see your Department putting out an advisory that says the threat environment has diminished or that we are returning to a baseline?

Mr. WAINSTEIN. Well, thank you, sir. I appreciate the question. Very nice to meet you.

That is an excellent question. I will say, personally, I was in Government dealing with the post-9/11 response up until I left, inauguration day of 2009, came back in after 13 years, and that is one of the questions I had. I had the sense that the level of concern about terrorism had diminished in relation to other threats, but I wasn't sure about that ratchet issue.

I don't know that I have an absolute answer in terms of what will happen in the future on that. But I think one thing that might be illustrative is the most recent bulletin that we put out. It just went out 2 weeks ago.

We debated, you know? OK, so we don't have any triggering event that suggests that there is a threat that is heightened over what we announced in the last bulletin 6 months before, but it is still at a heightened level.

So what we tried to do is make very clear that we are putting that out as a bulletin—in other words, as an update—not as an alert, "Hey, everybody, take note of this. We see this credible evidence that there is a new threat, or a newly heightened threat." Rather, "We are still in a heightened threat environment."

Given what we have seen of late, I think that is the case, that we are still heightened. But that sort-of ducks the question a little bit of, heightened from where? I take your point that maybe at some point we should step back and say, maybe today we are in a new reality, and sort-of recalibrate that system.

Mr. MEIJER. It is probably an unfair question, but just that question of, where do we establish a baseline? I mean, you still walk into stores and there are "mask required" posters up on the wall, and nobody is wearing a mask, right? I mean, it is that——

Mr. WAINSTEIN. Uh-huh.

Mr. MEIJER. It becomes the intelligence advisory bulletin that cried wolf. You know, it just fades into the background, and then risks not being received.

But, again, that is just something I always keep in the back of mind on the intelligence side. Because it is so easy to put out an advisory. It is very difficult to—well, it is easy to say, be worried or be cautious. It is very hard to then face the consequences if you are wrong and there was a risk that hadn't been appreciated.

But just quickly on the clandestine intelligence collection side of the house, can you speak to how I&A deconflicts the various streams coming in and avoids circular reporting, which I think especially in the clandestine realm, given the necessity of protecting source information, is especially an acute risk?

Mr. WAINSTEIN. So, good question about the deconfliction. There is always a concern about deconfliction when you have multiple agencies—frankly, multiple actors within individual agencies doing intelligence work on the same target.

Just to be clear, we do not do clandestine work. We work very closely with the Bureau—that is probably the main place where that opportunity might arise—to make sure that they know what we are looking at, we know what they are looking at, and, to the extent that they, let's say, have an investigation going on, that we don't issue anything that would be problematic for the integrity of their investigation.

But since we are not running sources, you know, in the classic sort-of clandestine way or using covert means, it is a little less—that specific issue is a little less of a concern for us.

Mr. MEIJER. OK. So largely dependent on the FBI, or whoever that clandestine authority is, to be pursuing their own deconfliction, rather than on the analytical back end?

Mr. WAINSTEIN. Right. What we do on the analytical back end is, if we are, let's say, getting intelligence from NSA or the FBI that is, you know, covertly collected intelligence, you know, we make sure to deconflict with them to the extent of making sure we are not disclosing something, either in a Classified or un-Classified forum, that could be problematic. So we do do that.

But we draw on their intelligence, put it into a format that is appropriate. Sometimes we then downgrade it, because one of the—back to our sort-of original function of trying to serve the State and locals, oftentimes we will take Classified and downgrade it to un-Classified. Obviously, we need to get their opinion on the appropriateness of that downgrading.

Mr. MEIJER. I see our Chairwoman is not here for the moment, so I will just say in—I just want to make sure, from a terminology usage, "clandestine," where, you know, the role is masked, versus "covert," where it is never acknowledged, in terms of the ultimate source of the information or the ultimate collector of that information.

But I guess I will yield to our Ranking Member, Mr. Pfluger. There you go.

Mr. PFLUGER [presiding]. The Chairwoman has stepped out momentarily. So we will proceed with the second round of questions, and when the Chair returns, we will hand it back. But I now recognize myself for another 5-minute questioning period.

Thank you for the first round of, you know, where your mindset is.

I would like to shift gears a little bit and understand what you believe the definition of "domestic terrorism" or "domestic violent extremism" is.

Mr. WAINSTEIN. Sir, that is a good question, and I think it is very pertinent. We have to constantly remind ourselves of that.

One of the purposes of this oversight apparatus that has really developed over the last couple years—and it is quite comprehensive. I would invite you, you know, to ask further questions about that or come see it. But one of the main purposes of that is to make sure that, in the terrorism space, that we are only collecting, we are only monitoring, we are only issuing intelligence when it comes to the possibility of violence.

So, in terms of domestic terrorism, as I mentioned earlier, we have domestic—well, home-grown violent extremists, who are home-grown extremists who were inspired by foreign terrorist organizations or foreign terrorist rhetoric. Then you have domestic violent extremists, who are U.S.-based individuals or small groups who get radicalized without inspiration or without direction from overseas.

Both are legitimate targets for intelligence collection and production for I&A. But the key is—and this is where the rubber meets the road in terms of our ability to act on it—is, it can't just be

somebody who is talking about an extremist political view. That is perfectly protected by the First Amendment. It can only be somebody who is coordinating, moving toward, discussing the possibility of violence. That is the key element in the definition of the type of domestic terrorism that we can collect on.

Mr. PFLUGER. Well, thank you for that, and I think it is important. In your 360 review, I would implore you to make sure that the people that are assigned as officers or employees of I&A understand that and make sure that—the rhetoric that we hear at times is not helpful on a political level but it is not helpful for our country either.

You know, when you get to some of the threats that we have seen—you mentioned the *Dobbs* decision. Do you believe that the threats that were made against certain religious organizations or pregnancy help centers in that aftermath were terroristic?

Mr. WAINSTEIN. Yes. If you look at the definition of "terrorism"—threats or acts of violence intended to shape public opinion or influence policy—there were such acts, yes. In fact, I think the document, the report that I mentioned earlier highlighted some of those.

We have done a lot with the faith-based community to discuss these threats, the possibility of them. Whether related to that particular Supreme Court decision or not, we have seen a lot of faith-based victimization over the last few months.

Mr. PFLUGER. Oh, we certainly have. Obviously, the antisemitic comments and violence that has played out in places like New York City and otherwise are extremely harmful.

You know, kind-of getting back to—and thank you for those answers.

As you look at your work force, something that was previously mentioned, can you kind-of talk to us about maybe the breakdown of the skills, the growth rate from 2002 until now of I&A and where those positions—I think you said you have 300-ish analysts. You know, what are the skill sets that you have hired? What is that, you know, growth rate over the past 20 years on a year-to-year basis, if you know that?

Mr. WAINSTEIN. A good question. That is something that I am learning as I am getting into this position, learning the history.

I will say, a number of my predecessors did a very good job of bringing in and recruiting strong people. We have really strong analysts. I mean, that is one thing I have been impressed with since I have come on board. These are people who care a lot. They know a lot. They work well with other agencies, which is really a key element of the job description at I&A—you have to be able to work well with other agencies—and are smart analytically.

But I will say that we have really ramped up the training program over the last few years. I have gone back and looked at the same reviews and reports about Portland and January 6, and there were concerns about the sufficiency of the training. That is one reason I highlighted this and one reason I have appreciated this committee and Chairman Thompson's focus on training over the last few months, and so I have been engaging with the committee. Because that is the key.

Mr. PFLUGER. Uh-huh.

Mr. WAINSTEIN. I mean, you can bring smart people in—and we have a tremendously successful internship program that brings these whip-smart young kids in in college, they work for the summer, and then a high percentage of them come on board permanently. They are great. They are a great raw material, but it needs to be shaped. That takes training and experience and mentoring. So we are really focused on that.

Mr. PFLUGER. Do I have 30 seconds?

Do you believe that MAGA supporters are terrorists?

Mr. WAINSTEIN. No. A MAGA supporter, in and of itself, is not a terrorist at all. A terrorist is somebody who seeks to use violence or the threat of violence to shape public opinion, to influence policy. I can tell you that at I&A we are very focused on that concern.

Just to broaden the question out here, the issue, the challenge here is that a good bit of domestic terrorism grows out of political views. That is inherent in your question, obviously. The challenge for the intelligence community and law enforcement community is making sure that you protect the right of people to believe whatever they want, at either end of the spectrum, as extreme as they want to believe, and only focus on those people who take those beliefs over the line to radicalization and violence.

Mr. PFLUGER. I am looking forward to telling my 90-year-old grandmother that she is not a terrorist, and I appreciate your answer.

I yield back.

Ms. SLOTKIN [presiding]. Thank you.

Sorry. I had to step out for a final vote in another committee.

Staying on the topic of domestic terrorism, right, I am of the belief, I think as you are, that, no matter who you are, on the left or the right, if you are espousing violence, that is where your freedom of speech ends, and you should be held to account, no matter what your views, if you are threatening or using violence against other American citizens.

But there is also a ladder of escalation that people climb, short of violence, that is indicating behavior of a problem.

In Michigan, we have had double the number of antisemitic incidents in the past year, in 2022. My own synagogue just had an incident last week where a man came and stood outside, screamed, "Death to Jews." This is the place where my grandparents helped build this place. When the police officers pulled him over afterwards, as long as he didn't have a weapon, he was good to go, and they fist-bumped him, and he went on his way.

We are having a huge community conversation about this in metro Detroit tomorrow. When I go to understand antisemitism and the rise of incidents in my State, I don't go to the Department of Homeland Security I&A. I go to the ADL, I go to other organizations.

So tell me what production you have done on things that may be short of violence but are indicators that violence is on the increase.

Mr. WAINSTEIN. That is an excellent question, Chairwoman Slotkin, as it relates to how you identify somebody who should be looked at, but how do you do that without monitoring someone who is just exercising the right to free speech.

We actually have been involved in putting out a set of indicators, radicalization indicators, to all, you know, our partners around the country to help them identify those things that suggest that somebody might be radicalizing toward violence.

It is a truism in our country that you are allowed to speak your mind and your opinion, even if that opinion is abhorrent, so long as it doesn't foment violence and is not intended to coordinate violent attacks.

So, in addition to those indicators, we have put a good bit of effort in the houses-of-worship area, because they have been a target recently. I think Ranking Member Pfluger just mentioned the New York situations recently that we have seen. We can get you the products that we have done on that. Happy to do so.

Also, I have been involved working with a number of faith-based groups, and we actually have a DHS-level faith-based group that draws on members from all around the country to talk about these issues. I have been focused on that in particular in the antisemitic area, where it has been—you know, we have heard a number of these hate crime incidents recently.

Happy to get you those materials, though.

Ms. SLOTKIN. Yes, and I am happy to take them.

I guess my point is, we are having this huge community meeting tomorrow, which unfortunately I have to miss because I am voting, but it includes, obviously, the local community. The FBI will definitely be there. Our attorney general will definitely be there. The ADL will definitely be there. What—I mean, is the Department of Homeland Security not part of that conversation?

I guess it just strikes me as like, if you want to be relevant and be in the game, it is not just about handing someone a piece of paper or a finished intel piece kind-of to show that you have done the work, but it is to push it out and make it available to a wider audience.

As the Chairwoman of a committee, the fact that I go to non-Governmental agencies to learn about the Proud Boys—which we had a real problem with. My district is where the raids happened for the plot to kidnap and kill my Governor, right?

Mr. WAINSTEIN. Uh-huh.

Ms. SLOTKIN. So it is a real thing for us on the ground. But the Government agencies—I understand it is a sensitive issue, but I couldn't feel more strongly about the importance of you all getting left and right limits, being really clear about it, and then coming up to proactively talk to us about this issue.

Because no one wants to go after someone for free speech, but when you have had double the incidents of antisemitism in my State, the question remains, like, what is my Government doing to help my population?

So I would just put that on your radar. Having it in your back pocket is not as useful as being at the table.

Mr. WAINSTEIN. No, I take your point. In fact, what I was trying to say earlier about how we have enhanced our engagement with our partners, a large part of that is with the faith-based partners.

There is not a First Amendment concern with us going out and explaining to organizations like the ones you cited and explaining what we see as, you know, mobilization indicators or radicalization

indicators. Which is to say, we put a product out, but we actually do try to get out to the table.

So, if you have meetings and you don't see us there or somebody, one of our people at the fusion centers—where you have now people at, you know, almost all our fusion centers around the country. I have been spending a lot of time—I was just out with the folks in the field in Texas, and they are very embedded with the local groups, including the faith-based groups. So——

Ms. SLOTKIN. Well, we will be——

Mr. WAINSTEIN [continuing]. Let us know.

Ms. SLOTKIN [continuing]. Looking for the DHS presence at this large community meeting tomorrow in the metro Detroit area.

Mr. WAINSTEIN. OK.

Ms. SLOTKIN. I yield to Representative Meijer.

Mr. MEIJER. Madam Chair, I just asked a question, but I am happy to yield to Representative Langevin, who I believe is also on the line.

Ms. SLOTKIN. Sure.

The Chair yields to the Representative from Rhode Island, Jim Langevin.

Mr. LANGEVIN. Thank you, Madam Chair. I am going to hold on questions for now. I just joined the hearing. I was in the House Armed Services Committee mark-up, so just joined, and I will hold on questions for now. Thank you.

Ms. SLOTKIN. OK.

I think, with that, anything else from my peers here?

We are very keenly aware that we have two intel officers and one military officer staring you down. We could, no doubt, go with you all day on these issues, but, in fairness—just checking with Ranking Member, are we good to go?

OK.

I appreciate your time in coming down here. We will enter into the record your opening statement.

I would just offer, since this is the first time you are appearing in front of this committee—it will be changing hands come January—that many of us serve on various committees, and there are agencies and departments that are proactive about coming to Congress, and there are those that wait to be asked. Given the IG reports, given the sort-of short history on I&A, my strongest recommendation, particularly on domestic terrorism issues, is to come up early and often, be open kimono about your rules and left and right limits, and help this staff understand.

Because, as you see, it is a sensitive issue, kind-of both ways. We want you to be doing this work, but we don't want you to be violating anyone's freedom of speech. So your help in being proactive in the next Congress would be appreciated, okay?

Mr. WAINSTEIN. You can count on that. Thank you very much.

Ms. SLOTKIN. Thanks very much. Thanks for coming.

Mr. LANGEVIN. Madam Chair?

Ms. SLOTKIN. Oh, yes, Representative Langevin?

Mr. LANGEVIN. Yes. I didn't realize we were going to be adjourning. If it is OK, I will go with two questions.

Ms. SLOTKIN. Sure. Sure. Please, go ahead.

Mr. LANGEVIN. OK.

So, in July, DHS OIG released a report entitled "The Office of Intelligence and Analysis Needs to Improve Its Open Source Intelligence Reporting." The report was the result of an OIG audit to determine the extent to which I&A has an effective process for managing and collecting open-source intelligence for operational and intelligence purposes.

So the OIG found that, while I&A has made recent efforts to address challenges related to insufficient guidance and technology, additional processes improvements are needed to ensure effective intelligence reporting.

So, if we could ask, you know, what steps were taken to address the issue, and do those steps involve plans to draft new policies, revise training, and upgrade technology?

Mr. WAINSTEIN. Thank you, sir.

Yes, the open-source office is one of the areas of our intense focus for two reasons: No. 1, because there were issues that were spotted there in the context of the Portland and Capitol attack situations; but, No. 2, because they are going to be so critical to so many of the threats that we deal with in the future. We just talked about domestic terrorism as one of them.

So, before I got there, many steps had been taken to enhance training. There is a mandatory open-source training class that was instituted, very comprehensive. We embedded an intelligence oversight officer down there among the 10 or so people who are on that group to give them sort of hands-on, direct, immediate guidance on the various issues about privacy that they encounter day in and day out.

We actually have—and this is, once again, before I got there—assigned the members of that group to particular portfolios so they get to understand the issues, aren't just generalists, but they are focused on particular threats so they become more expert, they are more able to, like, separate the wheat from the chaff.

We are also looking at resources. One of the issues that I do want to talk to Congress about, both now and in the future, is how we would deploy more resources for that group if and when we need to to deal with the different threats, many of which are carried out over social media and through publicly-available information.

So that is an area of intense focus, and happy to keep you, sir, and Congress informed of what we are doing on that front.

Mr. LANGEVIN. Thank you. Thank you for that answer, and look forward to having that follow-up.

Let me shift gears for a minute, now switching over to a cyber issue. How does the Cyber Mission Center within the Office of Intelligence and Analysis coordinate with the Cybersecurity Infrastructure Security Agency, or CISA, in the delivery of cyber intelligence products? Because I think that kind of coordination is really important, and I would like you to help us understand how that fits.

Mr. WAINSTEIN. That is actually an important sort-of operational question that occurred to me as soon as I started looking into I&A, before I was even, I guess, nominated.

CISA uses a good number of our analytical resources. We have analysts embedded over at CISA doing cyber work and cyber, you

know, threat intelligence work, and we work with them. I actually had a call with Jen Easterly before I came on board to talk about how that works, whether that is the most sensible approach or whether it makes more sense for CISA to have their own organic intelligence cadre.

To date, the reports we get from both operationally within CISA and from our people is that that relationship works really well. We bring the analytical expertise, CISA has the innate cyber expertise, and it works well, and we are getting the information out.

We actually—I just talked to Jen about this 3 days ago, and some of our colleagues had a meeting yesterday on this very issue, as to sort-of exactly how that deployment should work. So we are looking at it fresh just to make sure that in that absolutely critical area we are putting our best intel foot forward.

Mr. LANGEVIN. Thank you for the answer. I mean, that kind of coordination is very important. It really needs to be seamless. We get, obviously, a better product out of coordination. So I thank you for the work that you are doing.

With that, my time has expired, so I will yield back. Thank you.

Mr. WAINSTEIN. Thank you, sir. Appreciate the questions.

Ms. SLOTKIN. Thank you, Mr. Langevin.

I see Representative LaTurner has come on.

Representative LaTurner, would you like to ask a question?

OK. We will come back to him.

Representative Jackson Lee, you are recognized for 5 minutes.

Well—Ms. Jackson Lee, are you there?

Or Mr. LaTurner?

Going once, going twice.

Okay.

Any other further questions here?

Okay. Unless I hear from one of the two folks who are on screen who are not asking to be recognized, the Members of the subcommittee may have additional questions for the witness, and we ask that you respond expeditiously in writing to those questions.

The Chair reminds Members of the subcommittee that the record will remain open for 10 business days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 10:59 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN BENNIE G. THOMPSON FOR KENNETH L. WAINSTEIN

Question 1. In recent years, I&A has been plagued by reported abuses and politicization of intelligence, to include the previous administration's pursuit of tailored information to support its agenda regarding the Southwest Border.

How are you working to prevent future political interference? More specifically, what internal controls have been established for producing, reviewing, and sharing objective intelligence products?

Answer. The U.S. Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A) has implemented and updated a number of internal controls to ensure intelligence analysis is objective and free from political consideration. To educate the workforce, the analytic ombuds engages new analysts in the on-boarding process to communicate their role in the organization and to discuss politicization in analysis. Over the last year, we developed an e-learning module on Analytic Politicization using real-world events as a case study; this module has become mandatory training. Additional outreach to the analytic workforce includes listening sessions, webinars, and marketing and maintaining a website with resources available to all staff. The analytic ombuds meets monthly with senior leadership to keep them apprised of trends, distributes the Office of the Director of National Intelligence (ODNI) annual Analytic Objectivity and Process survey to analysts, and is the I&A representative of the Intelligence Community (IC) Analytic Ombuds Community of Practice, established August 2022, attending regular meetings with IC counterparts to discuss best practices. Based on recommendations from the DHS Office of the Inspector General (OIG) and under the guidance of the research director, I&A also has adapted its processes and procedures for producing finished intelligence to prevent attempts to politicize I&A analysis.

Question 2. In June, I sent you a letter detailing my concerns regarding several reports that found that analysts lacked appropriate training.[1]

I appreciate the detailed response and I understand I&A is working to address the training issues.

I believe that the good progress you have made on this should be codified and that more needs to be done to ensure I&A's employees receive the necessary training to guard against and mitigate the myriad of threats facing our country. I plan to introduce legislation to do just that. Will you commit to working with me to advance this legislation to ensure I&A has properly-trained personnel?

Answer. I&A remains committed to working in a collaborative and transparent way on all matters of interest to the committee, including on its ideas for enhancing the quality and comprehensiveness of our training. I&A has undertaken the following measures to improve its training:

- I&A developed a series of refresher oversight training sessions in partnership with the Office of the General Counsel (OGC). These cover I&A's authorities, application of the Intelligence Oversight (IO) Guidelines, whistleblower protections, and some of the discrete Constitutional and statutory considerations that I&A collectors faced while working on the Portland situation during the summer of 2020.
- Last year, I&A created a new mandatory training program for all new open-source collection officers, which includes reinforcement about the types of information I&A can and cannot collect and the procedures for disseminating this information to appropriate stakeholders.

[1] *Report on DHS Administrative Review into I&A Open Source Collection and Dissemination Activities During Civil Unrest Portland, Oregon, June through July 2020,* Department of Homeland Security Office of General Counsel, January 6, 2021, *http://cdn.cnn.com/cnn/2021/images/10/01/internal.review.report.20210930.pdf.*

- I&A is providing training webinars for its analysts on the conceptualization of finished intelligence products and I&A's Analytic Tradecraft Evaluation program to reinforce ODNI tradecraft standards.
- I&A has expanded training opportunities for intelligence personnel in other DHS components and among our State, local, Tribal, and territorial (SLTT) partners.
- In fiscal year 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 percent increase over fiscal year 2020.

Question 3. In your testimony, you wrote that "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." Please describe how this centralization differs from the current review process and what the expected benefit is.

Answer. Under the Research Director, I&A has instituted an executive-level review of I&A finished intelligence products to ensure that I&A's analysis is objective, timely, and relevant to homeland security stakeholders. This transition has helped restore uniform, multi-level quality review of finished intelligence products and mirrors best practices in other IC agencies.

Question 4a. In your testimony, you also wrote that "In March 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."

What is the status of that effort?

Question 4b. Does I&A's lack of authority to direct component intelligence impede the Department's ability to produce strategic level intelligence?

Answer. I&A is working with the Office of Privacy, the Office of Civil Rights and Civil Liberties, and OGC to finalize implementation plans that include:

- Designating types of products that require review,
- Establishing processes for immediate review of certain products,
- Updating DHS intelligence enterprise production standards, and
- Determining additional resource requirements and proposals.

Collectively, we are working with DHS components to develop individualized plans to account for variations in authorities, resources, and oversight requirements.

Question 4b [sic]. Does I&A's lack of authority to direct component intelligence impede the Department's ability to produce strategic-level intelligence?

Answer. The existing statutory framework attempts to strike an appropriate balance between I&A's consultative role to lead Departmental intelligence activities and the DHS operational component heads' discretion to employ intelligence personnel and resources to support their respective mission requirements. As the Department's chief intelligence officer, the under secretary for intelligence and analysis is required by statute and by DHS policy to, among other things, "coordinate and enhance integration among the intelligence components of the Department, including through strategic oversight of the intelligence activities of such components" and to "establish the intelligence collection, processing, analysis, and dissemination priorities, policies, processes, standards, guidelines, and procedures for the intelligence components of the Department, consistent with any directions from the President and, as applicable, the Director of National Intelligence." (6 U.S.C. § 121(d)). Each DHS intelligence component, in turn, has a reciprocal statutory obligation to, among other things (and consistent with guidance issued by the director of national intelligence), ensure that their intelligence activities "are carried out efficiently and effectively [and otherwise] in support of the intelligence mission of the Department, as led by the under secretary for intelligence and analysis." (6 U.S.C. § 124d)

Question 5a. On December 13, *Yahoo News* reported on a domestic terrorism analyst at I&A's account of being met with resistance when the analyst attempted to warn of the January 6, 2021 attack before its occurrence.[2] According to the report, "[t]he analyst was told to send an official Request for Information to the open source collection office . . . This tasking was essentially a way to turn what the analyst saw on-line into official Government reporting that could be sent out to law enforcement partners in raw intelligence reports that could be used to produce broader in-

[2] Jana Winter, "Exclusive: An intel analyst tried to prevent the Jan. 6 attack—but DHS failed to act," Yahoo! News (December 13, 2022), *https://news.yahoo.com/exclusive-an-intel-analyst-tried-to-prevent-the-jan-6-attack-but-dhs-failed-to-act-190922453.html.*

telligence assessments to warn local, State, and Federal agencies about an emerging threat."

Please describe the official process for taking information that a collector or analyst receives or uncovers and turning that information into an intelligence report for dissemination to partners.

Answer. When an I&A open-source collection officer receives information from another office within I&A or an external partner, the collection officer reviews the information to ensure that the information is publicly available and responds to a validated collection requirement. If the information meets this threshold, the collection officer will generate an Open-Source Intelligence Report (OSIR). Once written, the OSIR is reviewed by a peer, a senior collection officer, and finally a supervisor. Upon completion of all reviews, the supervisor publishes and disseminates the OSIR to customers with need to know.

Question 5b. Was the analyst who uncovered the information prohibited from producing the raw intelligence report for dissemination? Why was it necessary that the analyst had to send a Request for Information to the open-source collection office?

Answer. I&A Mission Centers do not have a separate open-source reporting and dissemination function. Additionally, analysts are not trained or certified to collect and disseminate raw intelligence information. Only I&A officers who are trained and certified to release such information, such as an open-source collection officer, can disseminate a raw intelligence report. Analysts produce finished intelligence products that analyze raw intelligence and use analytic tradecraft to assess the impact of that information.

Question 5c. The reporting indicates that a new process for submitting requests delayed action on it. When was the new process initiated? What was the reason for the change? Please describe how the new process deviated from the process before.

Answer. As noted to the journalist, some of the information provided in this article is mischaracterized or factually inaccurate. I&A did not create a new process for submitting requests.

Question 5d. Why was the analyst's note that this request was a time-sensitive/urgent matter not heeded?

Answer. On December 29, 2020, I&A analysts sent open-source collectors a request for threat information regarding January 6 events and noted the request was urgent, after which the collectors researched possible threats. There were several reasons why OSIRs on possible threats were not published, including concerns that the information did not meet the threshold for reporting under I&A Attorney General guidelines and hesitancy to report information following scrutiny of I&A's actions in Portland, Oregon in the summer of 2020, as noted in the DHS OIG report OIG–22–29 on I&A actions related to the January 6, 2021, U.S. Capitol breach, dated March 4, 2022. I&A concurred with the OIG recommendations in this report and in OIG–22–50 on I&A improving its open-source intelligence reporting and continues working to address these issues.

QUESTIONS FROM CHAIRWOMAN ELISSA SLOTKIN FOR KENNETH L. WAINSTEIN

Question 1a. The Office of Intelligence and Analysis plays a critical role in protecting the American people from harm by analyzing and disseminating timely threat information that allows those on the front lines—our State, local, and Tribal law enforcement partners—to adequately prepare for and neutralize threats. I&A is unique in that it is the only member of the intelligence community statutorily charged with delivering this information to these partners.

You testified that the Department was conducting a 360-degree review of I&A and attempting to recalibrate the office.

What is the status of that review and explain the steps you are currently taking to better articulate I&A's mission and its unique statutory role of delivering intelligence to State and local partners?

Question 1e. To what extent has the 360-degree review taken into account actions needed to implement the 2021 National Strategy for Countering Domestic Terrorism?

Answer. The review is on-going, and the most immediate product of that review is the delivery of recommendations to the deputy secretary, which are near completion. We are considering several proposed organizational changes based on feedback from the workforce, external reviews and audits, advice from former National security officials and I&A leaders, as well as IC best practices and the work that was done at I&A throughout fiscal year 2021 and 2022. We intend to formally request approval from the deputy secretary in the second quarter of fiscal year 2023, and then will begin assessing I&A's substantive mission areas under the prospective leadership structure later in fiscal year 2023.

The review is carefully considering that preventing and mitigating terrorism, including domestic terrorism, is a critical part of I&A's core mission (see Section 111 of the Homeland Security Act), as well as the DHS activities and responsibilities outlined. The administration's strategy for carrying out the domestic terrorism part of that mission is set forth in the 2021 National Strategy for Countering Domestic Terrorism. One of the priorities for DHS in that strategy is to advance I&A's support for policy makers and operational officials, including State, local, Tribal, and territorial officials, with their responsibilities for preventing, mitigating, and responding to domestic terrorism.

Question 1b. How do you measure the impact of I&A's products and other efforts on State, local, and private-sector partners, as well as on the intelligence community?

Answer. I&A collects and reviews production data related to dissemination/classification accessibility, viewership, citations, evaluations, and customer satisfaction feedback to develop a holistic view of its impact on SLTT and IC partners. We also keep in constant communication with our customers to identify emerging partner requirements.

Question 1c. What performance feedback do you collect from your customers and how do you use that information to better meet their needs?

Answer. I&A utilizes a customer feedback form appended to each finished intelligence product to reach a diverse range of recipient organizations at all levels of government and solicit customer perspectives (e.g., satisfaction ratings regarding the timeliness, relevance, usefulness, and responsiveness of a product).

Question 1d. Setting aside products that I&A creates, how does I&A foster intelligence-sharing throughout the broader homeland community?

Answer. I&A was established to fill a void that existed within our Nation's intelligence- and information-sharing architecture between Federal, SLTT, and private-sector partners. In support of this mission, I&A manages strategic relationships with key partners, including across Federal, SLTT, and private-sector stakeholders. I&A is committed to working closely with these partners, including the sharing of timely and actionable information to ensure they have the information they need to keep our communities safe. I&A systematically establishes and leverages these partnerships to promote multidirectional intelligence and information sharing; collaborates with key partners to build mutually beneficial relationships; facilitates the identification of partner requirements and needs; enables partner access to I&A products, resources, and expertise; and advocates partner equities across I&A in support of their respective Homeland Security missions.

Additionally, I&A has deployed over 130 intelligence professionals across the country to directly collaborate and share intelligence with their Federal, SLTT, and private-sector partners. These individuals focus on sharing actionable intelligence with our partners and are also responsible for ensuring our partners can expeditiously access the capabilities, resources, and expertise necessary to share information and intelligence and serve as full participants in the homeland security intelligence enterprise.

Question 2a. Unlike many other members of the intelligence community, I&A does not have a discrete mission—rather your mission is broad, requiring that you cast a wide net around intelligence needed to protect the homeland and prevent terrorist attacks.

How does I&A develop its intelligence priorities?

Answer. I&A is a unique member of the U.S. IC and is the only IC element statutorily charged with delivering intelligence to SLTT and private-sector partners and developing intelligence from those partners for DHS and the IC. This is at the core of why Congress established I&A, in part to fill a void that existed within our Nation's intelligence- and information-sharing architecture between Federal and SLTT partners. I&A uses a comprehensive framework of intelligence topics and subtopics, the DHS information needs, that corresponds to a National IC framework but also includes DHS-specific topics and subtopics. We use a process, Intelligence Threat Banding, to evaluate the overall impact of threats to the homeland and the extent to which we understand them from an intelligence perspective. For example, a high-impact threat on which there are many intelligence gaps is prioritized higher than a low-impact threat with few or no intelligence gaps. The results of this process are used to inform the Program of Analysis, which encompasses I&A's most strategically significant analytic production, and more generally to calibrate levels of effort across functional analytic portfolios and collection requirements office-wide. I&A also prioritizes short-term production and collection requirements dynamically based on emergent threats and in response to Departmental leadership direction.

Question 2b. How do these priorities relate to the authorities and priorities of other agencies within the intelligence community?

Answer. I&A priorities represent DHS Enterprise customer needs and ultimately drive production and collection requirements to address those constituencies. Any IC or other agency (e.g., DHS components) that provides information responsive to I&A requirements either as a result of an intelligence activity or collected incidentally as a result of operational activity does so under its own authorities, just as I&A collects intelligence only as consistent with our authorities. In many instances, I&A and national IC priorities coincide where there is specific authorized mission overlap and/or I&A has a specific capability or access that can lead to responsive intelligence reporting. When this occurs, the I&A collection activity and its associated raw reporting is conducted in accordance with our authorities and disseminated to authorized IC recipients.

Question 2c. How do I&A's written products and activities, such as briefings, align with its intelligence priorities?

Answer. I&A's intelligence priorities determine its organizational structure and require the development of subject-matter expertise in various functional analytic portfolios, the result of which is inherent alignment of written products and briefings with National, Departmental, SLTT, and private-sector customer needs. Analysts undertake substantive intelligence work only after they and their leadership determine that it addresses an authorized mission reflected in I&A priorities and consistent with oversight guidelines.

Question 3. The Domestic Terrorism Analytic Branch was established in March 2021, however, the committee has received very little information on how exactly the creation of the discrete branch has improved the Department's understanding of the rising threat of domestic terrorism and subsequently, the Department's efforts to combat the threat.

Please describe I&A's progress and accomplishments under the branch and what specific metrics have been developed to evaluate success, including the improvement of our understanding of the Domestic Terrorist threat.

Answer. I&A has been able to vastly improve its ability to directly support SLTT and private-sector customers, as well as senior DHS leadership's intelligence information needs on domestic terrorism—a consistent high-priority requirement for most customers. Providing dedicated support to this effort has allowed us to focus analytic efforts on the full range of domestic violent extremist threats and issues. Since 2021, I&A has authored or co-authored more than 100 finished intelligence products addressing domestic terrorism issues. In particular, I&A has taken the lead on assessments on topics such as possible threats associated with the anniversary of the Capitol breach, targeting of the health care sector, threats to the Nation's electrical grid, threats associated with the U.S. Supreme Court's decision in *Dobbs* v. *Jackson Women's Health Organization,* and threats to potential U.S. border policy changes. I&A also has co-authored a number of Joint Intelligence Bulletins and other products with Federal Bureau of Investigation (FBI), National Counterterrorism Center, U.S. Capitol Police, and fusion centers, and jointly updated the U.S. violent extremist mobilization indicators booklet to ensure the indicators also apply to domestic violent extremism.

I&A also has regularly delivered briefings to Federal, SLTT, and private-sector partners in the Homeland Security Enterprise to apprise them of changes in the domestic terrorism threat environment, and to help inform prevention, mitigation, security, and response efforts. I&A has prioritized briefing staff at the National Network of Fusion Centers and other State and local law enforcement partners throughout the Nation at the U//FOUO level. I&A also has engaged with foreign partners to share information, produce intelligence assessments regarding violent extremist threats, and identify commonalities and potential collaboration between these actors.

I&A measures progress against goals and objectives established in the National Strategy to Counter Domestic Terrorism and the DHS Framework for Countering Terrorism and Targeted Violence Posture Review, and by monitoring the numbers/types of briefing or engagement requests received, numbers/types of analytic requests received, and/or feedback on products. We are also constantly examining our internal priorities and resources to improve our ability to align analytic expertise to intelligence customer priorities.

Question 4a. According to the Strategic Intelligence Assessments and Data on Domestic Terrorism that your office produces, in collaboration with the FBI and National Counterterrorism Center, from 2016–2019 I&A produced 67 domestic terrorism-related finished intelligence products and 1,068 domestic terrorism-related raw intelligence products. From fiscal year 2020 to fiscal year 2021, I&A produced 100 domestic terrorism-related finished intelligence products and over 500 domestic-terrorism related raw intelligence products.

While there appears to be some increase in producing analytic products on domestic terrorism, what percentage does this make up of I&A's total intelligence production?

Question 4b. Relatedly, what is I&A's total intelligence production? In other words, how many pieces of finished intelligence generally would you say that the 300 analysts within the Office produce per month?

Answer. Although the majority of I&A's workforce comprises intelligence personnel in the GS–0312 job series, many of those personnel perform intelligence work in disciplines other than analysis, such as collection requirements management, information sharing/liaison roles, and indications & warning functions. Finished intelligence is produced almost exclusively in I&A Mission Centers with approximately 180 analytic, management, and support personnel—about 140 of whom are frontline analysts who research and draft all-source products. Approximately 10 percent of I&A's finished intelligence production is related to domestic terrorism.

In fiscal year 2022, I&A disseminated nearly 1,000 intelligence products. This metric does not include any products disseminated outside of I&A's finished production lines, including Presidential Daily Briefs and joint products published in other IC elements' product lines (CIA WIRe, NCTC Current, DIA DID, etc.). I&A production is driven by mission priorities, customer demand, and on-going threat streams, all of which can evolve based on current events and associated drivers. I&A and other intelligence agency production is focused on quality and value of the content to their respective customers, which is not accurately assessed based solely on average quantities.

Question 4c. According to the October 2022 Strategic Intelligence Assessments on Data on Domestic Terrorism, data related to domestic terrorism incidents were focused solely on incidents investigated by the FBI, but I&A also tracks domestic terrorism incident information. How did the FBI and I&A develop the methodology used to determine which incidents would be included in the report?

Answer. I&A Counterterrorism Mission Center has a formal process for continually collecting, coding, and analyzing domestic violent extremist incident data which is included in an internal incident tracker. This incident tracker has been in existence since 2016, and the methodology has been continually updated since its inception with a more comprehensive update undertaken in 2021. In August 2022, I&A widely released an FOUO Intelligence in View titled "Domestic Violent Extremist Attacks and Plots in the United States From 2010 Through 2021," which provided an overview of 2010–2021 fatal and non-fatal attacks and plots associated with domestic violent extremism.

For the Strategic Intelligence Assessments on Data on Domestic Terrorism, I&A, FBI, and the U.S. Department of Justice (DOJ) jointly agreed on the inclusion of specific incidents, based on FBI's and DOJ's respective roles as lead Federal agencies for terrorism investigations and prosecutions and their access to specific investigative data on these incidents. I&A will continue to coordinate with FBI and DOJ on future updates to this report to ensure these reports contain the most comprehensive data possible on significant incidents the Federal Government is aware of.

QUESTIONS FROM RANKING MEMBER AUGUST PFLUGER FOR KENNETH L. WAINSTEIN

Question 1a. A review of I&A's statutory authority, which lists approximately two dozen responsibilities within your office, reveals that there is no explicit provision for open-source collection. During the hearing on December 13, 2022, you said I&A mainly relies on authorities drawn from Executive Order 12333 to build out such a large collection capability. You also made clear that I&A's open-source collection is a major focal point for agency resources. Prior to the revised and re-issued EO 12333 by President Bush in 2008, where did I&A draw these collection authorities from?

Question 1b. What efforts is I&A making to ensure that its other authorities, which are designated by statute, are prioritized and carried out, over those which are solely granted by EO 12333?

Answer. The Homeland Security Act of 2002 directed I&A's predecessor office to, among other things, "access, receive, and analyze . . . information," "integrate relevant information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others)," and "ensure . . . the timely and efficient access of the Department to all information necessary to discharge the responsibilities [of I&A]." Implicit in these authorities is the authority to collect information, including publicly available (i.e., open-source) information. Recognizing this, and the increasing importance of open-source intelligence to I&A's work, Congress amended the Act in 2007 by explicitly

requiring I&A to, "whenever possible . . . produce[] and disseminate[] unclassified reports and analytic products based on open-source information" (emphasis added). As with I&A's authority to "access, receive, and analyze" all source information, this subsequently—added statutory requirement that I&A "produce and disseminate" intelligence based on open-source information necessarily implies the authority to collect such information.

As the statutorily designated office in DHS responsible for carrying out the Secretary's responsibilities relating to intelligence and analysis (6 U.S.C. § 121) and a designated element of the U.S. intelligence community (50 U.S.C. § 3003(4)(K)), I&A carries out all intelligence activities assigned to it—whether in law or Executive Order—in support of both National and Departmental missions in accordance with the intelligence priorities, policies, and guidelines established by or otherwise consistent with the direction of the President, the Secretary, and the director of national intelligence, and in consultation with intelligence, law enforcement, and other Federal, State, local, and private-sector homeland security partners.

Question 2a. I&A has faced bipartisan frustration throughout the years. In 2009, I&A produced a non-public report intended for law enforcement partners entitled "Right-wing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment." This report was heavily criticized by Congress and veterans' organizations for its characterization of the right-wing extremist group's recruitment of former service members. Since that report, the Privacy Office, Office of Civil Rights and Civil Liberties (CRCL), and General Counsel have reviewed and cleared analytic products that would be disseminated to non-Federal recipients. While well-intentioned, how has this process impacted I&A's ability to issue reports in a timely manner?

Answer. I&A has worked closely with these oversight offices as well as our own Privacy and IO Branch to build and maintain collaborative relationships that help us produce products that meet customer intelligence needs in a timely and meaningful way, that are consistent with our intelligence authorities, and that protect the privacy, civil rights, and civil liberties of U.S. persons. We have codified the roles and responsibilities of the relationship between the analytic workforce and the legal offices in I&A Policy Instruction IA–901: Production of Finished Intelligence. The instruction stresses that I&A personnel and the oversight offices work collaboratively to address any requested or required edits and includes a dispute resolution mechanism, which includes the I&A analytic ombuds, to ensure that the analytic workforce and the legal offices have avenues to express concerns with the review process. The timing of the review process can be adjusted as mission needs require through coordination with the oversight offices and it has not negatively affected product timeliness since the updated process was codified.

Question 2b. Has this process impacted the independent nature of I&A's analytical judgments? How much involvement do offices such as CRCL and Privacy—with personnel who are not familiar with intelligence—have with the content of products?

Answer. DHS's oversight offices provide consultation and advice to all I&A personnel concerning legal requirements, policies for the protection of privacy, civil rights, and civil liberties, and oversight and compliance guidelines for I&A Finished Intelligence Products, and affirmatively clear I&A Finished Intelligence Products that include information and analysis relating to U.S. persons, Constitutionally-protected activity, or other matters that have significant oversight equities. The oversight offices ensure compliance but seek to avoid altering or influencing analytic judgments of products or the substantive content on which they are based.

Question 3. I&A is charged with the administration of the Homeland Security Advisory System, which is meant to advise the public of specific warnings, protective measures, and countermeasures related to threats to homeland security. The National Terrorism Advisory System (NTAS) is the mechanism for communicating specific terrorist attack threats. For almost 2 years, a number of NTAS bulletins have continuously been in effect stating that the United States is in a "heightened threat environment." During the hearing on December 13, 2022, you reflected that the persistence of this designation and generality of the threat explanation could diminish the usefulness of the NTAS to the public and distract from the intent for I&A to communicate specific, targeted warnings, protective measures, and countermeasures to "triggering events" that disrupt the "baseline" threat environment. Given this reflection, how can the NTAS bulletins be leveraged into a more effective tool for notifying the American public without undermining its own efficacy with a persistent threat designation that is not comparable to a baseline?

Answer. DHS replaced the color-coded alerts of the Homeland Security Advisory System (HSAS) with the National Terrorism Advisory System (NTAS) in 2011, and the responsibilities for the NTAS have been delegated by the Secretary to the Department's Counterterrorism Coordinator. The NTAS is designed to communicate in-

formation about terrorist threats by providing timely, detailed information to the American public, through the provision of NTAS advisories (both Alerts and Bulletins). NTAS bulletins have typically been issued in 3- to 6-month increments and have ranged from 3 weeks up to 7 months in duration. In contrast to the HSAS, the NTAS provides value to the public by sharing resources and information associated with the threat. I&A shares the committee's concern that successive issuances of updated NTAS bulletins might be construed to diminish the significance of the heightened environment by relegating it to a perpetual baseline. Due to the volatile and ever-evolving nature of the current threat environment, DHS issues, cancels, or updates NTAS bulletins when deemed necessary. In the most recent update, we opted to issue the NTAS noting that conditions justified continuing to caution the public about the heightened threat environment despite the absence of a specific, emergent threat.

Question 4. I&A was originally envisioned to be the nexus of intelligence activities related to threats to the homeland, in partnership with the FBI and other intelligence agencies. However, for many reasons, I&A struggles to live up to this vision. Could you please describe the current operating procedure of DHS I&A within the rest of the intelligence community (IC)? What is I&A's unique value-add within the National security apparatus?

Answer. I&A is a unique member of the U.S. IC and is the only IC element statutorily charged with delivering intelligence to SLTT and private-sector partners and developing intelligence from those partners for DHS and the IC. This is at the core of why Congress established I&A, in part to fill a void that existed within the intelligence- and information-sharing architecture between Federal and SLTT partners. Carrying out this role as a bridge between the IC and our front-line SLTT and homeland security operators and decision makers ensures that these entities remain aware of the most pressing current and emerging threats to the Nation and contributes to our collective defense of the homeland. I&A is positioned to identify and collect information of intelligence value from non-Federal partners and make it available to authorized recipients across the IC that otherwise could never obtain it. In the other direction, I&A is able to facilitate SLTT and private-sector partners' access to National IC information, often at a lower classification level for greater utility. The intelligence shared by I&A supports the effective identification and mitigation of the threats we face from foreign and domestic terrorists, nation-states, transnational criminal organizations, cyber criminals, and emerging threats.

Question 5a. I&A has no clandestine intelligence collection authority and primarily operates as an integrator and disseminator of information among the DHS components; State, local, and Tribal agencies; private-sector entities; and other related elements of the IC. Could you please explain the flow of information from its initial collection in the IC or DHS component intelligence offices, to I&A, and out to I&A's consumer base?

Answer. While I&A does not have clandestine intelligence collection authorities, it does have the authority to collect raw, unevaluated information overtly or from publicly-available sources, and regularly provides unique information of intelligence value to DHS, the IC, and its SLTT partners. I&A collectors gather and report intelligence information in serialized raw reports that are disseminated to DHS, the IC, and SLTT analysts via IC reporting systems and the Homeland Security Information Network Intel portal. I&A analysts synthesize and integrate this information with other DHS, IC, and SLTT information and draft finished intelligence products on topics related to customer priority information needs. Once drafted the finished intelligence product is reviewed and cleared through I&A's review process and disseminated via one of I&A's externally-facing information-sharing websites and briefed to customers as needed and appropriate.

Question 5b. When I&A analyzes a product that it has received from the IC and/or enterprise, how and why does I&A make additional analysis to the original examination performed by the collecting agency or component? Is there a value-add provided by I&A's analysis?

Answer. It is important to distinguish between raw information of intelligence value and the process of its transformation, through analysis and integration with other information, into finished intelligence products. In addition to its own raw, unevaluated intelligence reporting, I&A analyzes component and other IC element-derived raw intelligence reporting to answer intelligence questions through original and strategic finished intelligence. I&A analysis provides value in that it takes raw information from all sources and synthesizes that information into finished analytic products tailored to DHS Enterprise customers, especially non-traditional consumers of intelligence such as State, local, Tribal, territorial, and private-sector partners—at the lowest classification for ease of dissemination to decision makers. I&A analysis also ensures that unique analytic insights and data from State and

local partners and DHS components are provided to National-level, traditional intelligence customers, which better informs more holistic understanding of National security threats.

Question 5c. Is I&A's analysis of such products ever re-evaluated or audited? If so, please elaborate.

Answer. I&A evaluates a sampling of its own published and disseminated finished intelligence products each month for adherence to ODNI Intelligence Community Directive (ICD) 203 Analytic Standards. I&A uses the results of these evaluations as a teaching tool for analysts and reviewers of draft finished intelligence products to improve future finished intelligence products.

Question 6a. The I&A workforce has grown substantially over the past several years. Could you please provide the committee with I&A's overall growth (reflected in both personnel and budget) since its inception, broken out by year?

Answer. See table below for I&A's authorized full-time equivalent positions. Top-line budget figures for IC organizations are Classified and I&A can provide a briefing on its funding and expenditures in a closed session.

Year	Number
Fiscal year 2007	301
Fiscal year 2008	312
Fiscal year 2009	365
Fiscal year 2010	473
Fiscal year 2011	657
Fiscal year 2012	636
Fiscal year 2013	617
Fiscal year 2014	612
Fiscal year 2015	548
Fiscal year 2016	544
Fiscal year 2017	590
Fiscal year 2018	623
Fiscal year 2019	653
Fiscal year 2020	674
Fiscal year 2021	732
Fiscal year 2022	758
Fiscal year 2023	781

Question 6b. Could you provide a breakdown of the types of hires, including skill sets, this growth has focused on?

Answer. Since the organization's inception, I&A's growth has been focused in the following three job categories: Intelligence Operations Specialists (0132 job series), Management & Program Analysts (0343 job series) and Information Technology Specialists (2210 job series).

Question 6c. Please explain how this growth strategically aligns with I&A's mission to deliver intelligence to State, local, Tribal and territorial partners as well as to develop intelligence from partners in the Department and IC.

Answer. I&A's growth and investment directly or indirectly supports our partnership and information-sharing mission, particularly in ensuring representation at all 80 State and major urban area fusion centers. Our investments are focused on enhancing the quality and timeliness of our intelligence production or enabling intelligence and information sharing to directly benefit State, local, Tribal, territorial, and private partners. This includes producing intelligence that addresses those partners' requirements and feedback and that is generally available at the un-Classified level. In fiscal year 2022, 66 percent of I&A products were at the un-Classified level, and investments in technology have focused on enhancing State and local access to intelligence, including through the new DHS Intel App that allows our partners to receive un-Classified intelligence on their mobile device.

Question 7. I&A boasts a robust internship program that operates in the functional areas of Intelligence Analysis, Intelligence Operations, Mission Readiness, Information Technology, and Data Science. How much has this internship program grown over the past 10 years, and how many of these interns convert to full-time I&A employees?

How many of these interns that convert to full-time employees have previous intelligence analysis experience?

Answer. I&A's Internship Program has become the primary driver to recruit entry-level talent across the organization. With strong and sustained leadership

support, I&A has been able to expand the applicant pool and refine the selection process to ensure an annual internship cadre reflects traditional markers of diversity as well as broad skill sets and interests that allow them to be assigned widely across I&A offices to leverage their talents. Adaptations gained during the pandemic now enable interns to support offices remotely while back in school and to receive virtual training sessions and briefings to develop their knowledge of I&A, DHS, and the IC.

Since 2014, I&A's internship program has grown by over 1,100 percent. In January 2014, I&A had four student interns on board and that number has grown to 49 as of the beginning of fiscal year 2023—peaking at 70 at the beginning of fiscal year 2020. Approximately 139 of I&A's over 300 student interns converted to full-time employees since 2014.

Question 7b. Could you provide the committee with the percentage of intern converts encompassing the entire I&A workforce?

Answer. At the beginning of fiscal year 2023, approximately 10.6 percent of I&A's current workforce are former I&A interns (78 employees).

Question 7c. How many of these interns that convert to full-time employees have previous intelligence analysis experience?

Answer. Nation-wide colleges and universities form I&A's internship candidate pool. We cannot rule out that an intern had prior intelligence analysis experience when entering the internship program; however, we do not explicitly recruit interns based on prior intelligence experience.

Question 8a. Over a year ago, DHS leadership stood up a working group to investigate malicious internet activity that permeated many of the threats the Department handled. This group was helmed by the DHS Office of Policy and I&A. Its members concluded last year that there wasn't a mechanism to address the policies governing how these activities are coordinated across the Department. This conclusion led to the creation of the DHS Disinformation Governance Board. Could you please describe I&A's exact role within the working group as well as its involvement in the subsequent Disinformation Governance Board?

Question 8b. Please elaborate on I&A's role within the misinformation, disinformation, and mal-information space. How has this role evolved over the past 5 years?

Answer. I&A has been asked to provide DHS leadership with a threat overview of malign foreign actors' efforts to spread mis-, dis-, and mal-information in ways that affect Departmental missions. I&A provided a similar threat overview to the Secretary's Homeland Security Advisory Council when that body was asked to review the Disinformation Governance Board's activities. Within this space, in 2019 I&A established the Foreign Influence & Interference Branch within the Cyber Mission Center to identify foreign malign influence activities, particularly but not solely with regard to election interference. This branch monitors influence efforts by statutorily designated malign foreign actors—under 50 U.S.C. Sec. 3059—including Russia, China, and Iran, and evolving tactics, techniques, and procedures by such actors seeking to influence U.S. audiences.

Question 9a. In its August 24, 2022 final report on the Disinformation Governance Board, the Homeland Security Advisory Council states that I&A should serve as a principal channel for obtaining disinformation warnings from the IC and from other entities. This is in part because I&A already identifies the spread of disinformation through all-source intelligence research, including open-source collection from known forums. Could you please elaborate on I&A's identification process for disinformation?

Question 9b. What are the standards set (and by whom) for I&A to define disinformation and what recourse exists once disinformation is identified? Are different standards utilized for information originating from foreign nation-states and Transnational Criminal Organizations versus American citizens?

Answer. I&A approaches the identification of mis-, dis-, and mal-information in a content-neutral manner. We do not assess the validity or veracity of narratives being spread on-line, but rather, focus on identifying the messaging of statutorily-designated malign foreign actors—under 50 U.S.C. Sec. 3059—including but not limited to China, Russia, and Iran. We also review the spread of messaging from these actors by other foreign governments. As these actors are designated under U.S. law as being involved in active efforts to influence U.S. audiences, spread information with malicious intent, and engage in activities such as interference with U.S. elections, I&A tracks the messaging of these foreign actors without independently seeking to assess the veracity of these governments' claims. I&A also identifies messaging on-line by transnational criminal organizations, often related to human smuggling and influencing migration to the U.S. border, to inform U.S. Customs and Border Protection (CBP) and other border security stakeholders.

Question 10. I&A's statutory authority describes agency responsibilities to be more of a facilitator of information between DHS and other components of the IC or Federal, State, and local law enforcement, as well as private-sector partners. Can you discuss the focus that I&A places on this facilitating and sharing function and the importance of it to the mission of DHS? How does this differ from the FBI's relationships and information sharing with State and local law enforcement?

Answer. I&A is a unique member of the U.S. IC and is the only IC element statutorily charged with delivering intelligence to SLTT and private-sector partners and developing intelligence from those partners for DHS and the IC. This is why I&A 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. In recognition of the importance placed on fostering these relationships, I&A has elevated its externally-focused engagement by creating the position of deputy under secretary for intelligence partnerships. I&A is only able to execute our mission when we have strong collaboration with our law enforcement and homeland security partners across the country. Additionally, through our partnership with the National Network of Fusion Centers, DHS deploys personnel across the country to share information on a broad range of threats. DHS remains committed to working closely with SLTT partners, including the sharing of timely and actionable information to ensure our partners have the information they need to keep our communities safe. DHS's primary focus is on the two-way sharing of threat information with our partners across all threats. In this capacity, we complement our partners at the FBI, which shares its information with SLTT partners through a variety of task forces and jointly-produced analytic products.

Question 11a. The predecessor to I&A was stood up on the heels of 9/11 while the Department took shape. Since I&A's official establishment in 2007, the threat landscape and the role of DHS have transformed. How would you assess I&A's role within DHS and its cooperation with other agencies in the IC has shifted?

Question 11b. From the feedback you have received from other elements of the IC as well as Federal, State, local, and private-sector partners, what do you believe is the perception of the value that I&A adds?

Answer. Following the September 11, 2001 terrorist attacks, the Homeland Security Act of 2002 created DHS and the Implementing Recommendations of the 9/11 Commission Act of 2007 established I&A as the first Federal agency statutorily mandated to share intelligence with State, local, Tribal, and territorial law enforcement, as well as the private sector—creating the necessity for a comprehensive approach and strategy to homeland security. The threat environment is never static, thus I&A remains dynamic in its actions to combat the challenges of today, as well as the future, through partnerships, information sharing, and a concrete understanding of the evolving landscape at home and beyond our Nation's borders. Terrorist networks continue operations to inspire and mobilize those in our country, transnational criminal organizations seek to exploit our borders, and state and non-state cyber actors target our critical infrastructure, information networks, and the American people.

In the early years of its existence, I&A was largely involved in facilitating the sharing of information acquired by other organizations and was a contributor to the analytic work of more well-established IC agencies. As I&A has matured, it has established its own native capability to overtly collect raw intelligence, fuse DHS-unique data from components, and produce tailored homeland-centric intelligence for a wide range of National and non-Federal partners in a way no other IC agency can. I&A is also on the leading edge of exploiting open-source intelligence while safeguarding privacy, civil rights, and civil liberties. As DHS engages, supports, and shares information with our partners, we enhance and bolster opportunities to protect the homeland, and ensure critical information and data resident within the holdings of our partners can be accessed and shared with DHS and the IC.

Question 12. In your testimony before Congress on December 13, 2022, you stated, "At the same time, I&A's production—including regular products in the President's Daily Brief last year—helped inform the IC and policy makers on the unique threats the Nation faces internally and at its borders." How much of this content was unique I&A analysis versus the modified analysis of another IC member or Intelligence Enterprise (IE) component?

Answer. The vast majority of I&A analysis is original analysis tailored to our unique customers' intelligence needs and incorporating unique insights from DHS data and expertise. At times, I&A will identify existing IC and Intelligence Enterprise (IE) production that we believe would be useful to our customers and will work with the originating agency to further disseminate production—often at a downgraded classification level—to those additional customers if they do not already have

access to it. DHS IE components also post their finished intelligence products to our externally facing production websites which customers are able to access given appropriate clearances and need-to-know. Additionally, in cases where a topic would be better informed by the unique analysis, expertise, and data from multiple agencies or components, I&A produces jointly authored products with those IC agencies and DHS IE components to tell a more holistic story.

Question 13a. The Department of Homeland Security often engages with the Committee on Foreign Investment in the United States (CFIUS) and Team Telecom to review transactions that potentially pose a risk to the Department's interests. As part of this review, I&A submits information to the Office of the Director of National Intelligence (ODNI) to inform CFIUS and Team Telecom determinations. Exactly how many I&A personnel are dedicated to the CFIUS and/or Team Telecom review processes?

Answer. Currently there are three I&A personnel dedicated to supporting the Committee on Foreign Investment in the United States (CFIUS) and/or Team Telecom review processes.

Question 13b. Please explain what information I&A provides ODNI to inform these processes.

Answer. I&A manages the DHS Intelligence Enterprise's (IE) participation in the IC's threat assessment process for CFIUS. I&A solicits threat information from the DHS IE, requesting information from each DHS component to look at the transaction and vet/assess if it were to take place, would the transaction pose a threat or concern to their component mission interests. I&A consolidates the DHS IE threat information, places it into context informed by operator perspectives, and sends it to ODNI for the IC-coordinated threat assessment. I&A is uniquely positioned to reach counterparts across DHS operational components' broad missions, vast repositories of exploitable information, and deep field expertise that can be leveraged to inform CFIUS decision makers.

Question 13c. How often do these information exchanges occur?

Answer. I&A corresponds on each CFIUS request received (in 2022 there were 289 CFIUS transactions and 55 Team Telecom requests).

Question 13d. What other IC and IE information exchanges are occurring in support of CFIUS and Team Telecom?

Answer. Currently, I&A holds a quarterly meeting with the DHS IE for the CFIUS portfolio. I&A also participates in an ODNI—hosted weekly CFIUS meeting for the IC.

Question 13e. How much of the information shared is the result of I&A's own collection and analysis versus that of another member of the IC or IE?

Answer. The information I&A provides to ODNI for CFIUS cases comes from the DHS IE and their data sources. I&A receives Team Telecom requests from the DHS Office of Strategy, Policy, and Plans' Foreign Influence Risk Management and I&A conducts reviews on these Team Telecom requests for foreign ownership, control, and influence in open source, commercial, and Classified data.

Question 14. How many Full-Time Employees (FTE) and contractors does I&A employ? Please provide a breakdown of the categories of roles each of these FTEs and contractors perform within I&A, including those that perform collection versus analysis roles or other categories of responsibilities. Please provide the budget allocations associated with each of these categories of roles.

Answer. I&A's fiscal year staffing levels averaged approximately 750 full-time employees, and the budget allocations and percentages by primary function are below.

The data reflect an approximate level of effort or resource investment, but variances occur throughout the year based on mission priorities.

	Percent of I&A Budget	Personnel (Fed) costs (%)	Non-personnel costs (%)	Percent of I&A Staffing (%)
Analysis & Production	11	92	8	30
Collection & Exploitation	8	58	42	21
Information Sharing & Partnerships	18	75	25	19
Department Integration	12	50	50	8
Technology & Data	35	16	84	8
Corporate Resources & Services	16	60	40	14

Question 15. The committee was informed that the Special Event Assessment Rating (SEAR) process would be relocated under I&A as part of a DHS reorganization process. Has this relocation occurred yet? If so, how many staff are assigned to this

work? If not, when can we expect this relocation to occur? What is the budget allocation required to support this function? Will that funding transfer with the movement of the function?

Answer. In 2021, the Department identified a number of strategic infrastructure transformation priorities as a path forward on how to better organize the Department for the challenges we will face in the years to come. One of the outcomes of the process was a recommendation to move the DHS Special Events Program (SEP) into I&A. I&A has been collaborating with SEP on the anticipated transition since early 2022. SEP's transition into I&A became official when Congress enacted the fiscal year 2023 budget in January 2023, authorizing the transfer of 11 SEP billets and $2.2 million to I&A.

Question 16. The National Vetting Center (NVC) is a collaborative, interagency effort to provide a clearer picture of threats to National security, border security, homeland security, or public safety posed by individuals seeking to transit our borders or exploit our immigration system. Does I&A provide technical support to the NVC? If so, how many staff are assigned to this work and what is the budget allocation required to support this function?

Answer. I&A acts as a technical service provider on behalf of CBP, which administers the National Vetting Center (NVC). CBP provides reimbursable funding to I&A each year for several technical services (software, hardware, labor) that, in totality, comprises the NVC's case management system, known as the High Side Vetting Unified Environment. With the passing of the fiscal year 2023 budget, CBP intends to transfer approximately $20 million to DHS I&A under its reimbursable authorities. I&A executes the funds across several contracts that provide different functional services, such as: (1) Development and on-going operations and maintenance support to vetting programs, project management, and integration with IC partners; (2) IT security to provide the review of incremental system changes; (3) cross-domain infrastructure and engineering to automate the secure transfer of information across classification domains; (4) cloud engineering support; and (5) Amazon Web Services cloud storage and processing and other software licenses. About 40 contractor staff support the NVC from I&A, but contract staffing levels can vary depending on the activity. Currently, there is one I&A Federal employee serving as the NVC's Technical Director with two additional full-time employees pending selection and hiring.

Question 17. During the hearing December 13, 2022, Representative Slotkin inquired about I&A's policy and procedures, if any, for monitoring individuals who have projected hateful rhetoric but have not committed a crime or threatened to do so. What is I&A's official policy and procedure for monitoring speech in such individuals or situations?

Answer. I&A's intelligence activities surrounding on-line speech are regulated primarily by the interaction of two key provisions in I&A's Attorney-General approved IO Guidelines. I&A's IO Guidelines provide that I&A personnel may engage in intelligence activities where they have a reasonable belief that the activity supports one or more of the National or Departmental missions listed in this section of the Guidelines. Departmental missions include not only domestic terrorism, but a variety of other significant threats that could overwhelm our State, local, or Federal partners with homeland security missions. In addition, the guidelines provide that I&A personnel are prohibited from engaging in any intelligence activities for the purpose of affecting the political process in the United States, for the sole purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States, or for the purpose of retaliating against a whistleblower or suppressing or burdening criticism or dissent. Further, as a matter of internal DHS policy, I&A personnel are not permitted to engage in intelligence activities based solely on an individual's or group's race, ethnicity, gender, religion, sexual orientation, gender identity, country of birth, or nationality. As such, I&A's work that touches on hateful rhetoric focuses on identifying, understanding, preventing, and mitigating threats of terrorism and targeted violence.