S. Hrg. 117–480

EXAMINING THE ROLE OF THE DEPARTMENT OF HOMELAND SECURITY'S OFFICE OF INTELLIGENCE AND ANALYSIS

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

MAY 18, 2021

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

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
45–998 PDF WASHINGTON : 2022

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
ROY S. AWABDEH, *Senior Counsel*
PAMELA THIESSEN, *Minority Staff Director*
ANDREW DOCKHAM, *Minority Chief Counsel and Deputy Staff Director*
KIRSTEN D. MADISON, *Minority Director of Homeland Security*
ERIN E. KUHLS, *Minority Investigative Counsel*
SHANI M. ROSENSTOCK, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*
THOMAS J. SPINO, *Hearing Clerk*

CONTENTS

WITNESSES

TUESDAY, MAY 18, 2021

ALPHABETICAL LIST OF WITNESSES

APPENDIX

EXAMINING THE ROLE OF THE DEPARTMENT OF HOMELAND SECURITY'S OFFICE OF INTELLIGENCE AND ANALYSIS

TUESDAY, MAY 18, 2021

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10 o'clock a.m., via Webex and in room SD–342, Dirksen Senate Office Building, Hon. Gary C. Peters, Chairman of the Committee, presiding.

Present: Senators Peters, Hassan, Sinema, Rosen, Ossoff, Portman, Johnson, Romney, Scott, and Hawley.

OPENING STATEMENT OF CHAIRMAN PETERS[1]

Chairman PETERS. The Committee will come to order.

Today we will hear from former homeland security intelligence officials, as well as national security and civil rights experts, on their views of the appropriate roles, responsibilities, and authorities for the Department of Homeland Security's Office of Intelligence and Analysis (DHS I&A).

I would like to thank each of our witnesses for joining us today and for their work in the public and private sectors to protect the American people.

Today's testimony will give the Committee critical insight into how the Office of Intelligence and Analysis operates and what role it should play in providing threat assessments and domestic terrorism intelligence to Department of Homeland Security leadership, State and local law enforcement partners, and other private entities.

We will also hear testimony on how to ensure citizens' fundamental civil rights and civil liberties are safeguarded as we work to better tackle a rising domestic terrorism threat.

Earlier this year, the Committee heard about how systemic breakdowns in planning and preparation led to the deadly attack on the U.S. Capitol, the heart of our democracy.

The Office of Intelligence and Analysis, along with other intelligence and counterterrorism agencies, failed to effectively identify the threat on January 6th.

We need to understand the factors that led to that failure and what concrete steps can be taken to better understand the current threats that we face and ensure the Department of Homeland Se-

[1] The prepared statement of Senator Peters appear in the Appendix on page 33.

curity is effectively sharing information with local and State law enforcement.

I appreciate the hard work and the ongoing dedication of the national security experts in the Office of Intelligence and Analysis, and I recognize they have faced challenges that they must address. However, it is apparent that the office must also do more to effectively counter the rising threats posed by white supremacist and anti-government violence that threaten communities all across our country.

One of the greatest challenges the Office of Intelligence and Analysis has faced is the pressure to politicize domestic terrorism threats. Under the previous administration, the office reportedly downplayed the threat posed by white supremacist and anti-government violence and reportedly censored some intelligence information under pressure from President Trump.

At times, this political pressure led to problematic and inaccurate analysis related to peaceful protest movements, overstating the roles of certain groups, and even reportedly developing intelligence on American journalists.

Our national security and the safety of Americans cannot depend on political whims or individual leaders' biases.

That is why Congress must work to ensure that analysis conducted by the intelligence community (IC) is separated from the political environment and based in facts and in data that accurately assess security threats.

The office also struggles with employee morale, a challenge identified by the Government Accountability Office (GAO) reports and employee surveys, possibly because of a lack of consistent leadership and direction.

Since this office was first created 19 years ago, it has had more than a dozen different leaders. Only three of those individuals, including one of our witnesses today, led the office for more than two years.

These obstacles, and other challenges, must be addressed quickly. Our Nation faces very real and deadly domestic terrorism threats, and our national security agencies must ensure that our counterterrorism efforts and resources align with those threats.

A recent, long-delayed joint report from the Federal Bureau of Investigation (FBI) and DHS identified racially or ethnically motivated extremists, primarily white supremacists, as the most significant national security threat based on data from recent years.

While I appreciate the initial steps the Biden administration has taken to begin addressing the alarming rise of these threats, it is clear that there is so much more work to be done. American lives are at risk, and we must ensure that we are taking all appropriate action to safeguard the American people and protect their most fundamental rights as well.

I look forward to hearing from our witnesses, who bring unique perspectives on how we can improve the Office of Intelligence and Analysis to meet our security goals.

I have no doubt that this Committee can work in a nonpartisan way to strengthen our homeland security and protect Americans from all threats, both foreign and domestic.

With that, I turn it over to Ranking Member Portman for your opening comments.

OPENING STATEMENT OF SENATOR PORTMAN[1]

Senator PORTMAN. Thank you, Mr. Chairman, and thank you for holding this hearing. It is important and timely for us to learn more about what Homeland Security's Office of Intelligence and Analysis does and how to ensure that they are doing their job better.

DHS is responsible for protecting the homeland, and I believe its intelligence and analysis capabilities are absolutely essential to that effort. So let me start by saying I think the role that is being played is critical, and I look forward to discussing how to best equip the Department and its partners with critical, timely, and actionable intelligence to keep us safe from both foreign and domestic adversaries.

There are plenty of challenges right now. The events of January 6th have just been talked about. Domestic terrorism, recent attacks on Federal facilities and law enforcement, Mexican and other foreign cartel networks that are now operating much more so, as I understand it, within our cities, the ongoing threat, of course, posed by foreign terrorists—all this underscores the need for ongoing intelligence and analysis focused on identifying and mitigating threats to our country.

Since its inception, DHS has had an intelligence office to support its mission, understandably. Congress underscored the importance of intelligence and information sharing in the Implementing Recommendations from the 9/11 Commission. This was back in 2007, and that formally established the Office of Intelligence and Analysis.

While it is one of the smaller entities within the intelligence community, I&A is the only IC member charged with delivering intelligence to our State, local, tribal, territorial (SLTT), and our private sector partners and developing intelligence from these important partners for the Department and for the intelligence community. To put it simply, I&A is intended to facilitate a key layer of communication and domestic coordination required, in my view, to help support the effort at DHS to protect the homeland.

In my home State of Ohio, we have three fusion centers that have benefited greatly from the partnership with I&A. I visited one of them a couple of times, the Cincinnati fusion center, where I have seen the importance of the support and the partnership that I&A provides. For example, I recently learned that an I&A intelligence officer at one of our fusion centers, in Columbus, Ohio, provided critical information on a suspect who had a plot to cause mass violence at large music concert venue in Columbus. By leveraging I&A's capabilities, the Columbus fusion center was able to quickly work with law enforcement to locate that suspect and place this individual on the Transportation Security Administration (TSAs) no-fly list. The suspect was then intercepted while attempting to board a flight on his way to Columbus to carry out the at-

[1] The prepared statement of Senator Portman appears in the Appendix on page 35.

tack. That is one example, but there are many like that, where I&A has played a critical role.

The Committee learned from our oversight investigation into the January 6th attack on the Capitol that I&A fell short in reporting on the potential threat. They were not the only ones, but they did fall short, in my view. Security officials have cited the lack of intelligence and information sharing from I&A and other intelligence agencies as a reason law enforcement was not better prepared to respond. In our investigation, the then-Acting Under Secretary of I&A revealed weaknesses in how I&A distributes information, collects intelligence from social media platforms, and leverages its relationships with State, local, tribal, territorial, and private sector partners to learn of new, evolving threats. And that will be part of the report that we will be issuing here in the next few weeks.

Notably, I&A has an important role to play in combating transnational criminal organizations (TCOs)—including those responsible for drug trafficking, violence, human smuggling, child exploitation, and a host of other criminal activities. As I said earlier, TCOs are increasingly present here in this country. They are always evolving, they are always adapting to maximize their profits as they did as Coronavirus Disease 2019 (COVID–19) reshaped supply chains and transport patterns. In fact, according to the Drug Enforcement Administration (DEA), once they adjusted to the initial disruption of COVID, Mexican cartels "reinforced supplies of precursor materials, increased production and are sending larger fentanyl and methamphetamine loads into the United States." We certainly see that at the Mexican border.

It seems more important than ever for Federal and local partners to be in close coordination to understand and combat these dynamic threats. And, while these challenges are national, they have hit local communities, including many in my home State of Ohio, particularly hard.

There are a number of issues I hope we are able to explore today. There are differing opinions on what I&A's role is with regard to intelligence collection, production, and dissemination. In my view, having timely, quality intelligence is an essential component, again, to keep our communities safe. I hope today that we can talk about how DHS can appropriately provide these capabilities at a time when we face some threats that are home grown.

The threats we face are dynamic and becoming more complex every day. And they are not all focused on Washington, D.C. Considering the current environment, how can I&A best leverage those fusion centers we talked about and its partnerships with State, local, and private sector partners to meet the needs of the Department charged with securing our homeland?

Finally, over the years, I&A has faced challenges in recruiting qualified talent and has experienced consistently low morale and high rates of attrition. This is a deep concern of mine. I hope our witnesses can help us understand what can be done to address these longstanding personnel issues.

General Taylor, Ms. Cogswell, Mr. Sena, and Ms. Patel, I am looking forward to your testimony and some answers to those questions we pose today.

Thank you.

Chairman PETERS. Thank you, Ranking Member Portman, for your opening comments.

It is the practice of the Homeland Security and Governmental Affairs Committee (HSGAC) to swear in witnesses, so if our witnesses will please stand and raise your right hand? And our witnesses who are in video, raise your right hand so we can see you on the video. Do you swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

General TAYLOR. I do.

Ms. COGSWELL. I do.

Mr. SENA. I do.

Ms. PATEL. I do.

Chairman PETERS. The witnesses may be seated.

Our first witness today is General Francis Taylor, the former Under Secretary for Intelligence and Analysis at the Department of Homeland Security. Prior to his assignment at DHS I&A, General Taylor was vice president and chief security officer (CSO) for the General Electric Company. General Taylor has also served as the Assistant Secretary of State for Diplomatic Security and Director of the Office of Foreign Missions (OFM) with the rank of Ambassador. General Taylor also previously served as the U.S. Ambassador-at-Large and Coordinator for Counterterrorism for the Department of State from July 2001 to November 2002. Prior to that, General Taylor accumulated 31 years' military experience, rising to the rank of Brigadier General.

Mr. Taylor, former General, General Taylor, welcome to the Committee. You are recognized for your five minute opening remarks.

TESTIMONY OF THE HONORABLE FRANCIS X. TAYLOR, FORMER UNDER SECRETARY, OFFICE OF INTELLIGENCE AND ANALYSIS (2014–17), U.S. DEPARTMENT OF HOMELAND SECURITY

General TAYLOR. Chairman Peters, Ranking Member Portman, and Members of the Committee, thank you for the opportunity to appear before you today to talk about the DHS Office of Intelligence and Analysis. I have submitted written testimony and would ask that that be entered into the record,[1] and I will try to summarize that in my five minutes this morning.

Chairman PETERS. So ordered.

General TAYLOR. I&A's mission is integral to DHS, the intelligence community, and to the security of our Nation. It is the only U.S. intelligence agency that is specifically chartered to provide intelligence support to State, local, tribal, territorial, and private sector partners to improve the flow and quality of information sharing across our Nation. As the intelligence arm of DHS, I&A has a responsibility to support the intelligence needs of the senior leadership of the Department, to ensure that relevant intelligence from the IC is shared systematically with our State, local, tribal, territorial, and private sector partners, and that relevant information from those partners becomes intelligence that is shared more broadly with the IC.

[1] The prepared statement of Mr. Taylor appears in the Appendix on page 39.

As the Chief Intelligence Officer (CINT) for the Department, the Under Secretary of I&A coordinates and deconflicts the efforts of the DHS intelligence enterprise to meet the intelligence needs of the Department and our IC partners. Additionally, the Under Secretary's responsibility to lead information sharing and safeguarding for the Department provides a unique opportunity to use the myriad of data generated by DHS and to turn that data into effective information to share with our SLTT, Federal, and international partners.

There are several initiatives that I believe I&A leadership must focus on.

First, restoring trust. I&A leaders will need to focus on rebuilding trust with key stakeholders within and across DHS and the Intelligence Enterprise (IE), as well as externally, with the broader IC and Congress. Controversies surrounding I&A activities and the use of intelligence authorities in recent years have undermined its reputation and raised questions about the integrity and objectivity of the information it provides to stakeholders. In order to rebuild stakeholder and public trust, I&A will need to focus on advancing its core mission and demonstrating that it brings invaluable mission expertise to its customers.

Second, focus on SLTT and private sector partners. Moving forward, I&A should focus on effective prioritization of its information-sharing activities, ensuring that they meet the needs of State and local law enforcement and yield intelligence information that could be useful to the broader IC, as a complement, not as a competitor, of the FBI. Likewise, I&A should continue to engage its partners in private industry to gain perspectives on the national and homeland security challenges facing their sector and ways to facilitate public-private partnerships.

Third, reinvent intelligence analysis for DHS and the IC. I&A leaders should focus the office's intelligence analysis activities on the creation of intelligence products that draw on unique DHS data sets and data science, within a robust framework for privacy and civil liberties. I&A can be a leading player in government focusing on data science to create unique insights and produce clearly differentiated intelligence products. With access to special data sets and a focused set of priorities, I&A can lead the IC in reinventing does intelligence.

I believe the mission center concept that was established by the most recent Under Secretary is a great idea and needs to be further developed within I&A and within the DHS IE. I&A should create a budget, annual strategy, metrics, and fully resource each mission center to appropriately support the needs of the intelligence enterprise components, the Department leadership, and the broader IC. Finally, I&A should lead in data analytics using the unique data generated by the Department.

DHS generates a tremendous amount of relevant information in its daily mission activities. When I was there, that information sat in more than 900 mutually independent databases. That needs to change.

Finally, as Senator Portman and Senator Peters mentioned, we need to invest in our workforce, and I would be happy to talk about that and morale during your questions.

Thank you for the opportunity to be here today.

Chairman PETERS. Thank you, General Taylor, for your testimony.

Our second witness today is Patricia Cogswell, former Deputy Administrator of the Transportation Security Administration. Ms. Cogswell is currently a senior strategic adviser for Guidehouse National Security. Prior to serving as Deputy TSA Administrator, Ms. Cogswell had a long and distinguished career in public service, including leading programs at the White House, Department of Homeland Security, and the Department of Justice (DOJ) related to intelligence, information sharing, border security, screening and watchlisting, and aviation, maritime, and surface transportation.

Ms. Cogswell, welcome to the Committee. You are recognized for your opening statement.

TESTIMONY OF PATRICIA F.S. COGSWELL,[1] FORMER DEPUTY ADMINISTRATOR (2018–20), TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. COGSWELL. Thank you, sir. Chairman Peters, Ranking Member Portman, and distinguished Members of the Committee, thank you for the opportunity to testify before you this morning as you examine the role of DHS' Office of Intelligence and Analysis. My comments for the Committee today are in formed by my more than 24 years of career Federal civilian and from the various capacities in which I have both led and worked with DHS I&A.

During my tenure, I served in multiple DHS leadership roles, including with three different headquarters elements and three different DHS component agencies, as well as a 3-year tour at the National Security Council (NSC).

When I served as the Deputy Assistant Secretary for Screening Coordination, as Special Assistant to the President for Transborder Security at the National Security Council, and, most recently, as the Deputy Administrator for TSA, I was a consumer of DHS I&A's intelligence products. While at DHS Policy, another headquarters office, I partnered with DHS I&A to lead development of interagency strategic and policy initiatives, collaborated on reports for the Secretary and other DHS leaders, and to lead DHS governance processes.

As the Assistant Director for Intelligence at Immigration and Customs Enforcement (ICE), I was a member of the Homeland Security Intelligence Council (HSIC), working with DHS I&A to inform strategic direction, policy, priorities, requirements, and production. Finally, I led DHS I&A serving as the Acting Under Secretary while the nominee was undergoing confirmation.

During my time I found the highest value roles for DHS I&A to be:

Supporting the Homeland Security Intelligence Enterprise; the Under Secretary, as the Chief Intelligence Officer, in collaboration with the HSIC, should lead development of strategy, policy, and an integrated set of priorities, including training and budget;

Advocating for the DHS mission to the intelligence community and through associated budget processes. DHS I&A should advo-

[1] The prepared statement of Ms. Cogswell appears in the Appendix on page 43.

cate on behalf of operators and policy personnel for prioritization of intelligence collection, access to IC information, use of IC information-sharing platforms and tools, and associated resources;

Providing the Secretary, Deputy Secretary, and headquarters organizations with intelligence services, ensuring that headquarters offices and the Secretary have access to the same high-quality intelligence at their counterparts do, particularly in advance of interagency and policy meetings;

Coordinating production of "sense of community" analyses to support DHS and homeland security-unique needs in coordination with the HSIC. In addition to products like the Homeland Security Threat Assessment (HTA), the CINT should support development of "sense of community" products to support policy and operational decisions. Development of individual products should be by the DHS entity best positioned to speak on behalf of the entirety of the information, including not only traditional intelligence and law enforcement information, but also analysis developed by DHS in support of its ongoing programs, and other knowledgeable stakeholders, including academia and associations, and that the products are scoped to answer relevant questions for the conversations;

Engaging the fusion centers. DHS I&A should support State, local, territorial, and tribal partners with training, information, and all source analysis that helps those partners, based on the partner needs;

And collaborating with other DHS entities to enable an effective information-sharing environment. DHS I&A should support the design and funding of technical architectures and multi-use tools that enhance DHS's ability to match and exchange information, where appropriate, to achieve their missions, in collaboration with the operating components and other headquarters offices. DHS I&A should work to ensure it can perform effectively across these functions with variance in approach based on the needs and capabilities of its partners. To do so, DHS I&A needs to examine staffing and morale, including in particular stabilizing its organizational structure, mission, and role. The workforce needs consistency and continuity, something that lasts beyond the tenure of a single Under Secretary, as well as a mission that is unique and valued where they can be recognized as having subject matter experts and are seen as partners;

Enhancing career development opportunities. DHS I&A leadership should invest in changes that will provide supervisors incentives to positively coach and mentor their personnel and career paths that enable staff to grow, including mobility to DHS agencies, increasing their opportunities and exposure to the wider homeland security mission;

Depoliticizing products, and career staff. DHS I&A should enhance its strategic communications with its customers and stakeholders, providing the opportunity for input into I&A's analytic product selection process, methodology, data used, how it is assessed, and ensure that it seeks out support from partners and oversight, including this Committee, for efforts in areas that may become controversial.

As this Committee examines DHS I&A's role, I would encourage you to consider how to develop changes in a way that will support

the organization for years to come. Organizational, transformational, and cultural change take investment in time, developing talent, a willingness to measure impact and modify activity based on those results, and in commitment to strategic communications.

Thank you again for the opportunity to testify before you today. I look forward to your questions.

Chairman PETERS. Thank you, Ms. Cogswell.

Our next witness is Mike Sena. Mr. Sena serves as the president of the National Fusion Center Association (NFCA), which represents State and major urban area fusion centers. These centers work to enhance public safety and encourage effective, efficient, ethical, lawful, and professional intelligence and information sharing and prevent and reduce the harmful effects of crime and terrorism on victims and communities. In addition to his leadership positions, Mr. Sena serves on law enforcement and homeland security advisory committees for the members of the President's Cabinet, the Department of Homeland Security, the Federal Bureau of Investigation, and the Attorney General (AG) of the United States.

Mr. Sena, welcome to the hearing. You may proceed with your opening comments.

TESTIMONY OF MIKE SENA,[1] PRESIDENT, NATIONAL FUSION CENTER ASSOCIATION

Mr. SENA. Thank you, Chairman Peters, Ranking Member Portman, and Members of the Committee. I appreciate the invitation to be with you today.

My name is Mike Sena, and I am the Director of the Northern California Regional Intelligence Center (NCRIC), and the president of the National Fusion Center Association. The NFCA represents the interests of 80 State and locally owned and managed fusion centers, with over 3,000 public safety employees. We refer to all 80 centers together as the "National Network of Fusion Centers."

Fusion centers assist in the identification, prevention, mitigation, response, and recovery of terrorist acts and other major criminal threats. We depend on DHS I&A as the only U.S. intelligence community element that is statutorily charged with supporting our network. A locally integrated and engaged I&A is critical to enhancing capacity among fusion centers and our partners to analyze and share threat-related information that is relevant and timely.

We are offering several concrete recommendations that would help ensure I&A is able to maximize its potential capacity to protect the homeland. I&A must increase the forward deployment of well-trained and experienced personnel to fusion centers. They must offer high-quality training on analytics tradecraft and on privacy, civil rights, and civil liberties. They must invest in modernizing information-sharing systems and technologies. They must also ensure reliable access to critical data, including criminal justice information and classified data. Finally, they must be empowered to have direct coordination authority of DHS resources that are allocated to support fusion centers. Having I&A's partner engagement function, which is routinely coordinating with us, and

[1] The prepared statement of Mr. Sena appears in the Appendix on page 48.

having them report directly to the I&A Under Secretary and Principal Deputy would be helpful in facilitating this.

Some fusion centers do not have any I&A presence, and some others have part-time I&A personnel. Currently, I&A only has a little more than 100 personnel deployed across the Nation. From our perspective, that is simply not sufficient. We strongly encourage Congress to support increased funding for I&A to ensure that it can hire, train, and deploy an adequate number of personnel across the Nation.

More than two-thirds of all the funding that supports fusion centers comes from State and local budgets. DHS grant funding is another critical source of support that primarily comes through our Urban Area Security Initiative (UASI) and State Homeland Security Grant Programs (SHSGP). Some centers are almost entirely grant funded, and some receive almost no grant funding. Some fusion centers provide operational support at the request of public safety partners, including the FBI's Joint Terrorism Task Force (JTTF), but in some cases the Federal Emergency Management Agency (FEMA) has limited or denied the ability for fusion centers to use grant funds to provide that support. We must find better ways to reduce bureaucracy and improve efficient authorization of grant funding in a timely manner.

I&A should be empowered to coordinate with FEMA's grant personnel to ensure that grant guidance and funding are more closely aligned with the needs of Federal, State, territorial, and local public safety partners.

Access to information systems is critical to the successful operations of our fusion centers, but some centers still lack access to critical databases, like the FBI's criminal justice services and Treasury's Financial Crimes Enforcement Network system. The National Data Exchange (N–DEx), brings together over 7,700 agencies' records systems, but we have over 18,000 agencies in America. Most agencies are not connected to this critical resource, and some fusion centers do not have access.

Fusion centers should be equipped to help protect everyone in America, regardless of where they are. I&A can play a supportive role by working with their Federal partners to ensure appropriate access to Federal systems by State and local partners.

I&A should continue to support the development and enhancement of existing systems, including the Homeland Security Information Network (HSIN), and work with us to identify and deploy more advanced technology. The HSIN Platforms are essential and trusted fusion center tools. The NFCA established the HSIN SitRoom for sharing information on physical threats, and the Cyber Intelligence Network (CIN)—room supports cyber threat collaboration for over 500 cyber analysts across the country. I&A should continue to support fusion center cyber capabilities by providing access to critical cyber analysis tools and increasing training opportunities.

Right now, fusion centers, the Regional Information Sharing Systems (RISS)—Western States Information Network (WSIN), and the FBI's National Threat Operations Center (NTOC) are analyzing data and sharing information on reported threats to life through

HSIN, the FBI's eGuardian System, and directly with local and public safety agencies.

The Criminal Intelligence Coordinating Council (CICC) and Global Advisory Committee are also writing recommendations for managing tips, leads, and threat-to-life reporting. We need DHS I&A resources to support this effort to mitigate the immediate threats to our communities.

In summary, strengthening I&A's capabilities to support the network and the Nation will require them to reorient their focus. Their focus must be on the H in DHS and the State, local, tribal, and territorial partners that are the heart of protecting our homeland. The recommendations I mentioned a minute ago would help DHS I&A support the national network in ways that are most relevant and helpful to our members and our partners across the Nation.

On behalf of the NFCA, I would like to thank you for the invitation to testify, and I look forward to your questions.

Chairman PETERS. Thank you, Mr. Sena, for your testimony.

Our final witness today is Faiza Patel, director of the Liberty & National Security Program at New York University School of Law's Brennan Center for Justice. Ms. Patel has previously testified before Congress regarding the government's surveillance of Muslim and Arab Americans following the September 11th attacks and has organized advocacy efforts against discriminatory State laws. She also helped establish an independent Inspector General (IG) for the New York Police Department (NYPD), and prior to joining the Brennan Center, Ms. Patel worked as a senior policy officer at the Organization for Prohibition of Chemical Weapons in The Hague and clerked for the judge at the International Criminal Tribunal in the former Yugoslavia.

Welcome, Ms. Patel. You are recognized for your five minute opening statement.

TESTIMONY OF FAIZA PATEL,[1] CO-DIRECTOR, LIBERTY & NATIONAL SECURITY PROGRAM, BRENNAN CENTER FOR JUSTICE, NEW YORK UNIVERSITY SCHOOL OF LAW

Ms. PATEL. Thank you, Chairman Peters, Ranking Member Portman, and Members of the Committee. I am really happy to be here testifying today.

As our country faces up to the persistent problem of white supremacist and far-right violence, as well as a range of other threats, I&A has the potential to play a constructive role in providing accurate and unbiased intelligence to help guide the response. The office has great influence because it sits at the center of a web of intelligence and law enforcement agencies spread throughout the country.

In light of its influence, it is critically important that I&A's output and advice meet the highest standards of respect for Americans' civil rights and civil liberties. This is especially true when it comes to domestic intelligence, which presents unique threats because of its obvious overlap with protected political speech and organizing.

[1] The prepared statement of Ms. Patel appears in the Appendix on page 58.

I&A is, of course, prohibited from collecting or disseminating information based solely on First Amendment-protected activities, but it has in the past targeted Muslim Americans for little apparent reason other than their religion, as well as protesters.

Last summer, as racial justice demonstrations triggered by the killing of George Floyd broke out across the country, I&A led the expansion of intelligence activities under the guise of protecting Federal courthouses. I&A staff were directed to collect information both about matters that can be reasonably considered threats to homeland security, but also matters that are traditionally handled by local authorities as part of their public safety mandate.

According to the Washington Post, I&A even had access to protesters' communications on telegram, which is not allowed by its guidelines, and these were written up in an intelligence report disseminated to its network. The office circulated three intelligence reports summarizing tweets written by the editor of a legal blog and a reporter for the New York Times.

It is particularly critical that I&A gets its house in order as DHS pivots to confront the threat of domestic terrorism. Secretary Mayorkas has designated domestic violent extremism (DVE) as a priority area and has created a team within I&A to focus on this threat.

Based on testimony and reports in the press, it seems that I&A will be looking at Americans' social media postings to identify narratives and grievances to gauge their prevalence and to see if they may influence acts of violence. I am concerned that this focus is likely to be both ineffective and invasive, sweeping in reams of information, including about constitutionally protected activities.

Targeting what people say online is unlikely to be effective in identifying violent actors. The reason is pretty simple: Large numbers of people believe in the types of narratives that DHS has already identified as drivers of violence in its January 27th bulletin. Anti-immigrant sentiment has a long history in the United States; many people believe that measures taken to control COVID–19 infringe on their freedoms; many Americans dispute the results of the 2020 elections; and police use of force against African Americans triggered demonstrations across the country.

We can argue about whether the people who hold these views are right or wrong, but they are hardly a way of distinguishing potentially violent actors. In technical terms, this method is highly sensitive, but it is not specific to the threat of violence.

The Acting Under Secretary of I&A recently acknowledged this fact, noting that it is difficult to discern actual intent to carry out violence from angry and hyperbolic speech on the Internet. This is supported by years of research which show the difficulty of interpreting social media posts without context or knowledge of the conventions in particular communities or platforms.

DHS of all agencies should know the limits of social media to find threats. According to its own internal documents, social media monitoring pilot programs for visa vetting did not help in finding security threats. The people charged with running these programs said that they were not able to reliably match accounts to people, and even when they were, they were not able to determine the context and reliability of what they saw.

To address the concerns I have outlined, I think it is critical to strengthen I&A's civil rights and civil liberties safeguards and oversight over its functions. I have four recommendations.

First, given social media's centrality to political discourse and the difficulty of identifying threats online, I&A should reconsider its plans to monitor these platforms for "narratives" and "grievances." At a minimum, it should explain how it intends to ensure that it is focused on identifying violent actors rather than simply keeping tabs on what Americans say on the Internet.

Second, oversight needs to be strengthened. This hearing obviously is a great example. But DHS also has a dedicated Office of Civil Rights and Civil Liberties (CRCL) and a Privacy Office. Their role in clearing I&A analyses was eliminated last year and should be restored. Congress should consider mechanisms for ensuring that these types of critical oversight functions cannot be so easily sidelined in the future. Regular audits can also help ensure that leadership has a holistic view.

Last, we need to pay attention to the enormous amount of information on Americans that is contained in DHS databases. Former DHS officials have said that this level of information raises privacy and due process concerns that dwarf those arising out of the National Security Agency (NSA) programs. This would be an appropriate topic of inquiry for the Privacy and Civil Liberties Oversight Board, in my opinion.

Thank you again for the opportunity. I look forward to answering any questions you may have.

Chairman PETERS. Thank you, Ms. Patel, for your opening statement.

General Taylor, in last year's Homeland Threat Assessment, DHS stated that domestic violent extremism, specifically white supremacist extremists, are the most persistent and lethal homeland security threat. That is a finding that both myself and Ranking Member Portman have been saying for some time now, and it is clear that this threat is real, and it is clear that we need to combat it.

So my question to you is: Beyond establishing the Domestic Terrorism Branch, which is certainly, I think we all agree, a step in the right direction, are there other changes to I&A's organization or authorities that you believe would help them address this threat?

General TAYLOR. It is my view that I&A has the requisite authorities to address this threat if it prioritizes that threat. In the last administration, it is my understanding that domestic terrorism was not considered a priority for I&A. In fact, the I&A leadership kind of deferred to the FBI on that. I think the authority exists. It is a focus on what the outcome is that I&A is trying to achieve and how they do that consistent with privacy, civil rights, and civil liberties going forward.

Chairman PETERS. So your testimony is that it just was not prioritized. They have the authorities to do it. Perhaps we can drill down on that a little bit, if we could, General. What do you see as the added value that I&A provides to the broader Federal intelligence community and partners in combating this? What is the specific value that they could bring if sufficiently prioritized?

General TAYLOR. Much of the work against violent extremists occurs in the 18,000 police departments across our country. Local law enforcement confronts these individuals, investigates these folks because they are committing acts in communities that those officers are sworn to protect.

It is my view that through the fusion centers I&A and its intelligence officers can bring better perspective to the national level of what these 18,000 police organizations are seeing trend-wise and tactics, techniques, and procedure-wise in their communities. The FBI plays an extraordinarily important role in its JTTF, but as Director Wray has testified, there needs to be a definitive act of violence for the FBI to get involved. I think that is the gap that I&A can help cover with its collection and production in the field.

Chairman PETERS. Very good. Ms. Patel, I guess this question is for you. As I&A continues to come to better understand and analyze the real threat posed by domestic terrorism, could you share with the Committee some of the concerns that communities of color in particular are facing with this effort to combat domestic terrorism?

Ms. PATEL. Thank you for that question. So for communities of color, when you have broad, open intelligence-gathering authorities and programs, there is a risk that they will be the target of those programs. We have seen this sort of systematically over the last two decades where Muslim Americans have been targeted for surveillance often on the basis of nothing other than their religion. We have seen this with African American communities being targeted. We have see the Black Lives Matter (BLM) movement being targeted, and this is a pretty well known phenomenon in the United States.

I think the overall concern is that domestic terrorism is discussed sort of almost a stand-in for white supremacist violence, but covers a much broader range of issues, as we have seen from DHS and FBI documents. So the concern is that these kinds of broad, open surveillance programs will actually be used to target communities of color, as has been the case in the past.

Chairman PETERS. Very good. General Taylor, last year you authored an op-ed noting your significant concern with I&A's reportedly problematic intelligence operations in Portland and the publishing of intelligence on journalists specifically. More recently, this Committee has found that I&A warned generally about the potential for election-related violence, but failed to issue a warning specific to the risk facing the Capitol on January 6th. In both examples, I&A clearly did not serve its customers or the American people in that respect.

My question to you is: In your opinion, what are the key reasons for I&A's failures over this past year?

General TAYLOR. It is hard for me, Senator, to kind of focus in on the key reasons for failure because I was not in the decision cycle. But I think organizations like I&A fail to meet their mission if they are not organized in a way that ensures consistency of production, consistency of focus. And it is my understanding that those processes and procedures that at least existed when I was there were no longer being used from an execution point of view. I think solid leadership and solid management will save the day.

By the way, I am a product of the Church Commission and the follow-on from Counter INTELPRO. I have been on the Privacy and Civil Liberties Commission for President Bush. Privacy and civil rights and civil liberties are fundamental to how we should think about domestic intelligence, and for whatever reason, that was not the case during the last year.

Chairman PETERS. So you talk about stability and continuity. I would assume the fact that we have had a lack of stability when it comes to I&A leadership over the years, that has contributed to the problem that you see?

General TAYLOR. I do. As you mentioned in your opening statement, 12 different I&A leaders over 19 years really does not give you a lot of confidence about continuity. And during my tenure, it has been my experience in the military that when you take over an organization, you try to organize it to focus on the mission. Much of what we put in place was dismantled after we left office in 2017.

Chairman PETERS. Thank you, General.

Ranking Member Portman, you are recognized for your questions.

Senator PORTMAN. Thank you, Mr. Chairman.

Let me start, if I could, with General Taylor and Ms. Cogswell. A fundamental question here. Both of you have a broad national security background, including having at one time had the role of managing I&A. Do we need I&A at DHS? Yes or no.

General TAYLOR. Yes.

Ms. COGSWELL. I agree as well.

Senator PORTMAN. OK. I think there is some fundamental rethinking going on right now, and I think it is important, in my view that we have this intelligence-gathering capability, particularly, as both of you commented on, because our State, local, tribal, and private sector coordination and communication goes through I&A. Nobody else has that responsibility. Is that correct?

General TAYLOR. That is correct.

Senator PORTMAN. One of my big concerns has been the growth of these so-called TCOs. They are responsible for a lot of criminal activity, as you know, but one that is particularly pernicious right now is the movement of drugs into our communities, particularly fentanyl and the other synthetic opioids, which, unfortunately, killed more people last year, from everything we know, than ever in our history. And they seem to be working their way into the system more. In other words, they are more vertically integrated in our communities themselves, not just bringing things across the border as they are certainly doing.

What are we doing with regard to I&A and that issue? Are we thinking expansively enough when it comes to combating these TCOs that have these tentacles into communities around the country? What is your view, General Taylor?

General TAYLOR. Senator Portman, I think that this is a problem for the entire DHS intelligence enterprise. The organization Ms. Cogswell led in ICE has a very important role to play in helping State and local law enforcement as well as other Federal partners gather the intelligence that is necessary to disrupt these TOC organizations going forward. I do not think it is just I&A, but it is how

the intelligence enterprise is organized to support the investigation and field work of U.S. Customs and Border Protection (CBP), of ICE, of DEA across the country, is the important role that I&A plays in trying to coordinate that effort.

Senator PORTMAN. How about the coordination with those 18,000 police forces around the country? Isn't that a key role?

General TAYLOR. Absolutely, and that is a part of understanding what is going on on the ground, what those priorities are, and sharing that information more broadly with Federal partners, not just I&A but with ICE and CBP, so we have a fuller picture of what is actually happening and how it can be——

Senator PORTMAN. Ms. Cogswell, do you have thoughts on TCOs?

Ms. COGSWELL. I do. Thank you very much. As you noted, a critically important topic for us. I would like to give one example to General Taylor's point from when I was actually still there. We were extremely fortunate as the National Security Council began examining the transnational organized crime issue that they said we want to look to have a law enforcement organization lead a whole-of-community effort to assess the threat across all the different dimensions that will help set the stage for us to have the right policy debate about how the U.S. Government can take better and broader action.

I was extremely fortunate that my team, my chief of staff at the time, was selected to lead the effort for the entire community with support of DHS I&A, as well as other members of DHS, the Department of Justice, and the intelligence community. I think that is a fantastic example of how the community comes together through these mechanisms to provide valuable intelligence that helps set direction for policy, whether additional legislation may be needed, where the resourcing is allocated.

Senator PORTMAN. From what you know—and, again, we do not have the Acting Under Secretary here with us because we are not mixing the public and private panels, but from what you all know, and those who are joining us virtually, speak up as well, do you think that the current administration is focused enough on the TCO threat?

Ms. COGSWELL. I know it is, in fact, a priority for them and that there is work underway, and in particular, I am aware of some very good discussions underway between DHS I&A, the Office of Policy, and the operating components of DHS.

Senator PORTMAN. General.

General TAYLOR. I agree. But, Senator Portman, one of the challenges at I&A, there are 700 people in the entire organization. There are directorates of the Central Intelligence Agency (CIA) or Defense Intelligence Agency (DIA) that have twice as many people. I think I&A is trying to satisfy as many customers as it can, but it does not have the resources to spread itself as wide as it needs to.

One of the things I think we should focus on is where should those priorities come from, where should those investments be made, and resources to prioritize——

Senator PORTMAN. I think that is a good point. That is one reason I am asking you about this, because we talked about domestic terrorism, and we all agree that is important. But I think these

TCOs, from what we know from open-source information as well as others, it is growing as a threat and, again, working its way, its tentacles into our communities.

You talked about the relatively small number of people compared to others in the IC community. We have a real problem with attrition, too, and morale. And both of you have been consumers of the intelligence. You have also been there working with the individuals, and I want to hear from our own colleagues, too, who are on virtually.

But, Ms. Cogswell, let me start with you quickly. What do you think I&A can do to deal with the consistently low morale and the lack of leadership? I would hope that the administration, by the way, would nominate somebody for that Under Secretary slot right away and that we could get somebody in there who is willing to stick around for a while to provide some leadership. But I would love to hear your comments on that.

Ms. COGSWELL. Thank you very much. I agree with you that consistency and leadership that will be there for a period of time is critically important. I would also say that assuming that this Committee proceeds forward with some recommended changes—I know DHS will be considering them as well—I am hopeful that those are built in a way that will pass the test of time, will frankly last for a period of years. Much like the reviews after 9/11 where you looked at how various activities occurred in the intelligence community, I would hope similar activities would play themselves out at DHS I&A and, frankly, across the homeland security enterprise.

Senator PORTMAN. I think our report that I mentioned earlier is going to be helpful in that regard as well.

Let me quickly end with one really comment, and it is a question but we do not have time to get into it. I see a contradiction, Ms. Patel, in some of the things you are advocating and what others are advocating. We want more focus on domestic terrorism. We certainly have seen with regard to January 6th we did not have the information needed. It was online. There were plenty of threats of violence that were actually followed through on. And yet, Ms. Patel, you seem to be saying we should not rely on online information, it is unreliable, it is free speech, and that violence that is threatened online does not necessarily mean it is really violence. But that seems contradictory to what our experience is. So can you comment on that quickly? And to the extent we do not have time, maybe we could get into that in a second round.

Ms. PATEL. Thank you. Thank you for the question. I think we have to apply what we are looking for online. I am not saying by any means that we can never tell that violence is going to occur or criminal activity is going to occur online. I think there are probably ways that we can figure that out.

What I am saying, though, is that we should start with the violence rather than focusing on different narratives and grievances which are widely shared. So it is really a question of whether you go broad to narrow or whether you start with actual threats of violence, criminal activity, and then fan out from there to find other people who might be involved.

Senator PORTMAN. Thank you.

Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Portman.

Just for the record, for our folks who are online, Senator Portman started with a fundamental question which I think is important: Do we need I&A given all of the rest of the intelligence community? We heard yes from the two witnesses that were here. I did not hear from the two witnesses. Ms. Patel, yes or no? Mr. Sena, yes or no?

Ms. PATEL. I think I&A plays a useful role in terms of its sharing of information in the networking with State, local, tribal, and territorial. I guess I would say, that does not necessarily mean that that role could not be played by somebody else, and we know that the FBI, for example, does have JTTFs which perform kind of a similar role in an investigative capacity. While I recognize the importance of the role, I guess I am not as committed to it necessarily being in I&A per se as the other commentators are.

Chairman PETERS. OK. We can pursue that further.

Mr. Sena, yes or no? Preferable?

Mr. SENA. A strong yes.

Chairman PETERS. A strong yes. Very good.

Senator Hassan, you are recognized for your questions.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you, Chair Peters and Ranking Member Portman, for this hearing. Thank you to all of our witnesses for being here today and for the service you have provided in multiple arenas.

Quickly, General Taylor, I wanted to give you a chance to comment on something that Senator Portman and Ms. Cogswell discussed. Would it help overall employee morale in I&A if there was a nominee to head the office?

General TAYLOR. Absolutely, and I would also say, Senator, that I&A's morale was in the dumps when I took over with Secretary Johnson, and we were able to improve morale by focusing on kind of basic taking care of people, the things I have learned over 40 years in the military, and to get people focused on mission. So it is not an impossible task, but leadership needs to focus on it and make it a priority.

Senator HASSAN. Thank you.

I also want to follow up. Senator Portman talked with both of you, General Taylor and Ms. Cogswell, about the role that I&A plays in particularly combating TCOs, but I would like you to expand a little bit on it. The Office of Intelligence and Analysis is one of 17 entities within the larger intelligence community. So please take this opportunity to briefly talk about how I&A is suited to take advantage of its authorities and relationships to inform its own activities and the activities of the intelligence community as a whole. And how is its relationship with State, local, and tribal authorities different from other agencies? Why don't we start with you, General Taylor, and then to Ms. Cogswell.

General TAYLOR. As I said in my opening comments, I&A is the only intelligence agency specifically chartered to provide intelligence support to our State, local, tribal, and territorial partners, really as a result of 9/11, and the fact that we had people in this country who were about to commit a terrorist act, and there was

no way to loop in the 18,000 police organizations and 800,000 cops to understand what the nature of that threat is. And that is what I&A and DHS has worked on over the years. So that is what makes it unique.

Most of the IC cannot do work in the homeland. The FBI can from an investigative perspective and counterintelligence perspective, and DHS I&A. But the rest of the IC is precluded from the kind of specific work, intelligence work, that I&A does in the homeland.

Senator HASSAN. Thank you.

Ms. Cogswell.

Ms. COGSWELL. I agree with everything that General Taylor said. I would add it is also uniquely situated within DHS, so it is partnered up with other elements who directly have mission responsibility to enact programs specifically to counter threats. In addition to the threat and intelligence picture, the ability to wrap in policy and operational entities to help formulate direction, and then work with counterparts, including at the State and local level to exercise them, critically important.

Senator HASSAN. Thank you.

General Taylor, I want to turn to the issue of cybersecurity for a minute. We have seen a recent series of high-profile cybersecurity breaches and attacks against the Federal Government and critical infrastructure, and we do not expect that these threats are going to diminish. How can the Office of Intelligence and Analysis work with the Cybersecurity and Infrastructure Security Agency (CISA), to help prevent these attacks from happening?

General TAYLOR. I think the most important part is I&A is already at CISA with about 30 of its analysts working directly with CISA and the Computer Security Division to produce intelligence coming out of the EINSTEIN system. I believe CISA should have its own dedicated intelligence organization to assist not only I&A but its Director in formulating intelligence that is specific to the data that is collected by CISA. I also think that that would allow them a much more robust relationship with the National Security Agency. While NSA cannot actually do domestic intelligence collection, its analytical capability, I think, is important to our understanding of what the cybersecurity risk is and informing our partners in the Federal Government and State and local and private sector what actions they need to take to address those issue.

Senator HASSAN. Thank you.

Now I want to turn to the issue of terrorism threats, and we have talked a little bit about it this morning. But, General Taylor, I am pleased that the Office of Intelligence and Analysis recently announced a new effort dedicated to analyzing the threat from domestic terrorism. I also remain concerned about the threats posed by international terrorists and homegrown violent extremists (HVE).

In your view, do you believe that the Office of Intelligence and Analysis has the capacity to adequately monitor the various terrorist threats?

General TAYLOR. Absolutely, in conjunction with NCTC and the FBI. It does not stand alone. This is a partnership between the intelligence community, the FBI, and DHS and understanding the

nature of the phenomenon we are seeing both in the homeland and overseas. And the international threat is not diminished. The Islamic State of Syria (ISIS) and al-Qaeda continue to threaten the United States, and we need to keep a very clear eye on that threat as well as what we are seeing in the homeland as it has unfolded over the course of the last two or three years.

Senator HASSAN. Thank you.

Ms. Cogswell, you testified today about the importance of depoliticizing the intelligence process. What specific steps can the Office of Intelligence and Analysis take to accomplish this goal? And how can Congress assist?

Ms. COGSWELL. Thank you so much, Senator, for the question. In particular, as I thought about this type of particular issue, I very much liken it to right after 9/11 where we had a whole-of-country kind of rethink about why we did not see that coming. What was our failure of imagination in that front?

We put in place a number of activities, different processes post that threat, and part of it was starting with how we did the intelligence analysis itself; the ability to have different entities look at the problem from multiple different viewpoints, a diversity of viewpoint; the ability to have war gamings that looked at both the most likely scenario and the worst-case scenario; the ability to have a community that knew how to receive that information and then take action based on the fact that there is a variety of potential options. Even if they did not think the worst case was likely, they at least had discussed it and prepared for it.

I think there is real opportunity in this space to take some of those lessons learned and practices and apply them here.

Senator HASSAN. Thank you.

Mr. Chair, would it be all right if I asked General Taylor to quickly comment on that same issue, how we can assist in depoliticizing the process?

Chairman PETERS. Absolutely. Proceed.

General TAYLOR. Politics has no place in intelligence. It is the anathema in my view of solid intelligence collection, analysis, and reporting. And so during my tenure or, actually, during my 50 years of doing this, speaking truth to power is what intelligence officials are supposed to do, and despite politics, that is our job, and we need to do it and do it effectively.

Senator HASSAN. Thank you very much.

Thank you, Mr. Chair.

Chairman PETERS. Thank you, Senator Hassan.

Senator Rosen, you are recognized for your questions.

OPENING STATEMENT OF SENATOR ROSEN

Senator ROSEN. Thank you, Chair Peters, Ranking Member Portman. I appreciate the good questions and testimony already given today and for everyone's service to our Nation.

General Taylor, I want to move over to white supremacist extremists that we have. As Chairman Peters has previously noted, ahead of January 6th, DHS did not issue a threat assessment or a joint intelligence bulletin specific to the event. On March 3rd, Acting Under Secretary of Homeland Security for Intelligence, Melissa Smislova, told the Committee, and I quote, "More should have

been done to understand the correlation between the information and the threat of violence and what actions were warranted as a result."

Elizabeth Neumann, a former high-ranking DHS official, stated, and I quote again, "But for reasons of fear"—"the Department did not issue a formal report."

General Taylor, can you speak to whether there is a current fear to report, either specifically toward domestic violent extremism as it turns into white supremacy, and/or broadly to other pertinent threats that you might be assessing?

General TAYLOR. Thank you for that question, Senator. I was not there and, therefore, I cannot get into the mind of the leadership of I&A. What I would say is we have a process in this country around major events of producing threat assessments culminating from the information that we have collected across the country. That did not happen. Why it did not happen, I cannot say what is in the mind of the leadership that was in charge at the time, but I find it difficult to accept the fact that that process was not applied to this event, as with all other events in our threat analysis process.

Senator ROSEN. Thank you. Like you said earlier, intelligence should be nonpolitical, because we know that the rise in anti-Semitism is closely correlated with the spread of extremist ideologies. The audit of anti-Semitic incidents (ADLs) recorded 331 anti-Semitic incidents in 2020 attributed to extremists.

So how do you think that DHS intelligence could better account, is there something that you might recommend for us to work with them to better account for this growing threat?

General TAYLOR. DHS has partnerships across the country in State and local law enforcement and think tanks and all sorts of organizations that are monitoring this type of activity. I think continuing to coordinate with those organizations and entities to get a better picture consistently of what is going on on the ground and what tactics, techniques, and procedures law enforcement can use, as well as the private sector. We have relationships with religious organizations that we give information to about what these trends are and how they can protect themselves. So sustaining those relationships with up-to-date information about the nature of how the threat is unfolding I think is the best prescription for success in defending those communities that are targeted.

Senator ROSEN. I think you are right, and we do have good partnerships, especially when it comes to our national fusion centers (NFCA). I would like to ask Mr. Sena about the role that fusion centers really play in protecting Americans from terrorism. In my home State of Nevada, our fusion center has been at the forefront of tracking the domestic violent extremist threat specifically emanating from militias. The Southern Nevada Counterterrorism Center (NCTC) also played an important role in addressing the October 1st shooting back in 2017, the deadliest mass shooting in modern American history. So on behalf of all of Nevadans, I want to thank our fusion center for their tremendous service to our State and our community.

But, Mr. Sena, you stated you were surprised that fusion centers did not receive any specific information ahead of January 6th. Why

do you think that is that no specific threat information was shared? Again, maybe you might speak to see if there is a fear to report across the Department?

Mr. SENA. Thank you very much, Senator, for that question. When we look at the National Network of Fusion Centers and our coordination effort with I&A, especially on events that, as was said earlier, information is online, so there are a lot of restrictions on how information is collected and analyzed. And, back in 2017, the National Network of Fusion Centers, in conjunction with the Criminal Intelligence Coordinating Council, developed a real-time, open-source analysis, guidance and recommendations. But within those roles and responsibilities, just because it is hate speech does not mean it is extremist violence speech.

So being able to collect the information is one key element to this. Having the personnel that can report on it and make it part of the reporting requirements is a key issue that we still continue to have. Prior to January 6th, we as a network, a National Network of Fusion Centers, held a call on the Monday before the event because we were concerned, we were worried, and that call was directly related to a request from the Director of the fusion center in Washington, D.C. We did have DHS I&A personnel on that call who did say that they would have personnel onsite at the fusion center because there is not always personnel that are available to help them. We tried to build that network to share that information, and I was surprised that there was not anything developed at that time. But we were communicating in real time with them.

So, those that need to talk about the threat, need to share the information about the threat, we were actively working with the Washington, D.C., fusion center to share information in real time. The Washington, D.C., fusion center had personnel with the U.S. Capitol Police (USCP) to try to make sure that information was shared in real time.

There are some issues with that real-time information sharing. One of the issues that we have is that, DHS I&A is a Title 50 agency, an intelligence community agency, but they do not have the law enforcement authorities that other organizations have, such as the FBI.

And the Washington, D.C., fusion center at the time was not considered a law enforcement agency. So they were restricted from having that law enforcement information, which hindered our ability to share information at times.

So moving forward, though, and how do we look at this, I believe that using that real-time, open-source analysis guidance, expanding the roles within our privacy, civil rights, and civil liberties policies that every fusion center has, along with the policies that I&A have, they need to have that law enforcement authority, but they also need to have the capacity to access that data online to address those threats and to push information out in a timely manner to every agency that needs it to address specific terrorism, domestic violent extremists, and whatever major criminal threat is coming that we are seeing as a pre-indicator online.

Senator ROSEN. Thank you for that answer. I am going to look forward to following up with you on some things that we can do to enhance the communication and collaboration you are already

doing, but make it a little bit more robust so that we can stop any of these violent attacks before they start.

Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Rosen.

Senator Johnson, you are recognized for your questions.

OPENING STATEMENT OF SENATOR JOHNSON

Senator JOHNSON. Thank you, Mr. Chairman.

General Taylor, when you look at the title of the agency you once headed, it is "Intelligence and Analysis." From my standpoint, the analysis is really all about gathering all that information and then trying to prioritize it so we can adequately address the threats that face this Nation.

I thought Ms. Patel had a pretty good suggestion, that you start with the violence, a pretty good way of prioritizing things. What is the greatest threat magnitude? How many people could lose their lives? How much damage can be done?

I have always thought it was a little strange. The Chairman is focusing on white supremacists. Listen, I do not condone them. I condemn white supremacists. I condemn any act of violence. I do not categorize it whether it is right-wing, left-wing. I condemn violence. But the fact of the matter is we lose 70,000 people a year on drug overdoses.

General Taylor, do you have any idea how many deaths, how many murders occur from drug violence, gangs?

General TAYLOR. I have no numbers, sir, but it is an epidemic across——

Senator JOHNSON. It is thousands, isn't it?

General TAYLOR. It is, across the country.

Senator JOHNSON. It is thousands. I do not know what is the current level of white supremacist killings, but I think it is in the hundreds. Again, I condemn it completely, but we are talking about thousands of drug-related murders every years, tens of thousands of drug-related overdoses, and now we are supposed to concentrate on domestic terrorism as the greatest threat? Again, it is not.

Right now, the New York Times reported 160 different nationalities of people being picked up on the Southern Border over the last couple months. Ms. Cogswell, would you believe that is somewhat of a threat?

Ms. COGSWELL. I think that we have to continue to look at the processes by which people are showing up at the border. It is always possible that these networks and routes can be used for those who intend to do us harm.

Senator JOHNSON. When we are clogging up our system with close to 6,000 apprehensions a day. General Taylor, when you were in the administration, we had a humanitarian crisis, according to President Obama, of 2,000 people being apprehended a day. During 2018 to 2019, it was a little over 4,000. The last couple months it has been 6,000 people per day on average, almost. Six thousand people. What happens to our system when it is clogged up with 6,000 people? Doesn't that open up the border to additional drug trafficking? Doesn't that create opportunities for transnational criminal organizations to exploit it? Doesn't that open it up to other human trafficking of, let us call it, "higher-value targets" to get in

here that could create acts of violence? Last week it was surreal in this Committee room. Secretary Mayorkas, first of all, blaming the previous administration for the crisis they created, and, quite honestly, Senator Peters talking about, oh, the numbers are coming down, we are getting this under control.

No. Six thousand people per day, and it is really not being abated at all. Isn't that a threat? Isn't that an enormous threat?

General TAYLOR. Absolutely, and it is a threat that we have to face along with the other threats that come at us from across the globe, from not just our international partners but international adversaries. Look, in my view, the myriad of threats facing this country are significant and broad and not just for the Department of Homeland Security but for our State and local law enforcement organizations, for the FBI, for the Department of Justice, in a coordinated effort to address——

Senator JOHNSON. Again, my point being is we really ought to concentrate on the numbers and the magnitude of the threat. Listen, I condemned what happened here on January 6th, but I condemn as well the more than 500 riots that occurred during the summer, including in Kenosha, Wisconsin. Two dozen people murdered, 700 law enforcement officers injured, $2 billion worth of property damaged, yet we all just want to move beyond that and let us just focus on January 6th.

Another thing that really concerns me is we just saw the Colonial Pipeline cyber attack. I do not know if that is a shot across the bow, whether that is a criminal organization getting a little out of control of the Russian handlers and maybe going too far. I do not know what that is. But I do know that no administration, as long as I have been serving here, has taken literally the vulnerability of our electrical grid seriously, not when it comes to potential electromagnetic pulse (EMP) or geomagnetic disturbance (GMD) or cyber attack. We have seen what has happened now in terms of the vulnerability of the electrical grid to some of this green energy in Texas.

In your time, both of you, Ms. Cogswell and General Taylor, was DHS I&A looking at the vulnerability we are introducing into our infrastructure, like our electrical grid, with some of these green energy ideas? Ms. Cogswell, we will start with you.

Ms. COGSWELL. I would say that both during my time with DHS I&A and my time at TSA, which, as you know, has responsibility with relation to pipeline security, cyber was of considerable interest to us. We were focused on what we saw as the greatest potential threats, where the vulnerabilities were, how to work with the owners and operators to conduct assessments and help them improve their basic security pipeline. We did not select one opportunity threat over the other, but looking at it holistically across the board.

Senator JOHNSON. General Taylor?.

General TAYLOR. Sir, critical infrastructure is critically important to the security of our country. Eighty-five percent of the critical infrastructure in this country sits in private sector hands that makes the decisions about how to protect themselves. The Sector Coordinating Councils (SCC) that DHS has established over the course of the last 15 years have done yeoman's work in working with those——

Senator JOHNSON. We have not made any move whatsoever, for example, to purchase and put in place large power transformers that are incredibly vulnerable to either EMP attack or potentially a GMD event. We have not done it. We are literally spending trillions of dollars and proposing spending trillions more, and nobody is talking about doing something that prophylactic, that sensible in terms of protecting our infrastructure, because, I am sorry, I am afraid we are focusing on, domestic terrorism that might kill a couple hundred people a year versus something that could really represent an existential threat.

Again, my only point is I think we have politicized the threats we face, and we are not keeping our eye on the ball on the things that really represent a real threat to this Nation, which right now border security is probably the number one, and we are ignoring that and denying reality.

Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Johnson.

Senator Ossoff, you are recognized for your question.

OPENING STATEMENT OF SENATOR OSSOFF

Senator OSSOFF. Thank you, Mr. Chairman, and thank you to our panel.

General Taylor, where is there overlap based on your experience in government between the role of I&A and its responsibilities and the role and responsibilities of FBI's Intelligence Branch?

General TAYLOR. I think that they are inextricably tied together. Because of the nature of the FBI's authorities and the nature of the Immigration and Nationality Act (INAs) authorities, we cannot do our job effectively without the FBI, and the FBI relies on us to work with State and local partners on a consistent basis outside of the JTTFs to ensure that that intelligence becomes a part of the overall intelligence that is available to the homeland for decision-making going forward.

Senator OSSOFF. Thank you, General. I appreciate that. You wrote an article last August, I believe, on the Lawfare blog and noted, "I&A has differentiated itself by informing audiences not usually served by the intelligence community," but you also noted that I&A's mission overlaps with that of other agencies.

Where is there redundancy in the roles and responsibilities of the agencies that have mission overlap with I&A that could lead to inefficiency or a lack of clarity about who has principal responsibility for critical missions?

General TAYLOR. I think when I wrote that article about mission overlap, it is complementary, not competitive. There are agencies that collect information that is of value to I&A and to I&A's customers, and rather than I&A going out trying to collect information independently, they should collaborate with those agencies to make sure that that information is available.

I do not see a whole lot of overlap as long as we are leveraged the rest of the IC and our law enforcement partners to ensure we are not duplicating work that is already being effective done by our partners.

Senator OSSOFF. Thank you, General Taylor. How do you think I&A and the IC more broadly can do a better job of ensuring that there is not duplicative or conflicting effort?

General TAYLOR. I think that is through governance of the intelligence community, governance of the Department of Homeland Security, continual cooperation or collaboration with our partners in the FBI, and certainly getting feedback from our State, local, tribal, and territorial customers of what they need and where those gaps are and addressing those gaps.

Senator OSSOFF. How would you describe the breakdown of responsibility? And let me ask the question this way: Which agency has principal responsibility for developing and analyzing intelligence with respect to cybersecurity threats that both public and private sector enemies face? Which agency is principally responsible for that? Whose job is it above all others to develop intelligence with respect to cybersecurity threats, please, General?

General TAYLOR. I think DHS has the primary responsibility in the homeland. That partnership is with CISA and I&A. But I also believe that there is a strong need for a close and collaborative relationship with the National Security Agency and the Cybersecurity Directorate of our intelligence organizations to strengthen the analytical capability that informs our domestic intelligence efforts.

Senator OSSOFF. Thank you very much.

Ms. Patel, you mentioned in your testimony the need for I&A to adhere to "the highest standards" when it comes to the protection of civil rights and civil liberties. Given the central role that I&A plays sharing information not just with the Federal Government but also with State and local officials and private sector actors, you mention in your testimony instances during both Democratic and Republican administrations when, in your view, I&A improperly collected or shared information about U.S. persons. I would like you to comment, please, on why you think there may be a tendency for I&A to cross this line, in your view, and how Congress might better define or constrain I&A's roles, responsibilities, and authorities to ensure that the civil rights and civil liberties of Americans are protected.

Ms. PATEL. So it is not just I&A. Most intelligence agencies run into this problem, and we have certainly seen this starting with the Church Committee onwards that there is always a temptation, there is mission creep, and bias always plays a role as well in intelligence collection. These things are really quite challenging to solve, and I think the best way really is to really strengthen the civil rights and civil liberties mechanisms that are within DHS and to strengthen congressional oversight.

There are a lot of different ways that you can do it. I suggested a few in my testimony, including having DHS CRCL actually clear I&A's analytical products, as well as increasing audits of I&A products by DHS for CRCL purposes. But there are additional ways in which that office can broadly be strengthened, which have been proposed, especially by people who previously worked in that office, such as direct reporting lines to Congress, greater congressional attention to the things that CRCL produces, insisting on really specific reporting about CRCL problems in DHS as opposed to very generic stuff, which is what we have seen in a lot of the reporting.

I think these are some of the ways in which I&A can be more respectful of civil rights and civil liberties.

Senator OSSOFF. Thank you, Ms. Patel.

With my remaining time, General Taylor, would you like to comment in any way on Ms. Patel's analysis there?

General TAYLOR. I think Ms. Patel's analysis is correct in the sense that strong civil rights, civil liberties oversight is key to effective intelligence collection and analysis in the homeland. I am not sure I would agree that I need CRCL to clear intelligence products. I would see that as the responsibility of the intelligence officer who produced it. But to ensure that that product does not violate civil rights, civil liberties, or the policies of the Department would be my way of stating it.

Senator OSSOFF. Thank you, General. Thank you, Ms. Patel.

Thank you, Mr. Chairman, Mr. Ranking Member. I yield.

Chairman PETERS. Thank you, Senator Ossoff.

The Chair recognizes Senator Sinema for your questions.

OPENING STATEMENT OF SENATOR SINEMA

Senator SINEMA. Thank you, Chairman, for holding today's hearing, and I want to thank all of our witnesses for being here.

It is critical that every decision the Department of Homeland Security makes about protecting our Nation is backed up by robust analysis. We cannot protect our communities and secure our border without a strong Office of Intelligence and Analysis, and that is especially true today when our Nation and my State of Arizona are struggling to overcome a pandemic while also dealing with a crisis at the border.

My first question is for General Taylor. The Office of Intelligence and Analysis is unique in the intelligence community with its task to coordinate with Federal as well as State and local government and law enforcement entities to protect our country from threats, including pandemics. The COVID–19 pandemic created challenges for many. Based on your prior experience, how would the situation with the pandemic impact your recommendations to improve the overall effectiveness and coordination through the Office of Intelligence and Analysis with State and local governments and law enforcement?

General TAYLOR. Senator, thank you for the question. I am not sure I understand what you are asking me to comment on. Could you clarify that a bit?

Senator SINEMA. So now that we have a pandemic that we are working through, would that impact any of your recommendations to improve the overall effectiveness and coordination of the Office of Intelligence and Analysis with State and local governments and with local law enforcement?

General TAYLOR. Look, I think pandemics and other sorts of disruptions occur every day. I do not think that changes the nature of how I&A or our State and local partners approach their business. Maybe there is isolation and that sort of thing, but, threats continue during pandemics, and we have to continue to focus our efforts on the collection and analysis of those threats, even during a period of pandemic when people are stuck at home and cannot

get out. Our adversaries see that as a potential and opportunity to be exploited.

Senator SINEMA. Thank you.

My next question is for Ms. Cogswell. As was previously discussed, transnational criminal organizations pose a significant threat to our national security by facilitating drug trafficking, human trafficking, and violence at our Southwest Border. Our Nation is also dealing with a migration challenge at the border with CBP reporting record numbers of encounters, which, of course, diverts resources and focus.

So what steps can the Office of Intelligence and Analysis take to more effectively respond to the ongoing TCO threats that will better engage law enforcement, CBP, and ICE's limited resources? The second question is: Does I&A have the resources it needs to effectively address this threat?

Ms. COGSWELL. Thank you, Senator, for the question. With respect to the first element, I think that one of the most important elements that I&A, especially through the mission center construct, can bring to this discussion is providing the opportunity and floor for that strategic assessment, that sense of community across all the actors to inform strategic discussions, strategic policy decisions, strategic discussions about resource allocation between various threats, as well as helping to clarify in those discussions how best to look for evidence about the impact their actions are taking and whether or not those efforts have been successful.

With respect to your second point on resourcing, frankly I think there is a very good question and discussion to be had across a number of elements of the intelligence and operational environment in which we are talking about to look at whether or not the resources are commensurate to the threats we are currently facing. I thank you very much and look forward to further conversations by the Committee in that regard.

Senator SINEMA. Thank you. Another question for you on this same general topic. We see a diverse population of migrants arrive at the Southwest Border in Arizona, including asylum seekers who are coming from dozens of countries. Given your past experience in this area, what unique challenges does this migration influx present DHS from an intelligence and analysis perspective? What steps should the office take to ensure that criminals are not gaining entry into the United States?

Ms. COGSWELL. Thank you very much for the question. So with respect to the first element, the unique aspect, DHS I&A I think very much is in a support role for the ongoing individual elements, much more so a focus in assistance when we talk about sort of that strategic picture and the dynamicism in terms of priorities amongst a range of threats and characteristics.

With respect to the individual threats posed within the migrant communities themselves and how to best assess and screen, there is a robust screening architecture already in place. The key here is ensuring that there is the time and resources dedicated and available to ensure that screening occurs.

One of the things I found most important over time is looking at not only how tools can be an assistance to the various entities performing these functions, but also some of the analysis that goes

along looking at the various encounters themselves. What can we learn based on that in terms of routes, trends, practices, tactics being used, funding, whether or not they are using different types of travel documents that had not been previously identified. These are some of the most important things that help us better deploy our resources and assets.

Senator SINEMA. Thank you.

A follow-up on this question for Ms. Patel. Do you have specific recommendations to help maintain the right balance between security, privacy, and civil liberty concerns when it comes to the work that I&A does to combat these TCOs and identify broader challenges?

Ms. PATEL. Thank you for the question, Senator. I think I have tried to identify those which are basically that I think it is important that we focus on violence. My concern is that there is a tendency to really broaden the aperture through which we look at threats so that we are looking across, different narratives and grievances and social media in an effort to winnow it down. What I would suggest is that instead we identify violent actors, which we have done certainly over the last several months as well, and then fan out from there in an effort to really constrain I&A to focus its work on the most dangerous people.

Senator SINEMA. Thank you. I appreciate that.

Mr. Chairman, I do have another question for Mr. Sena, but since my time has expired, I will submit it for the record.

I yield my time back, and I thank you for this hearing.

Chairman PETERS. Thank you, Senator Sinema.

As we start wrapping up here, I have one more question here actually for Mr. Sena. We have talked a great deal here at this hearing about the unique aspect of I&A and how they share information with State, local, tribal, territorial governments. We hear work with fusion centers, of course, is the center of all of that.

You mentioned in your opening testimony that you had some specific actions that you would recommend to strengthen the sharing of relevant, timely, actionable intelligence information across those centers. If you could share with the Committee some of those actionable ideas that we should consider?

Mr. SENA. Absolutely. One of the biggest pieces is that lack of the personnel resources that are on the ground. Whether it is intelligence officers, collections managers, reports officers, we have to have people in the local area, in the local regions across the country that have the capacity to share information in real time and to work closely with the FBI Field Intelligence Company and the Joint Terrorism Task Force and in that fusion center collocated environment. We need technology. Right now the Homeland Security Information Network is riding on technology that is, in some cases 18 years old. We need that capacity to have tools and resources that are easily accessible by all of our leaders out there, not just the folks in the fusion centers, but all of our partners.

We also need folks that are on the ground to help support the privacy, the civil rights, the civil liberties training, and I&A can play a pivotal role in that capability. We also need the capacity to have, personnel on the ground, that when we run into whether it is bureaucratic or whatever the hurdles may be, the fact that we

have centers right now that cannot get the critical data they need to prevent terrorist acts, to prevent major criminal threats, it is abysmal. Here we are almost 20 years later, and we do not have that capacity, so having advocates there—I often say that I get more done by having a DHS Regional Director three doors down from me than I do with many of the calls that we have in Washington, D.C., because that is where the rubber meets the road. That is where things get done. It is done at the local level because that is where the threats are.

I see the formation of I&A pivoting what has happened over the last number of years where the focus has been not as much on the State, local, tribal, and territorial partners, who are at the local level and looking at more of a larger intelligence community framework. There are lots of folks in the intelligence community that do a great job within their avenues of what they do. But the real strength of DHS I&A is with their State, local, tribal, and territorial partners. It really is, because that is where the information is at. That is where the threat is. That is where we are dealing with the opioid and overdose epidemics. That is where we are dealing with transnational criminal organizations. That is where we are dealing with domestic violent extremists and every other violent extremist and having the personnel there. We cannot do this with a little over 100 people. We have to have more folks in the field, and I agree the mission center idea is great, but it needs to incorporate those State, local, tribal, and territorial partners to be effective. And I&A in their unique role has the ability to be our champion for that State, local, tribal, and territorial community. I think that is where they need to be uplifted to, but they need the resources from Congress to make sure that they have capacity to achieve what they should be and what they were designed to be after September 11th. Thank you, sir.

Chairman PETERS. Thank you. Thank you for that answer. Thank you again to all of our witnesses here today for giving us your time and your expertise this morning.

This hearing is a part of our Committee's bipartisan effort to examine the security and intelligence failures on January 6th as well as to identify what reforms are needed to address the rising threat of domestic terrorism generally across the country.

Our witnesses today focused on the importance of I&A and how it needs to provide DHS and its partners—State and local governments, law enforcement, and the private sector—with more actionable intelligence. We also discussed the unique position of I&A as a domestic-focused intelligence agency and the need to ensure that we protect the privacy, the civil rights, and the civil liberties as they work to execute their mission.

I certainly look forward to working with my colleagues as we continue to examine how to combat the rise of domestic terrorism, including white nationalism and anti-government violence. Certainly I&A is the member of the intelligence community that is uniquely situated and suited to interact with both State and local enforcement, focus on strategic issues rather than specific law enforcement investigations, and leverage its existing domestic authorities to help us address that threat.

So, with that, the hearing record will remain open for 15 days, until June 2nd at 5 p.m., for the submission of statements and questions for the record.

This hearing is now adjourned.

[Whereupon, at 11:38 a.m., the Committee was adjourned.]

APPENDIX

Chairman Peters Opening Statement As Prepared for Delivery
Full Committee Hearing: Examining the Role of the Department of Homeland Security's Office of Intelligence and Analysis
May 18, 2021

Today, we will hear from former homeland security intelligence officials, as well as national security and civil rights experts, on their views of the appropriate roles, responsibilities, and authorities for the Department of Homeland Security's Office of Intelligence and Analysis.

I would like to thank each of our witnesses for joining us today, and for their work in the public and private sectors to protect the American people.

Today's testimony will give the Committee critical insight into how the Office of Intelligence and Analysis operates, and what role it should play in providing threat assessments and domestic terrorism intelligence to Department of Homeland Security leadership, state and local law enforcement partners, and other private entities.

We will also hear testimony on how to ensure citizens' fundamental civil rights and civil liberties are safeguarded as we work to better tackle a rising domestic terrorism threat.

Earlier this year, the Committee heard about how systematic breakdowns in planning and preparation led to a deadly attack on the U.S. Capitol, the heart of our democracy.

The Office of Intelligence and Analysis, along with other intelligence and counterterrorism agencies, failed to effectively identify the threat on January 6th.

We need to understand the factors that led to that failure, and what concrete steps can be taken to better understand the current threats we face, and ensure the Department of Homeland Security is effectively sharing that information with state and local law enforcement.

I appreciate the hard work and dedication of the national security experts in the Office of Intelligence and Analysis, and recognize they have faced challenges that must be addressed. However, it is apparent that the office must also do more to effectively counter the rising threats posed by white supremacist and anti-government violence that threaten communities across the country.

One of the greatest challenges the Office of Intelligence and Analysis has faced is the pressure to politicize domestic terrorism threats. Under the previous Administration, the office reportedly downplayed the threat posed by white supremacist and anti-government violence, and reportedly censored some intelligence information under pressure from President Trump.

At times, this political pressure led to problematic and inaccurate analysis related to peaceful protest movements, overstating the roles of certain groups, and even reportedly developing intelligence on American journalists.

Our national security and the safety of Americans cannot depend on political whims or individual leaders' biases.

That is why Congress must work to ensure that analysis conducted by the intelligence community is separated from the political environment, and based in facts and data that accurately assesses security threats.

The office also struggles with employee morale, a challenge identified in Government Accountability Office reports and employee surveys, possibly because of a lack of consistent leadership and direction.

Since this office was first created nineteen years ago, it has had more than a dozen different leaders. Only three of those individuals, including one of our witnesses today, led the office for more than two years.

These obstacles, and other challenges, must be addressed quickly. Our nation faces very real and deadly domestic terrorism threats, and our national security agencies must ensure our counterterrorism efforts and resources align with those threats.

A recent, long-delayed joint report from the FBI and DHS identified racially or ethnically motivated extremists, primarily white supremacists, as the most significant national security threat based on data from recent years.

While I appreciate the initial steps the Biden Administration has taken to begin addressing the alarming rise of these threats, its clear there is more work to do. American lives are at risk, and we must ensure we are taking all appropriate action to safeguard the American people, and protect their most fundamental rights.

I look forward to hearing from our witnesses, who bring unique perspectives on how we can improve the Office of Intelligence and Analysis to meet our security goals.

I have no doubt, that this Committee can work in a nonpartisan way to strengthen our homeland security and protect Americans from all threats, foreign and domestic.

Opening Statement
Ranking Member Rob Portman
U.S. SENATE COMMITTEE ON HOMELAND SECURITY
& GOVERNMENTAL AFFAIRS
"EXAMINING THE ROLE OF THE DEPARTMENT OF HOMELAND SECURITY'S OFFICE OF INTELLIGENCE & ANALYSIS"
MAY 18, 2021

Thank you, Chairman Peters. It's important and timely for us to be holding this hearing today to examine the Department of Homeland Security's Office of Intelligence and Analysis (I&A).

DHS is responsible for protecting the homeland, and I believe its intelligence and analysis capabilities are essential to this effort. I look forward to discussing how to best equip the Department and its partners with critical, timely, and actionable intelligence to keep our nation safe from both foreign and domestic adversaries.

The events of January 6, domestic terrorism, recent attacks on federal facilities and law enforcement, Mexican and other foreign cartel networks operating in our cities, and the ongoing threat posed by foreign terrorists all underscore the need for ongoing intelligence and analysis focused on identifying and mitigating threats to our country.

Since its inception, DHS has had an intelligence office to support its mission. Congress underscored the importance of intelligence and information sharing in the *Implementing Recommendations of the 9/11*

Commission Act of 2007, which formally established the Office of Intelligence & Analysis (I&A).

While one of the smaller agencies in the Intelligence Community (IC), I&A is the only IC member charged with delivering intelligence to our state, local, tribal, territorial, and private-sector partners and developing intelligence from those critical partners for the Department and the IC. To put it simply: I&A is intended to facilitate a key layer of communication and domestic coordination required to safeguard the nation.

In my home state of Ohio, the three fusion centers have benefitted greatly from the partnership with I&A. I have visited the Cincinnati fusion center where I learned the importance of the support and partnership that I&A provides. For example, I recently learned that an I&A intelligence officer at the Columbus fusion center provided critical information on a suspect that had a plot to cause mass violence at large music concert event in Columbus. By leveraging I&A's capabilities, the Columbus fusion center was able to quickly work with law enforcement to locate the suspect and place this individual on TSA's no-fly list. The suspect was then intercepted while attempting to board a flight on his way to Columbus to carry out the attack.

The Committee learned from our oversight investigation into the January 6 attack on the Capitol that I&A fell short in reporting on the potential threat. Security officials have cited the lack of intelligence

and information sharing from I&A and other intelligence agencies as a reason law enforcement was not better prepared to respond. In our investigation, the then Acting Under Secretary of I&A revealed weaknesses in how I&A distributes information, collects intelligence from social media platforms, and leverages its relationships with state, local, tribal and territorial, and private sector partners to learn of new, evolving threats.

Notably, I&A has an important role to play in combatting the transnational criminal organizations (TCOs) – including those responsible for drug trafficking, violence, human smuggling, child exploitation, and a host of other criminal activities. TCOs are always evolving and adapting to maximize their profits as they did as COVID-19 reshaped supply chains and transport patterns. In fact, according to the DEA, once they adjusted to the initial disruption of COVID, Mexican cartels "reinforced supplies of precursor materials, increased production and are sending larger fentanyl and methamphetamine loads into the US." It seems more important than ever for Federal and local partners to be in close coordination to understand and combat these dynamic threats. And, while these challenges are national, they have hit local communities, including many in my home state of Ohio, particularly hard.

There are a number of issues I hope we will explore today.

There are differing opinions on what I&A's role is in regard to intelligence collection, production, and dissemination. In my view, having timely, quality intelligence is an essential component of keeping our communities safe. I hope today that we can talk about how DHS can appropriately provide these capabilities at a time when we face some threats that are home grown.

The threats we face are dynamic and becoming more complex every day. And they aren't all focused on Washington, D.C. Considering the current environment, how can I&A best leverage the fusion centers and its partnerships with state, local and private sector partners to meet the needs of the department charged with the security of our homeland?

Finally, over the years, I&A has faced challenges in recruiting qualified talent and has experienced consistently low morale and high rates of attrition. I hope that our witnesses can help us understand what can be done to address these longstanding issues.

General Taylor, Ms. Cogswell, Mr. Sena, and Ms. Patel, I am looking forward to your testimony and answers.

Thank you.

Statement of Francis X. Taylor
Former Under Secretary, Office of Intelligence and Analysis,
Department of Homeland Security
Before the Senate Homeland Security & Government Affairs Committee
May 18, 2021

Chairman Peters, Ranking Member Portman, and members of the Committee, thank you for the opportunity to testify on the future of the Office of Intelligence and Analysis.

I&A's mission is integral to DHS, the intelligence community, and to the security of our nation. It is the only US intelligence agency that is specifically chartered to provide intelligence support to State, Local, Tribal, and Territorial, as well as private sector partners to improve the flow and quality of information sharing across our Nation. As the intelligence arm of DHS, I&A has a responsibility to support the intelligence needs of the senior leadership of the Department, to ensure that relevant intelligence from the IC is shared systematically with our State, local, tribal, territorial and private sector partners and that relevant information from these partners becomes intelligence that is shared with the broader IC. As the Chief Intelligence Officer for the Department, I&A coordinates and deconflicts the efforts of the DHS intelligence enterprise to meet the intelligence needs of the Department and our IC partners. Additionally, the Under Secretary's responsibility to lead the information sharing and safeguarding entity of the Department provides a unique opportunity to use the myriad of data generated by DHS and turn it into effective information to share with our SLTT, federal and international partners.

When President Obama nominated me to become the Under Secretary, I needed to understand the organization's mission, how the mission was being executed, by whom, what the results were from the mission effort and how customers felt about those results. I quickly learned that the organization was internally disconnected and, depending on the audience, was seen as ineffective. The organization did not have a clear standard of mission execution. It was bloated with SES leaders and many of these leaders were not focused on the coordinated collection, analysis and dissemination of the intelligence that I&A's customers were seeking. After my confirmation, I spent considerable time examining the organization at every level and determined that the organization needed a consistent mission focus with measurable outcomes, customer feedback and a clear process to adjust priorities and products as customer requirements changed and the threat evolved. So, we reorganized the organization, cut the number of senior executives in half and focused on unity of command in the execution of the intelligence mission. I established a Deputy Under Secretary for Intelligence Operations and charged that leader with responsibility for organizing and executing intelligence operations that support the Secretary and the Department's leadership, our state in local tribal and territorial partners and the IC. We developed clear metrics around performance and outcomes, developed a clear and consistent operating review process that allowed us to discuss our progress and made adjustments as the mission requirements changed over time. That organization was essentially dismantled in the last

administration but not replaced. It is my understanding that the priorities changed consistently, ideas for the new initiatives we're not always met with action, and the morale of the organization continued to devolve. I&A needs to return to the basics of intelligence production and customer feedback to adjust priorities.

Restore Trust

I&A leaders will need to focus on rebuilding trust with key stakeholders within and across DHS and the Intelligence Enterprise (IE), as well as externally, with the broader IC and Congress. Controversies surrounding, I&A activities, and use of its intelligence authorities in recent years, have undermined its reputation and raised questions about the integrity and objectivity of the information it provides to stakeholders. In order to rebuild stakeholder and public trust, I&A will need to focus on advancing its core mission and demonstrating that it brings invaluable mission expertise to its customers.

Secretary Mayorkas should be commended for the recent creation of an I&A domestic terrorism branch and re-committing I&A to producing sound and timely intelligence on the domestic terrorism front. However, in order for I&A to effectively fulfill its mission, it must take additional steps to refocus on production of quality intelligence and analysis.

I&A will need an active engagement strategy focused on Congress and oversight entities. It must invest in building and sustaining open and transparent relationships with members and staff of core oversight committees in Congress. I&A should restart regular intelligence briefings to appropriate committees and adequately resource its legislative outreach to respond to congressional inquiries and requests, particularly in light of congressional interest in reforming I&A through legislation. I&A should work to restore confidence in the value it provides to DHS, the IC, and its state, local, tribal, and territorial (SLTT) partners, and position itself once again as an important player on matters of intelligence among oversight bodies.

Focus on SLTT and Private Sector Partnerships

I&A must continue making investments in its SLTT and private sector partnerships. One of the distinguishing features of I&A's integrated missions is its ability to share information with state and local partners through centers across the United States. I&A's field organization of intelligence and collections officers allows access to potentially relevant intelligence information from state and local law enforcement that can be leveraged to identify threats across the IC and DHS components, particularly on issues such as domestic terrorism. Moving forward, I&A should focus on effective prioritization of its information sharing activities, ensuring that they meet the needs of state and local law enforcement and yield intelligence information that could be useful to the broader IC,

as a compliment to the FBI. Likewise, I&A should continue to engage its partners in private industry to gain perspectives on the national and homeland security challenges facing their sector and ways to facilitate public-private partnerships.

Reinvent Intelligence Analysis for DHS and the IC

I&A leaders should focus the office's intelligence analysis activities on the creation of intelligence products that draw on unique DHS data sets and data science, within a robust framework for privacy and civil liberties. I&A can be the leading player in government focusing on data science to create unique insights and produce clearly differentiated intelligence products. With access to special data sets and a focused set of priorities, I&A can lead the IC in re-inventing intelligence analysis. I&A can do this by focusing on the development of intelligence analysts who have data science skills and are trained to exploit data and discover non-obvious correlations and findings. In addition, I&A must reinvigorate its relationship with DHSs Office for Civil Rights and Civil Liberties (CRCL) and the Privacy Office. Regular communication and fast and flexible coordination with these offices is central to ensuring that I&A's intelligence products and analysis comply with applicable legal, policy, and statutory requirements.

Bolster Mission Centers

The one area where previous I&A leaders and I have agreement is agency focus on mission centers. However, that focus did not receive sustained attention from management and therefore had uneven outcomes. If organized effectively, mission centers are well positioned to utilize the information they receive from DHS components. I&A leaders should take care to establish metrics which can be used to ensure the centers are serving their purposes. Success of mission centers should be touted as an example of DHS capabilities and operational support. I&A should create a budget, annual strategy, metrics and fully resource each mission center to appropriately support the needs of the intelligence enterprise components, the Department leadership and the broader IC. .

Lead in Data Analytics using the unique data generated by the Department

DHS generates a tremendous amount of relevant information in its daily mission activities. When I was there, that information sat in more than 900 independent and unconnected data bases that were not available beyond the owner of the data base. With significant Congressional and Departmental support, we launched a data framework to begin the process of integrating DHS data more effectively in the Department and where appropriate make that data available across the government agencies that needed that information. That initiative has stalled and needs to be restarted. The collaboration of information and connecting the dots is why the Department was created, this effort is essential for the Department to meet its mission responsibilities.

Invest in Workforce/Human Capital Initiatives

In order to continue advancing its vital mission within DHS, I&A must dedicate significant focus to workforce development and human capital. I&A leadership must prioritize attracting talent in early career stages, investing in training and new skills such as data science, and promoting the career development of I&A's intelligence professionals. Given the competition I&A faces in recruiting and retaining talent from within government and externally, it needs a workforce and human capital strategy to build a flexible, diverse, and experienced cadre of professionals equipped to meet its mission needs. Furthermore, I&A needs to offer its professionals a true career path. Entry-level employees must see that they can rise within the organization to assume key leadership positions such as Under Secretary, as is the case at other intelligence agencies. There is also a need for I&A to adopt a data-driven approach to understand and manage its intelligence workforce, which includes the ability to identify gaps or trends in attrition and retention,

Focus on Employee Morale

The lack of consistent leadership, negative press, and building relocations have weakened the morale of I&A's workforce. Therefore, incoming I&A leaders will need to focus on uniting personnel behind the I&A mission, recognizing the role they play in new opportunities shaping its future, and the importance of their contributions in keeping the country safe. During my tenure, we were able to improve morale in a statistically significant way. My focus was on listening to the people, addressing their concerns with definitive action to fix problems. We created an employee advisory council that allowed a consistent process for employee to raise concerns for redress. We focused on rewarding great performance and ensuring poor performance did not go unaddressed. People respond to clearly concerned leadership.

DHS I&A has a needed mission to the Department, the State & Local and private sector partners, and the IC. There is a clear lane for I&A to produce unique DHS intelligence with information colleting across the operational components that is valuable to all U.S. Government leaders. There is critical role for I&A to play in data analytics across the Department and through the essential mission centers. Above all, I&A must be apolitical and speak truth to power as is the responsibility of all intelligence professionals. There is an exciting future for I&A because there are men and women who go to work there every day to make a positive difference in the lives of all Americans.

I look forward to answering your questions. .

TESTIMONY
OF
PATRICIA F.S. COGSWELL
SENIOR STRATEGIC ADVISOR FOR NATIONAL SECURITY
GUIDEHOUSE

For the

UNITED STATES SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

"Examining the Role of the Department of Homeland Security's Office of Intelligence and Analysis"

May 18, 2021

Chairman Peters, Ranking Member Portman, and distinguished members of the Committee, thank you for the opportunity to testify before you this morning, as you examine the role of DHS' Office of Intelligence and Analysis (I&A). The comments I share with the Committee today are informed by my 24 years of federal service, my tenure as a founding member of DHS serving on Day 1, and the varied capacities in which I have both led and worked with DHS I&A.

During my tenure at DHS, I served in multiple leadership roles including with three Headquarters elements and three different DHS component agencies, as well as completing a nearly 3-year tour at the National Security Council (NSC). In those roles:

- I was a consumer of DHS I&A's intelligence products, when I served as the Deputy Assistant Secretary for Screening Coordination in DHS' Office of Policy, as Special Assistant to the President for Transborder Security at the NSC, and, most recently, as Deputy Administrator for the Transportation Security Administration (TSA).

- I was a member of a fellow Headquarters office while at DHS Policy, working jointly with DHS I&A to lead development of strategic and policy initiatives that crossed agencies; collaborate on products for the Secretary and DHS leadership that explained DHS' relevant strategic direction or operational activity in relation to current intelligence; and to lead DHS governance processes, including the Information Sharing and Safeguarding Committee, to ensure that those processes provided timely direction and support for DHS mission needs.

- I was a member of the Homeland Security Intelligence Enterprise, as the Assistant Director for Intelligence for Immigration and Customs Enforcement, working with I&A to inform strategic direction, policy, priorities, requirements, and production.

- And I led I&A, serving as the Acting Under Secretary while the nominee was undergoing confirmation.

Based on those experiences, I found that the highest value roles for DHS I&A were to:

- Support the Homeland Security Intelligence Enterprise. Similar to the Undersecretary for Defense for Intelligence (USD(I)), the Under Secretary, as the DHS Chief Intelligence (CINT) Officer, in collaboration with the Homeland Security Intelligence Council (HSIC), should lead development of strategy, policy, and an integrated set of priorities, including training and budget. DHS I&A should support this governance process.

- Advocate for DHS mission intelligence needs to the Intelligence Community (IC) and through the budget process. DHS I&A should enable and support the DHS mission, including advocating on behalf of DHS operators and policy personnel. This includes enabling DHS access to IC information and tools, ensuring that homeland collection needs are prioritized, and advocating for resourcing for specific capabilities through both the IC and DHS processes. During my tenure, I saw a successful example in the enhancement of DHS' counterintelligence program. I&A, working with component representatives, co-created a joint budget enhancement request that resulted in additional appropriations, and deployment of dedicated staff to both headquarters and component agencies. It's also important to note the intentional use of the word "advocate." Productive relationships exist between DHS organizations and the IC, such as those I experienced working at both ICE and TSA; DHS I&A should support and foster such partnerships, rather than on being a gatekeeper.

- Provide the Secretary, Deputy Secretary, and headquarters organizations with intelligence services. DHS Policy and other headquarters elements are often tasked to attend interagency meetings to develop policy and to support the Secretary and Deputy in Departmental and interagency decision with their counterparts. DHS I&A should collaborate with other HQ offices to ensure that they, and the Secretary and Deputy Secretary, have access to the same high-quality intelligence their counterparts do. DHS I&A should also be able to provide the Secretary, Deputy Secretary, DHS and other homeland senior leaders with a complete "state of the homeland" intelligence picture to inform policy and operational decisions, and effectively manage risk.

- Coordinate production of "sense of the community" analyses to support DHS and homeland security-unique needs with the HSIC. In addition to products like the Homeland Security Threat Assessment, the CINT should seek to provide "sense of the community" products to support DHS decision making. Critical to the success of these products is that they are led by the DHS entity best positioned to speak on behalf of the entirety of the information, including not only traditional intelligence information and law enforcement information, but also analysis developed by DHS in support of its ongoing programs, and by other knowledgeable stakeholders, such as academia, think tanks, and associations, and that the products are scoped to answer the questions relevant for the conversation. These types of products must developed through a collaborative

process. While the entity best positioned to speak to the information should lead the content development, DHS I&A can manage the coordination process and support the development of these products.

As an example, DHS I&A may be best to lead the development of an assessment on terrorism in support of a discussion on issuing a National Terrorism Advisory System Bulletin. But Immigration and Customs Enforcement and Customs and Border Protection are likely best to lead an assessment of cross-border trade violations in support of a discussion about how to update programmatic direction or legislation.

- Engage the fusion centers. DHS I&A staff should support state, local, territorial, and tribal partners with training, information, and all source analysis that helps partners, based on the partner's needs. As fusion centers differ, the services provided by DHS I&A personnel assigned to those centers will differ.

- Collaborate with other DHS entities to enable an effective information sharing environment. DHS I&A should support the design and funding of technical architectures and multi-use tools that enhance DHS's ability to match and exchange information, where appropriate, to achieve their missions. To do so, they will need to collaborate with the DHS operating component as well as with a number of DHS headquarters offices, including: DHS Policy; the Chief Information Officer; Privacy; Civil Rights and Civil Liberties; and General Counsel. DHS I&A's support to the National Vetting Center, housed at Customs and Border Protection, is a positive example of this role.

Over my tenure, I've seen DHS I&A perform all of these functions. I can cite positive examples, and highlight the great work of numerous personnel. DHS I&A should work to ensure that it can perform well consistently, across these functions and with variance appropriate in approach based on needs and capabilities of its partners. I've also seen DHS I&A seek to fill other roles over that time, which overlapped or competed with existing activities already underway by others in DHS or in partner organizations. DHS I&A is an important member of DHS. DHS I&A can make the greatest mission impact by leading in those unique areas where others aren't already operating, and by supporting and enabling others in the areas already within their missions.

To effectively perform the six roles outlined above, DHS must address DHS I&A staffing and morale. Improving morale is not just good from the perspective of caring for the workforce – its also a national security imperative. Based on my experiences, there are a few areas where improvements would have some of the greatest effect on DHS I&A staff morale.

- Stabilizing organizational structure, mission, and role. At my first town hall as acting Under Secretary, I was asked if I was going to reorganize or issue updated priorities. When I said I expected to continue the direction of the previous acting, who at that point was in the confirmation process, had started, they seemed relieved. They workforce needs continuity and consistency that lasts more than the term of one Under Secretary and one Secretary.

In addition, the workforce needs a mission that is unique and valued. DHS I&A employees are understandably frustrated when they are perceived as duplicating the roles of others in DHS, or within the IC. DHS I&A leadership should identify areas that are unique, and where they can be recognized as having subject matter depth – rather than trying to synopsize or "integrate" other's work where they don't.

- Enhancing career development opportunities. While personnel at DHS I&A, as members of the intelligence community, are required to complete joint duty assignments, they often lack understanding of and direct experience with DHS component mission sets. Not only does this inhibit their ability to partner with others in DHS to develop well-rounded intelligence products, but it also limits their career options, particularly at senior levels. This, in turn, can limit innovation and creativity. Employees who see their career development limited are also less likely to invest in developing junior staff, or to bring in new talent to increase the diversity of perspectives needed address emerging threats.

  DHS I&A leadership should invest in changes that will provide supervisors incentives to positively coach and mentor their personnel, and career paths that enable staff to change organizations – either to intelligence community entities, or to DHS component agencies – increasing their opportunities and exposure to the wider national and homeland security mission.

- De-politicizing products, and career staff. By its nature, intelligence analysis is intended to look at difficult problems and emerging threats, and assess potential vulnerabilities and risks. These assessments are not always comfortable – and may not align with what the consumer wants to hear. This is difficult when assessing foreign actors and threats; it's all the more difficult when looking at domestic threats, such as domestic violent extremism or domestic terrorism risk given the need to appropriately address first amendment rights, privacy, and other civil liberties concerns. While politicization concerns have increased in recent years, DHS I&A has faced criticism over many administrations.

  It's entirely appropriate for, and the intelligence community expects, intelligence product consumers to closely examine and critique the analytic tradecraft and data sources used in making an assessment. It's also appropriate for knowledgeable people to assess the same data differently. This is why the intelligence community allows for dissenting opinions.

  DHS I&A should seek to enhance its strategic communications with its customers and stakeholders, particularly those who may not regularly receive intelligence products other than those from DHS I&A. Consumers need to understand how DHS I&A selects the topics it analyzes and its production development methodology, and have additional opportunity to provide feedback and input. DHS I&A should also seek support from partners and oversight, such as from this Committee, for efforts in areas that may become controversial.

As this Committee examines DHS I&A's role, I would encourage you to think about the high-value roles, and the changes needed to improve DHS I&A morale that I outlined above, as

building blocks for a mature organization that fills a critical role in the homeland security enterprise. Organizational, transformational, and cultural change take significant investments in time, in developing and maintaining talent, in a willingness to measure impact and modify activity based on the results, and in commitment to strategic communications, both internally and externally. As you consider changes, I would encourage you to develop them in a way that will support the organization over years to come, and will survive both the test of time, and changes in Administration.

Thank you again for the opportunity to testify before you today. I look forward to your questions.

Statement of

Mike Sena

President, National Fusion Center Association

Director, Northern California Regional Intelligence Center (NCRIC)

United States Senate
Committee on Homeland Security and Governmental Affairs

"Examining the Role of the Department of Homeland Security's Office of Intelligence and Analysis"

May 18, 2021

Chairman Peters, Ranking Member Portman, Members of the Committee,

My name is Mike Sena, and I am the Director of the Northern California Regional Intelligence Center (NCRIC), which is the fusion center for the San Francisco Bay and Silicon Valley region from Monterey County to the Oregon border. I currently serve as the President of the National Fusion Center Association. The National Fusion Center Association represents the interests of 80 state and major urban area fusion centers, and over 3,000 public safety employees. On behalf of the NFCA and our executive board and regional co-chairs, thank you for the opportunity to share our perspective on the important role the Department of Homeland Security's Office of Intelligence and Analysis (I&A) plays in supporting the National Network of Fusion Centers and State, Local, Tribal and Territorial intelligence and information sharing efforts overall.

Fusion centers were created by state and local governments across the nation in the aftermath of September 11, 2001, to assist in the identification, prevention, mitigation, response and recovery of terrorist acts and other major threats to public safety and the lives of every citizen in our country. Fusion centers bring together law enforcement, public safety, fire service, emergency response, public health, and private sector security personnel to understand local implications of national intelligence and add state and local information and context to federal intelligence, thus enabling local, state, and federal officials to better protect our communities.

The National Network of Fusion Centers (National Network) is the hub of much of the two-way intelligence and information flow between the federal government and our State, Local, Tribal and Territorial (SLTT) and private sector partners. The Office of Intelligence and Analysis (I&A) is the only U.S. Intelligence Community element that is statutorily charged (Section 210A of the Department of Homeland Security Act) with supporting our network. An effective and active Office of I&A is critical to SLTT partners across the nation to be able to identify, deter, or respond to threats to our communities. Therefore, the strength of the National Network depends in part on I&A's ability to help fusion centers and their partners develop capacity to analyze and share threat-related information.

Strengthening I&A's ability to support the National Network requires I&A to reorient its focus to supporting SLTT partners overall. In other words, ensure a primary focus on the "H" in DHS. This can be accomplished by increasing the forward deployment of well-trained and experienced personnel to fusion centers; offering high-quality training in analytics and privacy, civil rights, and civil liberties; investing in modernizing information sharing systems and technologies; and ensuring reliable access to critical data, including classified data.

DHS Strategy for Engagement with Fusion Centers

In March of 2020, the President signed into law the bipartisan DHS Field Engagement Accountability Act (Act), now Public Law 116-116. The Act requires DHS, in consultation with fusion center officials, to develop an engagement strategy with fusion centers, study the performance metrics of deployed personnel to fusion centers, develop policies to ensure effective use of the Homeland Security Information Network (HSIN) and submit reports to Congress on these topics. The National Network and the NFCA welcome this effort and are prepared to assist in providing guidance and technical assistance to our Federal partners.

However, we are not sure whether the deadlines specified in the Act have been met, including a one-year deadline for development of the strategy, 180 days for the personnel performance metrics, and 180 days for the development of policies to support HSIN. We have submitted areas of focus for the plan, that includes previous recommendations from Congress, but to my knowledge, fusion centers have not been formally consulted by the Department in the development of these requirements at this point.

The National Network understands first-hand the growth and improvement that can result from an organizational strategy. In 2013, the United States House of Representatives Committee on Homeland Security released a Majority Staff Report on fusion centers and identified the lack of a comprehensive state and locally driven National Strategy for Fusion Centers as a barrier to the National Network reaching its full potential. In response to this report, the NFCA established a National Strategy Development Team and Executive Steering Committee to create the 2014-2017 National Strategy for the National Network of Fusion Centers. In 2018, the NFCA led an effort to review the 2014-2017 National Strategy and publish the 2018-2021 National Strategy, which can be an instructive guide for the Department in the development of the strategy required by the Field Engagement Accountability Act.

Deployment of I&A Personnel and Training

One of the primary objectives of the fusion center strategy is enhancing analytical collaboration in the field. The support provided by I&A personnel assigned to fusion centers is critically important. We strongly encourage I&A to prioritize the deployment of well-trained and experienced I&A intelligence professionals throughout the network.

Currently, I&A only has a little more than one hundred personnel deployed across the nation. This is simply not sufficient. There are a total of 15 fusion centers that lack an assigned intelligence officer, and 7 fusion centers lack any I&A presence at their centers. Additionally,

fusion centers are not consulted by I&A when the Department makes decisions on deploying field-based resources to ensure best alignment with the centers' missions and needs. I&A has struggled with their deployment of personnel for years and that struggle has included limitations by Congress on the number of personnel assigned to fusion centers.

The NFCA strongly encourages Congress to support increased funding for I&A to ensure it can hire, train, and deploy an adequate number of personnel across the Nation. Every fusion center should have an I&A intelligence professional with the authority to collect and share raw information to include release authority, execute joint production, and effectively share 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 center directors and I&A. This has created gaps in several fusion centers that do not have dedicated DHS I&A personnel filling critical roles 100% of the time at their centers.

In addition to the assignment of personnel, DHS 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 and federal analysts 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 civil rights and civil liberties protections. With many analysts and centers adapting to remote working environments, and limited by travel and budgetary restraints, more virtual training opportunities are needed.

Federal Funding for Fusion Centers

In March, DHS Secretary Alejandro Mayorkas testified before the House Homeland Security Committee about the importance of ensuring that fusion centers have sufficient resources. Today, there are no direct DHS funding sources for fusion centers. The indirect funding models vary widely across the National Network, some centers are nearly entirely grant-funded through the Urban Area Security Initiative (UASI) and/or the State Homeland Security Grant Program (SHSGP), and some receive almost no federal grant funding. Overall, more than two-thirds of all funding that supports fusion centers comes from state and local budgets.

The NFCA strongly supports the Law Enforcement Terrorism Prevention Activities (LETP) requirement in the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L.

110-53). That law requires that 25% of SHSGP and UASI funding be used for "law enforcement terrorism prevention activities" and specifies some types of activities including support for fusion centers. While states and designated urban areas have latitude to allocate funding according to risk and priorities, we agree with the intent of the 2007 law and believe that terrorism prevention and threat information sharing activities should be a constant priority. However, I&A must coordinate with FEMA to ensure that grant guidance and funding are more closely aligned with the needs of state and local partners.

Currently, fusion centers' support to federal, state, and local public safety partners is being limited or denied for potential life and death critical incidents and immediate requests for assistance by the FBI's Joint Terrorism Task Force (JTTF). Fusion centers must obtain pre-approval to use grant funding for unknown threats or future unknown requests for assistance from the JTTF months prior to receiving the threat or the request. Neither fusion centers nor the JTTF have a crystal ball to identify those threats ahead of time, but we are being asked to forecast the unknown. Over the last month, Secretary Mayorkas has promised to work with all public safety stakeholders to improve the alignment of the grant processes to decrease the current gaps and enhance our ability to protect America. We are greatly encouraged by his commitment and support to improve the current grant funding process.

Access to Data

Access to local, regional, state, and federal sources of information from law enforcement records, criminal intelligence databases, the Homeland Security Information Network (HSIN), Homeland Security Data Network (HSDN), the FBI's Criminal Justice Information Services (CJIS), the Treasury's Financial Crimes Enforcement Network (FinCEN), FBINet, DHS TECS, and tips, leads and threat to life data collection systems allow fusion centers to add local and regional context to national intelligence, as well as provide information and value-added intelligence to support counterterrorism and other criminal investigations that would otherwise be difficult or unlikely for lead Federal, state, or local investigative agencies to obtain.

Each fusion center has methods of information distribution across local, regional, and statewide technical and personal networks that Federal investigative and intelligence agencies themselves could not build or maintain. Some fusion centers still lack access or have trouble accessing critical criminal information databases, like the FBI's CJIS and the Treasury's FinCEN system. We have come a long way from where we were on September 11, 2001, with the expansion of FBI-CJIS National Data Exchange (N-DEx) that brings together over 7,700 Federal, state, and local agencies' records systems, but we have over 18,000 agencies in America that

are not connected to this critical data sharing resource and some fusion centers do not have access to the system either.

After almost twenty years of attempting to overcome critical Federal data access issues, the National Network needs help to break down the barriers that are currently keeping us from the information that we need to protect America from acts of terrorism and other homeland security threats. The fight to access CJIS Data, criminal history information, and financial crimes data must be resolved for the security of our nation. Everyone in America deserves equal levels of protection from their fusion center, whether they are in West Virginia, Ohio, New Mexico, Michigan, or in the seat of our Nation's Capital. I&A can play a supportive role by advocating for appropriate access to federal systems by state and local partners.

Technology Resources

HSIN is an essential tool for the protection and security of our nation. The National Network of Fusion Centers uses HSIN for the trusted sharing of sensitive but unclassified information. Fusion center leaders and analysts use HSIN to access homeland security data, send requests securely between agencies, manage operations, coordinate planned event safety and security, respond to incidents, and share the information they need to fulfill their missions and keep their communities safe. HSIN virtual situational awareness rooms are utilized routinely by the network and other public safety partners during planned and critical events that are associated with physical and cyber threats. Our analysts are trained to make critical contributions on HSIN to prevent terrorism and targeted violence and rely on the free-flowing exchange of information to make real-time, local decisions. We encourage DHS I&A to protect and encourage the free exchange of information on platforms like HSIN. I&A should continue to support the development and enhancement of technology to improve the availability, dissemination, and coordination of information to fusion centers and our partners by looking to more advanced technology that improves access to data for personnel with a need and right the know the information, while maintaining the highest level of security.

Cybersecurity

Furthermore, the National Network is uniquely positioned to address the country's growing physical and cybersecurity threats. Each recognized fusion center has established baseline capabilities related to analysis and sharing of physical and cybersecurity threats. The NFCA has established and supports the Nationwide SitRoom for physical threats and the Cyber Intelligence Network (CIN) room, which provides a collaborative environment for cyber analysts across the country who share cyber intelligence and produce analytic products on cyber threats. Using HSIN, our analysts, including our cyber analysts, share information in real-time,

coordinate and prevent duplication of efforts, and connect analysts nationwide to enhance overall efforts. The physical threat and National Cyber Situational Awareness Rooms have over 500 CIN members that include Federal, state, and local partners outside of the fusion center. I&A should continue to support fusion center cyber capabilities by providing access to critical cyber analysis tools and increasing training opportunities. For example, the DHS Intelligence Training Academy (ITA) provides important cybersecurity training programs to our analysts. However, many of our analysts need more advanced courses to address the cyber threats of tomorrow.

Collaboration to Address the Current Threat

Through the Attorney General's Global Advisory Committee (Global) and the Criminal Intelligence Coordinating Council (CICC) we have helped develop national guidance on fusion center development and information sharing to protect America from physical and cyber threats. We also now have four field-based regional integration plans to improve our steady state and critical incident coordination and collaboration thanks to the support of the Office of the Director of National Intelligence (ODNI), FBI, DHS I&A, the nation's High Intensity Drug Trafficking Areas (HIDTA), and our nation's Regional Information Sharing Systems (RISS) partners.

Fusion centers help to protect America every day through information sharing that saves lives and protects our critical infrastructure. We currently have the largest Global/CICC task team ever assembled writing recommendations and best practice for the collection, triage, analysis, sharing, and response to tips, leads, and threat to life reporting. At this moment, Fusion Centers, the Regional Information Sharing Systems – Western States Information Network (RISS-WSIN) and the FBI CJIS National Threat Operations Center (NTOC) are coordinating the collection, triage, and information sharing of potential threat to life (TTL) reports so that local public safety agencies can appropriately respond to save lives.

We must have the resources, personnel, technology, training, access to data, and the best privacy, civil rights, and civil liberties protections in place to stop the myriad of homeland security threats. The offices of partner engagement within I&A, the FBI, and ODNI must also have direct reporting to and support from the leadership of their organizations to help fusion centers and our partners collectively leverage the incredible resources of our nationwide public safety partners. The growing list of threats to our nation may seem insurmountable, but with the support of all our partners, especially DHS I&A, we can make the vision for a National Network of Fusion Centers after 9/11, into the most effective threat prevention, mitigation, and response resource possible.

Governors across the nation have continued to see the importance of establishing and expanding the National Network of Fusion Centers, as we have grown to a network of 80 centers. On May 6, 2021, the Governors Homeland Security Advisors Council (GHSAC) sent me the attached letter that states that the GHSAC "relies on the National Network of Fusion Centers (National Network) as a key partner in protecting the public. We are happy to reaffirm the importance of and our commitment to the National Network and their crucial role in meeting the threats of today."

On behalf of the NFCA, thank you for the invitation to testify. We are happy to provide input as you work to strengthen the authorities and resources for our partners at DHS I&A that will enable them to support the National Network in ways that are the most relevant and helpful to our members and our partners across the nation.

GOVERNORS
HOMELAND SECURITY ADVISORS
COUNCIL

May 6, 2021

Mr. Mike Sena
President
National Fusion Centers Association
Washington, D.C.

Dear Mr. Sena,

Our country continues to face complex and evolving threats to the health and safety of the American public. This year alone, we have seen a rise in threats from natural and manmade disasters, domestic violent extremism, violent crime, and cyberattacks on critical sectors. It is our responsibility as homeland security advisors to advise the nation's Governors and share critical information and expertise to prevent and respond to such threats. To support our collective homeland security mission, the Governors Homeland Security Advisors Council (GHSAC) relies on the National Network of Fusion Centers (National Network) as a key partner in protecting the public. We are happy to reaffirm the importance of and our commitment to the National Network and their crucial role in meeting the threats of today.

Established in the aftermath of the September 11th attacks, the National Network is comprised of 80 state and locally-owned and operated fusion centers which serve as focal points for collecting, analyzing, and disseminating real-time threat information. The role of fusion centers has since expanded beyond counterterrorism to include an all-hazard approach, underscoring their importance to various mission areas and facilitating collaboration across jurisdictions and sectors to detect, prevent, investigate, and respond to threats and incidents effectively and efficiently.

Now more than ever, Federal, state, local, tribal, and territorial officials are relying on the National Network to ensure the timely and secure sharing of actionable threat information, identify potential suspects, and fully integrate a variety of agencies and departments. A fusion center is comprised of a multidisciplinary set of liaisons from Federal, state and local law enforcement, fire service, healthcare, emergency management, corrections, parole, probation, and many others. They work together 24/7 within their jurisdictions and across state lines to carry out their missions in a manner that ensures First Amendment rights and civil liberties of U.S. citizens are protected while effectively sharing information and ensuring decisionmakers have strong situational awareness and data to make operational decisions.

The National Network continues to provide value in a host of ways and is often at the forefront responding to and mitigating mass casualty incidents, assisting first responders with real-time analysis of the size and scope of incidents, vetting suspicious activity reporting for actionable intelligence, identifying individuals that demonstrate violent intent, and building bridges among partners across the public safety and emergency response disciplines.

In March 2021, U.S. Department of Homeland Security Secretary, Alejandro Mayorkas, testified in front of the House Homeland Security Committee about the importance of ensuring fusion centers have sufficient resources to help partners address ongoing homeland security and public safety threats.

Also in March 2021, Jill Sanborn, Assistant Director for the FBI Counterterrorism Division testified in front of the Senate Committee on Homeland Security and Governmental Affairs and the Senate

GOVERNORS HOMELAND SECURITY ADVISORS COUNCIL

Committee on Rules and Administration about the value of information sharing between federal partners and the National Network of Fusion Centers.

As we mark the twentieth anniversary of September 11th, we must not forget the lessons learned following that incident and continue to strengthen our efforts to disseminate and share accurate, actionable threat information with our Federal, state, tribal, territorial, and local partners. On behalf of the GHSAC, thank you for your commitment to the fusion center network especially during these challenging times. We stand ready to work with you to identify ways to strengthen the partnerships and operational performance of the National Network.

Sincerely,

Lt. Col. Chris A. Kelenske
Chair, GHSAC
Deputy Homeland Security Advisor
Deputy Director, Michigan State Police
State of Michigan

Walter F. "Pete" Landon
Vice-Chair, GHSAC
Director, Homeland Security and Deputy Chief of Staff
Office of the Governor
State of Maryland

BRENNAN CENTER FOR JUSTICE

Written Testimony of

Faiza Patel
Co-Director, Liberty & National Security Program

Brennan Center for Justice at New York University Law School

Hearing: Examining the Role of the Department of Homeland Security's Office of Intelligence and Analysis

Before the United States Senate
Committee on Homeland Security and Governmental Affairs
Tuesday, May 18, 2021

Chairman Peters, Ranking Member Portman, and members of the Committee, thank you for inviting me to testify regarding the role of the Office of Intelligence and Analysis (I&A) of the Department of Homeland Security (DHS).

As our country faces up to the persistent problem of white supremacist and far-right violence, as well as a range of other threats, I&A has the potential to play a constructive role in providing accurate and unbiased intelligence to help guide the response. At the same time, I&A must ensure that its intelligence collection efforts and the threat analyses it produces and disseminates do not infringe on civil rights and civil liberties. This is necessary both to protect our constitutional rights and to maintain the office's legitimacy. Given the serious concerns raised by I&A's past targeting of protestors and Muslim Americans, this requires, at a minimum, the revitalization of oversight mechanisms and clarity on how the office will separate First Amendment protected speech and activities from threats of violence.

Introduction

The Office of Intelligence and Analysis (I&A) supports the mission of the Department of Homeland Security (DHS) by gathering, receiving, analyzing, and sharing intelligence.[1] While I&A does not itself have enforcement functions, it provides terrorism-related analyses to federal, state, local, tribal, and territorial entities, many of which are law enforcement agencies who may act on it within their jurisdictions. The office also shares analyses with private sector and international partners and with other parts of DHS that carry out enforcement responsibilities.[2] Much of this sharing of information occurs through fusion centers, which were established to help prevent terrorist attacks by serving as a hub for federal agencies to share information and analysis with state and local authorities and the private sector, and to receive information from those entities.[3] In other words, I&A sits at the center of a web of intelligence and law enforcement agencies spread throughout the country. Its intelligence products and the guidance it gives to its partners shape their perception of the threat environment we face and their response.

In light of the role that I&A plays, it is critically important that its output and advice meet the highest standards of respect for Americans' civil rights and civil liberties. This is especially true when it comes to the collection of domestic intelligence, which presents unique threats because of its obvious overlap with protected political speech and organizing.

As documented by the Church Committee, established by the U.S. Senate in 1975, unchecked surveillance authorities allowed the Federal Bureau of Investigation (FBI) to open over 500,000 files on Americans, including on the National Association for the Advancement of Colored People, the women's liberation movement, conservative Christian groups, and university and church groups opposed to the Vietnam War.[4] The Central Intelligence Agency investigated at least 200,000 individuals inside the United States opposed to the war. These two agencies intercepted hundreds of thousands of

letters, including from the Federation of American Scientists and American peace groups such as the American Friends Service Committee. The Internal Revenue Service opened intelligence files on more than 11,000 Americans on the basis of political rather than tax criteria.

Many of the reforms instituted to curb the systemic abuses discovered by the Church Committee were rolled back in the wake of the attacks of 9/11. For the last two decades, we have seen renewed collection of domestic intelligence untethered from suspicion of criminal activity. This poses several overlapping types of risks: abuse of authority in order to pursue social and political movements; suppression of speech and association; invasion of privacy; discriminatory targeting of minority communities; and politicization.

Unfortunately, there is evidence that I&A has—at time—used its mandate as a cover for collecting information about minority communities, protest movements, and journalists. While the examples outlined below reflect only some of I&A's activities, they are significant enough to require a serious discussion of whether internal controls and external oversight have been sufficient to ameliorate civil rights and civil liberties risks. As DHS in general—and I&A in particular—pivot to responding to domestic terrorism, there is an even more urgent need to develop more robust safeguards against these risks.[5]

I. I&A Authorities

The Homeland Security Act of 2002 gives DHS the responsibility for integrating law enforcement and intelligence information relating to "terrorist threats to the homeland," and I&A is authorized to access, receive, and analyze information "in support of the mission responsibilities of the Department and the functions of the National Counterterrorism Center."[6]

The Intelligence Oversight Guidelines ("guidelines") that govern I&A's collection, retention, and dissemination of information concerning U.S. persons define these missions broadly, breaking them down into national missions and departmental missions.[7] DHS's national missions include assisting the president and executive branch officials "in the development and conduct of foreign, defense, and economic policies or the protection of the United States national interests from foreign security threats."[8] Departmental missions include assisting DHS, other government agencies and authorities, and the private sector "in identifying protective and support measures regarding threats to homeland security."[9] Examples include the expected—for example, the threat of terrorism (both domestic and international), threats to critical infrastructure, and major disasters—but also the open-ended category of "[s]ignificant threats to the Nation's economic security, public health, or public safety."[10] Supporting DHS leadership and other parts of the Department "in the execution of their lawful missions" provides a final catch-all basis for intelligence activities.[11]

Generally, I&A personnel are only authorized to use "overt collection methods"[12] and to "collect information from publicly available sources."[13] The past decades have seen an explosion in the quantity and accessibility of publicly available information, and it is increasingly regarded as an important source of intelligence.[14] While this information is often easily available, it raises First Amendment and privacy concerns. In the words of the Supreme Court, cyberspace—and social media in particular—is the most important place for the exchange of views,[15] implicating core free speech concerns.[16]

I&A combines the information it collects with foreign intelligence from the Intelligence Community (IC), law enforcement information from federal, state, local, territorial and tribal sources, and private sector data about critical infrastructure and strategic resources, as well as information collected by DHS components as part of their operational activities.[17] For example, I&A has access to data submitted by airlines on people flying to, from, or through the U.S.,[18] Department of Motor Vehicle records, law enforcement and intelligence holdings, immigration records, and more.[19] I&A also shares federal terrorism-related information to and from state and local law enforcement, often via state, local, and regional law enforcement intelligence fusion centers.[20] Private entities are another source of information, such as LookingGlass Cyber Solutions, a firm that produced a report on protests against family separation that was widely distributed by I&A.[21]

Based on publicly available information, I&A can access this smorgasbord of information so long as it reasonably believes that it supports one of the broad national or departmental missions described above.[22] I&A's guidelines allow information to be "permanently retained" as long as its officials believe it remains relevant.[23] Material in I&A's repository can be shared easily with a range of federal, state, and local agencies as long as it would help the recipient carry out legally authorized public safety functions.[24] There is little accountability for what happens to this information. I&A can disseminate data that it collects on U.S. persons—without suspicion that they are engaged in criminal activity—but then has little control on how it is used or how long it is kept by the entity that receives it, or whether it might be misinterpreted without further context after it is shared. The office is required to establish internal procedures and audits to ensure compliance with the guidelines for the protection of U.S. person information, but the degree to which such measures have been implemented is not clear to the public.[25]

In sum, I&A has broad authorities, and its access to information reaches well beyond what it collects from public sources. Unfortunately, there is limited publicly available information on when and how I&A uses this information and how it concretely accounts for civil rights and civil liberties concerns. As described below, however, there is reason to be concerned about the impact of its activities on Americans' constitutionally protected rights.

II. Targeting Minority Communities and Protest Movements

As reflected in its guidelines, I&A is prohibited from collecting or disseminating information based solely on First Amendment protected activities, such as speech and assembly. It has not always respected this prohibition.

Muslim Americans have often been in its crosshairs for little apparent reason other than their religion. In 2007, for example, I&A undertook a study on the Nation of Islam, in which the office speculated about who would succeed Louis Farrakhan as the group's leader. The document was disseminated to hundreds of federal and local officials and members of Congress. It was quickly withdrawn, with a senior official conceding that "[t]he organization - despite its highly volatile and extreme rhetoric - has neither advocated violence nor engaged in violence."[26] The same year, I&A issued a report on refugees from Somalia. While the report itself is not publicly available, Senators Russ Feingold (D-WI) and John Rockefeller (R-WV) complained to the then head of I&A that it inappropriately sought information from a range of federal, state, and local agencies on "American organizations and American citizens, such as private attorneys, members of refugee organizations or even church groups" without any "indication of wrongdoing" by those groups.[27] And in May 2008, I&A issued yet another report about innocuous activities. Titled "TERRORISM WATCHLIST: Information Regarding a Flier Posted at a Mosque in Ohio Announcing an Upcoming Conference in Georgia," the report highlighted a flier announcing an upcoming conference and listing speakers.[28] While these documents were flagged by internal review procedures as potentially violating I&A guidelines, they demonstrate the Office's targeting of Muslim Americans for activity that is far removed from terrorism or violence.

In 2009, I&A published a report on "Rightwing Extremism,"[29] which was quickly quashed. In recent years, the suppression of the report has been cited as evidence of security agencies' refusal to take seriously the threat of far-right violence.[30] While the author of the report may have been prescient about a looming danger, the report itself ran afoul of the prohibition on intelligence based on First Amendment protected expressions of belief. It started by conceding that I&A had no specific information that "domestic rightwing terrorists were currently planning acts of violence," but warned that "rightwing extremists may be gaining new recruits by playing on their fears about several emergent issues," such as the economic recession, the impact of trade agreements on the availability of jobs, and the election of the first African American president.[31] It focused on the beliefs of people, such as anti-tax, anti-abortion and pro-gun activists, rather than on any suspected or actual criminal activity. It is a forgotten fact that the report was issued over the objections of DHS's Civil Rights and Civil Liberties (CRCL) office and was criticized by both Republicans and Democrats in Congress, as well as the ACLU, for targeting nonviolent actors.[32]

When I&A creates intelligence products about protest movements that involve some level of violence or criminal activity, it faces a delicate situation because its efforts

can easily slide into (or at least be perceived as) targeting political viewpoints. This has been the case over the previous year.

Last summer, as racial justice demonstrations triggered by the killing of George Floyd broke out across the country, I&A led the expansion of intelligence activities under the guise of protecting federal courthouses, apparently identifying protestors for agents to apprehend.[33] On June 26, 2020, President Trump issued an executive order which declared that "[i]t is the policy of the United States to prosecute to the fullest extent permitted under Federal law, and as appropriate, any person or any entity that destroys, damages, vandalizes, or desecrates a monument, memorial, or statue within the United States or otherwise vandalizes government property."[34] Among other things, the order directed DHS to provide "personnel to assist with the protection of Federal monuments, memorials, statues, or property."[35]

An undated "job aid" published by the legal blog Lawfare shows that DHS operationalized this order to expand "intelligence activities necessary to mitigate the significant threat to homeland security."[36] In addition to collecting information about threats that can reasonably be considered as relating to homeland security (e.g., threats to law enforcement personnel), analysts were directed to focus on "threats to damage or destroy any public monument, memorial, or statue."[37] The information that could be collected was defined expansively and included "information that … informs an overall assessment" of the threats to monuments.[38]

During this operation, DHS engaged in extensive and intrusive surveillance of protestors: the Washington Post obtained an internal DHS document showing that I&A had access to protesters' communications on the electronic (supposedly encrypted) messaging app Telegram, and that these conversations were written up in an "intelligence report" that was disseminated to federal, state, and local law enforcement agencies.[39] Under its governing statute and guidelines, I&A is not authorized to conduct electronic surveillance but must obtain the assistance of another federal agency (such as the FBI) in order to obtain private messages. It is not clear how the office obtained access to these messages.[40] While the messages have not been made public, according to the Washington Post, they did not "show the protesters planning to harass or target police or damage property," but instead were focused on "how to avoid encounters with police, particularly federal officers, who they knew had detained protesters."[41]

Journalists too were scrutinized by I&A during this time. The Office compiled and disseminated three intelligence reports summarizing tweets written by the editor in chief of Lawfare and a reporter for the New York Times, highlighting their publication of leaked, unclassified documents about DHS operations in Portland.[42]

Reacting to reports in the press, the Chair of the House Intelligence Committee, Rep. Adam Schiff (D-CA), wrote to the Acting Secretary of DHS, Chad Wolf, and the Acting Undersecretary of I&A, Brian Murphy, seeking information about the intelligence activities in response to protests.[43] If the reports were true, Schiff said, DHS was

distorting its authorities by treating "threats of graffiti, vandalism, or other minor damage to monuments, memorials, statutes [sic], and federal buildings … in the same fashion as it would seek to counter acknowledged threats to U.S. homeland security, such as terrorism, significant cyber intrusions, or attacks against federal facilities or personnel."

Rep. Schiff's characterization was shared by local officials, who generally opposed the Department's intervention.[44] While I&A's guidelines identify "[s]ignificant threats to the Nation's economic security, public health, or public safety" as a basis for intelligence operations, it is surely a reach for an entity set up to combat terrorism to turn its attention to the types of public safety matters that are typically handled by police forces and local officials.

Shortly afterwards, I&A withdrew the job aid. While asserting there was more than one legitimate view of its authority, it stated it was choosing to take a "narrower interpretation to better align with the threats of concern to I&A."[45]

In contrast to its aggressive posture in Portland and vis-a-vis racial justice protests in general,[46] I&A did not issue any specific warnings ahead of Congress's certification of electoral college votes or trigger any special intelligence effort. In testimony submitted to this committee for a hearing on March 3, 2021, I&A's Acting Under Secretary, Melissa Smislova, noted that the office had issuedOffice by pointing to its issuance "strategic warnings," both public and non-public, about election-related violence, but conceded that "concerning information was gathered and evaluated in the weeks prior to the attack on the U.S. Capitol" and "more should have been done to understand the correlation between that information and the threat of violence."[47]

The disparate treatment meted out by I&A in the two instances highlighted above—the racial justice protests in summer 2020 vs. the lead-up to the January 6 insurrection—naturally raises questions about bias and politicization of intelligence and shows the very real consequences that result. For I&A to be regarded as a reliable and neutral source of intelligence focused on the very real threats our country faces, guardrails must be established to prevent a recurrence.

III. Confronting the Domestic Terrorism Threat

It is particularly critical that I&A get its house in order as DHS pivots to confront the threat of domestic terrorism.[48] Recent actions by the Department underscore this shift in focus:

- On January 27, 2021, the Department's Acting Secretary issued an National Terrorism Advisory System (NTAS) Bulletin warning that "some ideologically-motivated violent extremists with objections to the exercise of governmental authority and the presidential transition, as well as other perceived grievances fueled by false narratives, could continue to mobilize to incite or commit violence."[49] The Bulletin identified specific issues motivating domestic violent

extremists, "including anger over COVID-19 restrictions, the 2020 election results, and police use of force." An updated version was issued on May 14, 2021.[50]

- In February, Secretary Mayorkas designated domestic violent extremism (DVE) a "National Priority Area," which requires state and local grant recipients to dedicate a portion of the funds received from DHS to combatting DVE.[51]

- On May 12, 2021, the Secretary informed the Senate Appropriations Committee that he had established a dedicated team within I&A to ensure the development of the "expertise necessary to combat this threat using sound, timely intelligence," and explained that DHS plans to leverage the fusion center network, increase information-sharing, and evaluate how online activities are linked to real-world violence.[52]

DVE (or domestic terrorism) is frequently equated with far-right violence, but the category actually covers a range of political violence. DHS, like the FBI, specifies five broad types of DVE threats:

- Racially motivated violent extremism (which melds together in one category white supremacists and Black separatists, among others);
- Anti-government or anti-authority violent extremists (which includes militias, sovereign citizens, and anarchists);
- Animal rights and environmental activists;
- Abortion-related extremists; and
- All other domestic terrorism threats.[53]

By listing this range of threats, DHS can claim that its response to DVE is ideology-neutral, an important framing given concerns about freedom of speech and association that arise in addressing political violence.

Regardless of whether the Department's programs, including the tasking of I&A, are neutral as *between* ideologies, they are clearly organized to focus on ideologies. The five threat categories, for example, are defined based on perceived similarities between ideologies while obscuring or entirely omitting the types of connections that would make sense from an operational point of view. For example, while both sovereign citizens and anarchists may be anti-government, they are hardly known for working together. On the other hand, some militias do have connections to white supremacist groups and a history of working together.[54] This framing elevates the role of what people think over their actions.

In March 2021, NBC News reported that DHS officials had indicated that the Department wants to identify online "narratives" that are likely to incite violence and flag people who may be susceptible to them based on their social media behavior.[55] John

Cohen, the Assistant Secretary for Counterterrorism and Threat Prevention, testified before Congress that the goal is to "identify emerging narratives as early as possible and assess whether those narratives are likely to influence acts of violence and how fast they're spreading across multiple platforms."[56] This was confirmed by Secretary Mayorkas, who said that the Department plans to "review how extremists exploit and leverage social media and other online platforms, and how online activities are linked to real-world violence."[57]

In operational terms, the focus on ideologies means that DHS—and particularly I&A—will be monitoring social media in search of threats. This is likely to be both ineffective and invasive, while sweeping in reams of information, including about constitutionally protected activities.

Outside of overt planning for violence of the type that was evident in the days leading up to the January 6 attack on the Capitol, targeting what people say online is unlikely to be an effective means of addressing the DVE threat.[58] The reason for this is simple: large numbers of people believe the types of narratives that DHS identified as drivers of violence in its January 27 NTAS Bulletin. Anti-immigrant sentiment has a long history in the U.S.; many people believe that the measures taken to control COVID-19 infringe on their freedoms; millions of Americans, including 65 percent of Republicans, dispute the results of the 2020 elections;[59] and police use of force against African Americans triggered demonstrations across the country last summer. These narratives can be found on social media platforms of all stripes, as well as on popular cable TV shows. They are hardly a way of distinguishing potentially violent actors from those who simply hold these views.

In fact, DHS's previous attempts to identify pre-terrorism indicators for international terrorism (i.e., violence connected to or inspired by groups like Al Qaeda and ISIS) show that such an endeavor is likely futile. The Department has given millions of dollars in funding to researchers to identify the precursors to extremist violence. While these researchers can make lists of factors that—when viewed retrospectively—seem to have contributed to an individual's decision to turn to violence, they uniformly caveat their work by noting that there are no indicators or hallmarks of someone who is about to become violent. As noted in a major DHS-commissioned study of terrorism prevention efforts conducted by the RAND Corporation: "Because there are no unambiguous early indicators of future violent behavior, the performance of risk assessment tools and methods to distinguish individuals who appear to be threats from those who actually do pose a threat is limited[.]"[60]

Moreover, there are severe limitations on the use of social media as a source for understanding the DVE threat. As the Acting Undersecretary of I&A recently acknowledged, "actual intent to carry out violence can be difficult to discern from the angry, hyperbolic – and constitutionally protected – speech and information commonly found on social media and other online platforms."[61] Social media poses multiple

challenges when it comes to accurately interpreting a speaker's intent, from the absence of "traditional context clues" that signal meaning to the different conventions that govern discourse on social media to variable uses of the technology depending upon the participant's age and background.[62] These barriers to interpretation are particularly acute when the reader lacks a shared context with the speaker.

DHS's previous attempts to use social media to identify threats amply demonstrate these limitations. In 2016, the Department piloted several programs that attempted to use social media to vet visa applicants. A February 2017 DHS Inspector General audit of these programs found that DHS had not measured their effectiveness, rendering them an inadequate basis on which to build broader initiatives.[63] USCIS evaluations of three out of the four programs used to vet refugees reported that information from social media "did not yield clear, articulable links to national security concerns," even when an applicant was flagged as a potential threat through other channels.[64] Officials pointed out that they were unable to reliably match social media accounts to the individual being vetted, and even where the correct accounts were found, it was hard to determine "with any level of certainty" the context and reliability of what they were reviewing.[65]

Another DHS effort to collect social media information also recently ran into trouble. In September 2019, the Department proposed a new rule authorizing it to collect social media identifiers from roughly 33 million people annually on its travel and immigration forms. In April, the White House's Office of Information and Regulatory Affairs (OIRA), the White House office that reviews federal regulations, rejected the proposal on the grounds that DHS had not "adequately demonstrated the practical utility of collecting this information."[66] OIRA told the Department that if it submitted a similar proposal in the future, it must demonstrate the utility of such collection and show that "such utility outweighs the costs - both monetary and social - of doing so."

IV. Recommendations

To address the concerns raised by the record outlined above, it is critical to strengthen I&A's civil rights and civil liberties safeguards and oversight over its functions.

First, the clearance authority of the oversight offices (CRCL, Privacy, the Office of the General Counsel, and I&A's Intelligence Oversight Section) should be restored and potentially written into law. Starting in 2009, DHS put in place an "interim clearance process" that ensured these offices reviewed all unclassified intelligence analysis before it was issued.[67] Disagreements were elevated to the Deputy Secretary for decision.[68] This process was formalized in 2013 and further elaborated in 2016.[69] But these internal rules were discarded in May 2020, with I&A's Undersecretary given "final decision authority for disseminating intelligence products."[70] In July, the oversight offices' influence was further diminished; I&A was given the authority to set time limits on their review and even publish intelligence products without review in "exigent circumstances."[71] DHS

leadership should (if it has not already) revive the role of the oversight offices and Congress should consider mechanisms for ensuring that these critical functions cannot be so easily side-lined.

Second, regular audits by an appropriate oversight office should be implemented. Under the current guidelines, I&A's Intelligence Oversight Officer is tasked with "periodic reviews" that include "unannounced reviews (i.e., 'spot checks'), reviews of audit logs, records reviews, and employee and contractor interviews."[72] If these reviews reveal any intelligence collection that is "unlawful or contrary to executive or presidential directive," the Associate General Counsel for Intelligence reports the conduct to the Intelligence Oversight Board (a standing component of the President's Intelligence Advisory Board) and the Office of the Director of National Intelligence.[73] Audits by an office like CRCL, however, would provide an opportunity for a holistic review of civil rights and civil liberties with the potential to identify program deficiencies or areas for improvement and training not evident during the more limited reviews currently required.

Third, in light of the fact that social media is a principal forum for political discussion and the limitations on identifying actual threats through this medium, I&A should reconsider its plans to monitor these platforms for "narratives" and "grievances." At a minimum, it should provide transparency about how it intends to cabin such monitoring to ensure that it is focused on identifying violent actors rather than simply keeping tabs on what Americans say on the Internet.

In addition, according to press reports, I&A currently uses human reviewers to review social media.[74] The office should clarify if this is the case or if it is using automated tools (either directly or via third-party vendors). While these tools are often hyped by the private companies that sell them, data scientists agree that algorithms that claim to be able to judge the meaning of text struggle to make even simple determinations, such as whether a social media post is positive, negative, or neutral.[75]

Finally, former Department officials have said that the privacy and due process concerns arising from DHS operations, including the retention of "huge amounts of data on individuals," dwarf those arising out of the National Security Agency's (NSA) more publicly scrutinized information collection.[76] The Privacy and Civil Liberties Oversight Board (PCLOB) should review I&A's access these data systems to assess the sufficiency of privacy and civil liberties safeguards.[77]

[1] Homeland Security Act of 2002, 6 U.S.C. § 101 (2002). I&A is also charged with providing input on the priorities of the intelligence community and with carrying out vulnerability assessments for key resources and critical infrastructure. HSA 6 U.S.C. § 121(d)(1)-(3).
[2] See Department of Homeland Security, "Resources for Fusion Centers," accessed May 14, 2021, https://www.dhs.gov/resources-fusion-centers.
[3] The number of fusion centers has grown dramatically in the years since 9/11, from nine in 2003 to eighty today. Jason Barnosky, "Fusion Centers: What's Working and What Isn't," Brookings Institution, March 17, 2015, https://www.brookings.edu/blog/fixgov/2015/03/17/fusion-centers-whats-working-and-what-isnt/. Despite the growth in numbers, the terrorism threat has not been large enough to occupy most fusion centers. Most have thus shifted to an "all hazards" approach, working to prevent ordinary crime and mitigate natural disasters. Blake Harris, "Fusion Centers May Strengthen Emergency Management," GovTech, June 9, 2009. In a 2012 survey of fusion center employees, only 28 percent said counterterrorism was their most important activity. Michael Price, *National Security and Local Police*, Brennan Center for Justice, 2013, 20 (citing Frank J. Cilluffo, Joseph R. Clark, Michael P. Downing and Keith D. Squires, *Counterterrorism Intelligence: Fusion Center Perspectives*, George Washington University Homeland Security Policy Institute, June 2012, 27, https://justiceacademy.org/iShare/Library-DHS/Fusion/HSPI%20Counterterrorism%20Intelligence%20-%20Fusion%20Center%20Perspectives%206-26-12.pdf).
[4] S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, *Intelligence Activities and the Rights of Americans,* S. Rep. No. 94-755 (1976).
[5] *Domestic Violent Extremism in America, Hearing Before the S. Comm. on Appropriations,* 117th Cong. (2021) (oral testimony of Alejandro N. Mayorkas, Secretary of Homeland Security).
[6] HSA 6 U.S.C. § 121(d)(1).
[7] As a member of the Intelligence Community, I&A is required to issue guidelines for its collection, retention, and dissemination of information about U.S. persons, which much be approved by the Attorney General in consultation with the Director of National Intelligence. Exec. Order No. 12333, 46 FR 59941 (December 4, 1981). U.S. persons are defined by federal law as any corporation, partnership, or other organization organized under the laws of the United States. 22 U.S. Code § 6010 (1992).
[8] I&A, *Intelligence Oversight Guidelines*, 1.1.1. The mission of the National Counterterrorism Center is to "lead and integrate the national counterterrorism (CT) effort by fusing foreign and domestic CT information, providing terrorism analysis, sharing information with partners across the CT enterprise, and driving whole-of-government action to secure our national CT objectives." National Counterterrorism Center, "Who We Are," accessed May 15, 2021, https://www.dni.gov/index.php/nctc-who-we-are/mission-vision.
[9] I&A, *Intelligence Oversight Guidelines*, 1.1.2.
[10] I&A, *Intelligence Oversight Guidelines*, 1.1.2.(c).
[11] I&A, *Intelligence Oversight Guidelines*, 1.1.2.
[12] I&A has defined overt collection broadly, to include, "[t]he acquisition of intelligence information from public media, observation, government-to-government dialogue, elicitation, and from the sharing of data openly acquired; the process may be classified or unclassified; the target and host governments as well as the sources involved normally are aware of the general collection activity, although the specific acquisition, sites, and processes may be successfully concealed." S. Homeland Security Comm., Subcomm. on Investigations, *Federal Support for and Involvement in Fusion Centers*, October 3, 2012, https://www.hsgac.senate.gov/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf; see also I&A, *Intelligence Oversight Guidelines*, Glossary.
[13] I&A, *Intelligence Oversight Guidelines*, 2.1.1. The guidelines also provide specific rules for counterintelligence activities involving the physical surveillance of I&A staff (current and former) and applicants, mail covers, and the use of monitoring devices. I&A, *Intelligence Oversight Guidelines*, 2.1.2.3.
[14] Congress has called for a study by the ODNI on the intelligence community's open source intelligence mission. Intelligence Authorization Act for Fiscal Year 2021, H.R.7856, 116th Cong. (2020); Consolidated Appropriations Act, 2021, Pub. L. 116-260, 134 Stat. 1182 (2020).
[15] Reno v. American Civil Liberties Union, 521 U. S. 844, 868 (1997).
[16] Packingham v. North Carolina, 137 S. Ct. 1730, 1731 (2017) (observing that social media users employ these websites to engage in a wide array of protected First Amendment activity on topics as diverse as human thought) (quotation marks and citation omitted).
[17] Department of Homeland Security, "Office of Intelligence and Analysis Enterprise Records System," 73 FR 28128 (June 16, 2008), https://www.federalregister.gov/documents/2008/05/15/E8-10888/privacy-act-office-of-intelligence-

and-analysis-enterprise-records-system; Congressional Research Service, *Selected Homeland Security Issues in the 116th Congress*, November 26, 2019, 3, https://fas.org/sgp/crs/homesec/R45701.pdf.

[18] U.S. Customs and Border Protection, *Passenger Name Record Privacy Policy*, September 13, 2019, https://www.cbp.gov/sites/default/files/assets/documents/2020-May/PNR-Privacy-Policy-%28508-Compliant%29.pdf. See CBP, *PNR Privacy Policy*, 3-4. Passenger Name Records contain everything from the payment a person used to buy their ticket, their contact information, travel itinerary, who they are traveling with, and more.

[19] See Department of Homeland Security, *Privacy Impact Assessment for the Automated Targeting System*, DHS/CBP/PIA-006(e), January 13, 2017, last updated May 5, 2021, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp006-ats-may2021.pdf; Department of Homeland Security, *Privacy Impact Assessment Update for the Analytical Framework for Intelligence (AFI)*, DHS/CBP/PIA-010(a), September 1, 2016, last updated August 2020, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-afi-august2020_0.pdf.

[20] Permanent Subcommittee on Investigations, "Investigative Report Criticizes Counterterrorism Reporting, Waste at State & Local Intelligence Fusion Centers," Senate Committee on Homeland Security and Government Affairs, October 3, 2012, http://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers; Faiza Patel and Michael Price, "Fusion Centers Need More Rules, Oversight," Brennan Center for Justice, October 18, 2012, https://www.brennancenter.org/our-work/research-reports/fusion-centers-need-more-rules-oversight. Fusion centers have been criticized for wasting security resources and for producing and disseminating inappropriate and unreliable intelligence reports about protest groups—often with little relationship to public safety. Permanent Subcommittee on Investigations, "Investigative Report Criticizes Counterterrorism Reporting." For example, the Maine Information and Analysis Center (MIAC) reportedly distributed reportedly intelligence on potential violence at anti-police-brutality protests based on far-right activists' social media posts. In May 2020, former state trooper George Loder filed an employment discrimination case against the center, claiming that he was demoted after he told his bosses that the center was collecting and maintaining data illegally, including information about people who had applied to buy guns from firearms dealers, those who legally protested, and those who worked at a Maine international camp for Israeli and Arab teens. See Mara Hvistendahl and Alleen Brown, "Law Enforcement Scoured Protester Communications and Exaggerated Threats to Minneapolis Cops, Leaked Documents Show," Intercept, June 26, 2020, https://theintercept.com/2020/06/26/blueleaks-minneapolis-police-protest-fears/; Nathan Bernard, "Maine Spy Agency Spread Far-Right Rumors of BLM Protest Violence," Mainer, July 7, 2020, https://mainernews.com/maine-spy-agency-spread-far-right-rumors-of-blm-protest-violence/; Judy Harrison, "Maine State Police Illegally Collecting Data on Residents, Lawsuit Claims," Bangor Daily News, May 14, 2020, https://bangordailynews.com/2020/05/14/news/state/state-agency-illegally-collecting-data-on-mainers-claims-trooper-in-whistleblower-suit/. Fusion centers are also a primary conduit for collecting and sharing "see something, say something" leads from the public that are packaged as "suspicious activity reports" (SARs) and disseminated through the ODNI's Intelligence Sharing Environment (ISE) and the FBI's eGuardian system. A survey of fusion center personnel criticized SARs as "white noise" that harmed intelligence analysis, and SARs obtained by the ACLU revealed bias driving much of the reporting. Julia Harumi Mass and Michael German, "The Government Is Spying on You: ACLU Releases New Evidence of Overly Broad Surveillance of Everyday Activities," American Civil Liberties Union, September 19, 2013, https://www.aclu.org/blog/national-security/privacy-and-surveillance/government-spying-you-aclu-releases-new-evidence.

[21] Ryan Devereaux, "Homeland Security Used a Private Intelligence Firm to Monitor Family Separation Protests," Intercept, April 29, 2019, https://theintercept.com/2019/04/29/family-separation-protests-surveillance/.

[22] I&A, *Intelligence Oversight Guidelines*, 2.1.3.1 (referencing 1.1, 2.2.3). I&A can only collect, retain, or disseminate information on U.S. persons if it fits within an information category defined in the guidelines. Moreover, I&A's use of shared databases must comply both with the guidelines and any more restrictive rules a given database's host may have. I&A, *Intelligence Oversight Guidelines*, 4.4; I&A, *Intelligence Oversight Guidelines*, Glossary-5 ("Shared Repository: A database, environment, or other repository maintained for the use of more than one entity. A database, environment, or other repository that a contractor or other entity maintains solely for the use of I&A, or those acting on its behalf, is not a shared repository."). There are also specific rules for "bulk data" likely to contain non-public U.S. person information, including the receipt of information that is responsive to demographic traits like a person's age or gender rather than "specific identifiers" like their name, date of birth or social security number. I&A, *Intelligence Oversight Guidelines*, 3; I&A, *Intelligence Oversight Guidelines*, Glossary-1 ("Bulk data transfer does not include the transfer of records responsive to specific identifiers (e.g., name, date of birth, social security number, etc.) but it does include the transfer of records identified through the application of search terms where the transfer would include a

significant number of records that, while responsive to the applied search terms, is not reasonably likely to have any ultimate intelligence or operational value to the recipient (e.g., records responsive to demographic profiles such as age, citizenship, or gender).”). Rules governing bulk data transfer, collection, retention, and dissemination generally incorporate additional safeguards—for example, the Under Secretary for Intelligence & Analysis must determine in writing that a bulk data collection is “the only practicable means of identifying or using the information in the collection that will support an authorized I&A mission[.]” I&A, *Intelligence Oversight Guidelines*, 3.1. One limit on I&A’s collection, retention, and dissemination of information gleaned from shared databases is that any rules governing a shared database that are more restrictive than I&A’s guidelines, such as restrictions on copying, storing or sharing information taken from the database, must be followed. I&A, *Intelligence Oversight Guidelines*, 4.4. However, some databases, like CBP’s Automated Targeting System, recognize the risk that shared intelligence will be stored longer than the ATS retention period (15 years). DHS, *ATS PIA*, 14.

[23] I&A, *Intelligence Oversight Guidelines*, 2.2.2.

[24] I&A, *Intelligence Oversight Guidelines*, 2.3.1; Department of Homeland Security, I&A “Enterprise Records System.” Under most circumstances, only data that qualifies for permanent retention may be disseminated, but even information that has not yet qualified for permanent retention may be disseminated to other elements of the IC. I&A, *Intelligence Oversight Guidelines*, 2.3.2.

[25] I&A, *Intelligence Oversight Guidelines*, 1.2.

[26] “Intelligence Oversight Inquiry into the Production and Dissemination of Office of Intelligence and Analysis Intelligence Note,” Memorandum from Charles E. Allen, Under Secretary for Intelligence and Analysis, to Gus Coldebella, DHS Acting General Counsel, March 28, 2008, https://www.eff.org/files/nationofislam.pdf; Richard B. Muhammad, Ashahed M. Muhammad and Askia Muhammad, “Nation of Islam Targeted by Homeland Security,” *Final Call News*, December 24, 2009, https://www.finalcall.com/artman/publish/National_News_2/article_6682.shtml.

[27] Russell D. Feingold and John D. Rockefeller IV, Letter from Senators Russell D. Feingold and John D. Rockefeller IV to Michael Chertoff, Secretary of Homeland Security, July 31, 2008, https://www.eff.org/files/filenode/intel_oversight/dhs_release_feb_1_2010.pdf

[28] Feingold and Rockefeller, Letter to Michael Chertoff.

[29] Department of Homeland Security Office of Intelligence and Analysis, *Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment*, April 7, 2009, https://fas.org/irp/eprint/rightwing.pdf.

[30] Spencer Ackerman, “DHS Crushed This Analyst for Warning about Far-Right Terror,” *Wired*, August 7, 2012, https://www.wired.com/2012/08/dhs/. Following the controversy surrounding the report, DHS also disbanded the small unit that studied “non-Islamic extremism.” Daryl Johnson, “I Warned of Right-Wing Violence in 2009. Republicans Objected. I Was Right,” *Washington Post*, August 21, 2017, https://www.washingtonpost.com/news/posteverything/wp/2017/08/21/i-warned-of-right-wing-violence-in-2009-it-caused-an-uproar-i-was-right/.

[31] DHS I&A, *Rightwing Extremism*, 2, 5.

[32] Tom Brune, “Homeland Security Admits Error with Extremism Report,” Newsday, April 17, 2009, https://www.newsday.com/long-island/politics/homeland-security-admits-error-with-extremism-report-1.1219261?firstfree=yes; Teddy Davis and Ferdous Al-Faruque, “Napolitano Facing Republican Calls for Her Ouster,” ABC News, April 23, 2009, https://abcnews.go.com/Politics/story?id=7412992&page=1; Brett Murphy, Will Carless, Marisa Kwiatkowski and Tricia L. Nadolny, “A 2009 Warning about Right-Wing Extremism Was Engulfed by Politics. There Are Signs It’s Happening Again,” USA Today, January 27, 2021, https://www.usatoday.com/story/news/investigations/2021/01/25/twelve-years-before-capitol-riot-warning-right-wing-extremism-buried/6658284002/; Michael German, “Soon, We'll All Be Radicals,” American Civil Liberties Union, April 16, 2009, https://www.aclu.org/blog/national-security/privacy-and-surveillance/soon-well-all-be-radicals?redirect=2009/04/16/soon-well-all-be-radicals.

[33] Steve Vladeck and Benjamin Wittes, “DHS Authorizes Domestic Surveillance to Protect Statues and Monuments,” Lawfare, July 20, 2020 https://www.lawfareblog.com/dhs-authorizes-domestic-surveillance-protect-statues-and-monuments.

[34] “Protecting American Monuments, Memorials, and Statues and Combating Recent Criminal Violence,” Exec. Order No. 13933, 85 FR 40081 (2020).

[35] EO 13933, Sec. 5.

[36] Vladeck and Wittes, “DHS Authorizes Domestic Surveillance.”

[37] Vladeck and Wittes, “DHS Authorizes Domestic Surveillance.”

[38] The memo makes clear that "[p]ersons merely engaging in non-violent protest activities near MMS [monument, memorial or statue], or making hyperbolic statements about MMS *likely* do not constitute a threat to MMS" (emphasis added). Vladeck and Wittes, "DHS Authorizes Domestic Surveillance." See also Shane Harris, "DHS Authorizes Personnel to Collect Information on Protesters It Says Threaten Monuments," *Washington Post,* July 20, 2020, https://www.washingtonpost.com/national-security/dhs-authorizes-personnel-to-collect-information-on-protesters-it-says-threaten-monuments/2020/07/20/6f58867c-cace-11ea-b0e3-d55bda07d66a_story.html.

[39] Shane Harris, "DHS Analyzed Protester Communications, Raising Questions about Previous Statements by Senior Department Official," *Washington Post*, July 31, 2020, https://www.washingtonpost.com/national-security/dhs-analyzed-protester-communications-raising-questions-about-previous-statements-by-senior-department-official/2020/07/31/313163c6-d359-11ea-9038-af089b63ac21_story.html; Zolan Kanno-Youngs, "Homeland Security Considered Snooping on Portland Protesters' Cellphones," *New York Times*, October 2, 2020, https://www.nytimes.com/2020/10/02/us/politics/homeland-security-portland-protesters.html.

[40] If they obtained them by infiltrating the protest group rather than through electronic surveillance, that would still appear to violate the guidelines governing actions taken by I&A agents on behalf of the office; it is not clear whether the use of informants would run afoul of the office's guidelines. See I&A, *Intelligence Oversight Guidelines*, 4.1, Participation in Organizations Within the United States (setting out the parameters for participation in U.S. organizations). It has also been reported that an elite FBI counterterrorism team was flown to Portland to "exploit" the phones of people who had been arrested, with the arrestees' (supposed) consent. Mattathias Schwartz, "The FBI Team Sent to 'Exploit' Protesters' Phones in Portland," *New York Review of Books*, October 8, 2020, https://www.nybooks.com/daily/2020/10/08/the-fbi-team-sent-to-exploit-protesters-phones-in-portland/.

[41] Harris, "DHS Analyzed Protester Communications."

[42] Shane Harris, "DHS Compiled 'Intelligence Reports' on Journalists Who Published Leaked Documents," *Washington Post*, July 30, 2020, https://www.washingtonpost.com/national-security/dhs-compiled-intelligence-reports-on-journalists-who-published-leaked-documents/2020/07/30/5be5ec9e-d25b-11ea-9038-af089b63ac21_story.html. The Department of Homeland Security acknowledged that this was inappropriate and said it would "discontinue" collecting information on members of the press.

[43] Adam B. Schiff, Letter from Rep. Adam B. Schiff to Chad F. Wolf, Acting Secretary of Homeland Security, and Brian Murphy, Acting Under Secretary for Intelligence and Analysis, July 22, 2020, https://intelligence.house.gov/uploadedfiles/20200722hpsci_chm_letter_to_dhs.pdf. Wolf acknowledged that the collection of intelligence about journalists' tweet was unwarranted and demoted the Acting Head of I&A, Brian Murphy. Shane Harris, "DHS Compiled 'Intelligence Reports'"; Zolan Kanno-Youngs and Adam Goldman, "Homeland Security Reassigns Official Whose Office Compiled Intelligence on Journalists," *New York Times*, August 1, 2020, https://www.nytimes.com/2020/08/01/us/politics/brian-murphy-homeland-security-protesters.html. Murphy in turn filed a whistleblower complaint, claiming that the office was not allowed to report on white supremacist threats and was told to emphasize "the prominence of violent 'left-wing' groups." Brian Murphy, Whistleblower Reprisal Complaint, Department of Homeland Security, September 8, 2020, https://int.nyt.com/data/documenttools/homeland-security-whistleblower/0819ec9ee29306a5/full.pdf.

[44] Sergio Olmos, Mike Baker and Zolan Kanno-Youngs, "Federal Agents Unleash Militarized Crackdown on Portland," *New York Times*, September 1, 2020, https://www.nytimes.com/2020/07/17/us/portland-protests.html.

[45] Benjamin Wittes (@benjaminwittes), image of DHS memo attached to Tweet: "DHS I&A rescinds "job aid" about which @steve_vladeck and I wrote on @lawfareblog a few weeks back. Here is the memo:" Twitter, August 19, 2020, 10:56 a.m., https://twitter.com/benjaminwittes/status/1296144054770642947. This prompted a response from Schiff that expressed disappointment with I&A's position and its "inability to fully repudiate such overreach," and promised to explore legislative options to clarify I&A's authorities and mission and institute necessary guardrails. Adam B. Schiff, Letter from Rep. Adam B. Schiff to Joseph B. Maher, Principal Deputy General Counsel and Senior Official Performing the Duties of the Under Secretary for Intelligence and Analysis, August 19, 2020, https://intelligence.house.gov/uploadedfiles/20200819hpscichmfollowuplettertodhsia.pdf.

[46] Yael Halon, "DOJ 'Targeting and Investigating' Leaders, Funders of Far-Left Groups and Rioters, Wolf Tells Tucker," Fox News, August 31, 2020, https://www.foxnews.com/politics/chad-wolf-doj-investigating-far-left-rioters (citing interview in which Wolf says, "'This [arresting and charging leaders of "antifa" and the Black Lives Matter movement] is something that I have talked to the AG personally about[.]'").

[47] *Examining the January 6 Attack on the U.S. Capitol, Hearing Before the S. Comm. on Homeland Sec. and Gov't Affairs and S. Comm. on Rules and Admin*, 117th Cong. (2021) (testimony of Melissa Smislova, Acting Under Secretary for the Office of Intelligence and Analysis).

[48] The U.S. uses separate frameworks for international and domestic terrorism, and in the two decades since the 9/11 attacks has focused much of its intelligence gathering and law enforcement prowess on the former. Terrorism is categorized as international if the perpetrator has a connection – operational or ideological – with a foreign terrorist group. It is treated as domestic if the perpetrator's operational or ideological affiliation is with a U.S.-based group. Over the last few years, U.S. security agencies have been paying increasing attention to far-right violence as high-profile attacks, which often target minority communities, have ramped up. *Oversight of the Federal Bureau of Investigation: The January 6 Insurrection, Domestic Terrorism, and Other Threats, Hearing Before the S. Judiciary Comm.*, 117th Cong. (2021) (statement of Christopher Wray, Director of the Federal Bureau of Investigation) ("As has been stated multiple times in the past, preventing terrorist attacks, in all forms, remains the FBI's top priority… The top threat we face from DVEs continues to be those we identify as racially or ethnically motivated violent extremists (RMVEs), specifically those who advocate for the superiority of the white race, and who were the primary source of ideologically motivated lethal incidents of violence in 2018 and 2019."); Department of Homeland Security, *Homeland Threat Assessment*, October 2020, 18, https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf ("2019 was the most lethal year for domestic violent extremism in the United States since the Oklahoma City bombing in 1995…Among DVE actors, WSEs conducted half of all lethal attacks (8 of 16), resulting in the majority of deaths (39 of 48)."). The 1/6 attack on the Capitol, which was marked by the significant presence of groups such as the Proud Boys, as well as individuals bearing or wearing white supremacist insignia, catapulted this threat to the top of the Biden administration's agenda. Washington Post Staff, "Identifying Far-Right Symbols That Appeared at the U.S. Capitol Riot," *Washington Post*, January 15, 2021, https://www.washingtonpost.com/nation/interactive/2021/far-right-symbols-capitol-riot/; Zolan Kanno-Youngs and Nicole Hong, "Biden Steps up Federal Efforts to Combat Domestic Extremism," *New York Times*, April 4, 2021, https://www.nytimes.com/2021/04/04/us/politics/domestic-terrorism-biden.html.

[49] Department of Homeland Security, "National Terrorism Advisory System Bulletin."

[50] Department of Homeland Security, update of the "National Terrorism Advisory System Bulletin," May 14, 2021, https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-may-14-2021.

[51] Department of Homeland Security, "DHS Announces Funding Opportunity for $1.87 Billion in Preparedness Grants," February 25, 2021, https://www.dhs.gov/news/2021/02/25/dhs-announces-funding-opportunity-187-billion-preparedness-grants.

[52] Mayorkas, *Domestic Violent Extremism in America.*

[53] FBI and DHS, *Intelligence Assessment on Domestic Terrorism,* 5.

[54] *The Rise of Domestic Terrorism in America, Hearing Before the H. Comm. on the Judiciary, Subcomm. on Crime, Terrorism, and Homeland Sec.*, 117th Cong. (2021) (testimony of Michael German, fellow at the Brennan Center for Justice) https://docs.house.gov/meetings/JU/JU08/20210224/111227/HHRG-117-JU08-Wstate-GermanM-20210224.pdf.

[55] Ken Dilanian, "DHS Launches Warning System to Find Domestic Terrorism Threats on Public Social Media," NBC News, March 10, 2021, https://www.nbcnews.com/politics/national-security/dhs-launches-warning-system-find-domestic-terrorism-threats-public-social-n1266707.

[56] *Racially and Ethnically Motivated Violent Extremism: The Transnational Threat, Hearing Before the H. Comm. on Homeland Sec. Subcomm. on Intelligence and Counterterrorism*, 117th Cong. (2021) (oral testimony of Cohen, Assistant Secretary of Homeland Security for Counterterrorism and Threat Prevention).

[57] Mayorkas, *Domestic Violent Extremism in America.*

[58] Devlin Barrett and Matt Zapotosky, "FBI Report Warned of 'War' at Capitol, Contradicting Claims There Was No Indication of Looming Violence," *Washington Post*, January 12, 2021, https://www.washingtonpost.com/national-security/capitol-riot-fbi-intelligence/2021/01/12/30d12748-546b-11eb-a817-e5e7f8a406d6_story.html; Carol D. Leonnig, "Capitol Police Intelligence Report Warned Three Days before Attack That 'Congress Itself' Could Be Targeted," *Washington Post*, January 15, 2021, https://www.washingtonpost.com/politics/capitol-police-intelligence-warning/2021/01/15/c8b50744-5742-11eb-a08b-f1381ef3d207_story.html; Dina Temple-Raston, "Why Didn't the FBI and DHS Produce a Threat Report Ahead of the Capitol Insurrection?," NPR, January 13, 2021, https://www.npr.org/2021/01/13/956359496/why-didnt-the-fbi-and-dhs-produce-a-threat-report-ahead-of-the-capitol-insurrect.

[59] Carrie Dan, "Meet the Press Blog: Latest News, Analysis and Data Driving the Political Discussion," NBC News, May 13, 2021, https://www.nbcnews.com/politics/meet-the-press/blog/meet-press-blog-latest-news-analysis-data-driving-political-discussion-n988541/ncrd1261306#blogHeader ("The survey, conducted February 25 – March 1, found that 65 percent of Republicans believe that Biden's win was solely the result of voter fraud.").

[60] Brian A. Jackson, Ashley L. Rhoades, Jordan R. Reimer, Natasha Lander, Katherine Costello and Sina Beaghley, *Practical Terrorism Prevention: Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence*, RAND Corporation, 2019, https://www.rand.org/pubs/research_reports/RR2647.html.
[61] Smislova, *Examining the January 6 Attack*, 3.
[62] Lyrissa Barnett Lidsky and Linda Riedemann Norbut, "#I[redacted]U: Considering the Context of Online Threats," *California Law Review* 106 (2018): 1891.
[63] Department of Homeland Security Office of Inspector General, *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success (Redacted),* February 27, 2017, https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf.
[64] U.S. Citizenship and Immigration Services, "Social Media," in *U.S. Citizenship and Immigration Services Briefing Book*, 181, https://www.dhs.gov/sites/default/files/publications/USCIS%20Presidential%20Transition%20Records.pdf.
[65] USCIS, *Briefing Book*, 183.
[66] Office of Information and Regulatory Affairs, "Generic Clearance for the Collection of Social Media Information on Immigration and Foreign Travel Forms," No. 202007-1601-001, April 2, 2021, https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202007-1601-001; Harsha Panduranga, "White House Office Rejects DHS Proposal to Collect Social Media Data on Travel and Immigration Forms," Brennan Center for Justice, April 27, 2021, https://www.brennancenter.org/our-work/analysis-opinion/white-house-office-rejects-dhs-proposal-collect-social-media-data-travel.
[67] *Fiscal Year 2010 Budget for the Office of Intelligence and Analysis of the Department of Homeland Security, Hearing Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Sec.*, 111th Cong. (2009) (testimony of Bart R. Johnson, Acting Under Secretary for the Office of Intelligence and Analysis) ("To strengthen our existing processes, an interim clearance process was put in place shortly after the release of the April 7, 2009 assessment. That process established mandatory review and concurrence by four offices - Civil Rights and Civil Liberties, the Privacy Office, Office of the General Counsel, and I&A's Intelligence Oversight Section. Any non-concurrence that could not be resolved was elevated to the Deputy Secretary for review, ensuring a much more coordinated review of I&A's products than had previously been in place.").
[68] Bart Johnson testimony, *Fiscal Year 2010 Budget for the Office of Intelligence and Analysis.*
[69] Tia Sewell and Benjamin Wittes, "The Evolution of DHS Intelligence Review Policy," Lawfare, August 14, 2020, https://www.lawfareblog.com/evolution-dhs-intelligence-review-policy.
[70] Benjamin Wittes, "How the DHS Intelligence Unit Sidelined the Watchdogs," Lawfare, August 6, 2020, https://www.lawfareblog.com/how-dhs-intelligence-unit-sidelined-watchdogs.
[71] Wittes, "DHS Intelligence Unit Sidelined the Watchdogs."
[72] I&A, *Intelligence Oversight Guidelines*, Appendix A.
[73] I&A, *Intelligence Oversight Guidelines*, Appendix A. Previously, under Executive Order 12863, Inspectors General and General Counsel of IC member agencies, including I&A, were required to report to the Intelligence Oversight Board on a quarterly basis any "concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive." President's Foreign Intelligence Advisory Board, Exec. Order 12863 (September 13, 1993). The Board also had the authority to "review the practices and procedures of the Inspectors General and General Counsel" for identifying and investigating potential violations. Congress should give thought to whether these authorities should be restored.
[74] Ken Dilanian, "DHS Launches Warning System to Find Domestic Terrorism Threats," ("So far, DHS is using human beings, not computer algorithms, to make sense of the data, the officials said").
[75] Coalition Letter to DHS Opposing the Extreme Vetting Initiative, letter from civil society organizations to Elaine C. Duke, Acting Secretary of Homeland Security, November 16, 2017, 2n12-13, https://www.brennancenter.org/sites/default/files/Coalition%20Letter%20to%20DHS%20Opposing%20the%20Extreme%20Vetting%20Initiative%20-%2011.15.17.pdf (referencing Ahmed Abbasi, Ammar Hassan and Milan Dhar, "Benchmarking Twitter Sentiment Analysis Tools," Proceedings of the Ninth International Conference on Language Resources and Evaluation, Reykjavik, Iceland, May 2014; Julia Hirschberg & Christopher D. Manning, "Advances in Natural Language Processing," *Science* 349 (2015): 6245; Su Lin Blodgett & Brendan O'Connor, "Racial Disparity in Natural Language Processing: A Case Study of Social Media African-American English," Proceedings of the 2017 Fairness, Accountability, and Transparency in Machine Learning Conference, Halifax, Canada, 2017 (showing failure to perform on English text as used by a specific demographic community)).
[76] Chappell Lawson and Alan Bersin, "The Future of Homeland Security," in *Beyond 9/11: Homeland Security for the Twenty-First Century*, ed. Chappell Lawson, Alan Bersin and Juliette N. Kayyem (Cambridge, Mass: MIT Press, 2020), 303.

[77] The PCLOB is a bipartisan body which was established by the 9/11 Commission Act of 2007 to ensure that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties. Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53, 121 Stat. 266 (2007). It has reviewed some of the most sensitive intelligence programs of the U.S. government, providing much-needed transparency about their scope.

Post-Hearing Questions for the Record
Submitted to Mike Sena
From Senator Josh Hawley

"Examining the Role of the Department of Homeland Security's Office of Intelligence and Analysis"
May 18, 2021

1. You write in your testimony that you believe that assigning more personnel from the Office of Intelligence & Analysis to fusion centers is critically important. Can you elaborate on why this is the case?

The Office of Intelligence & Analysis (I&A) is the only Intelligence Community (IC) element statutorily charged with providing intelligence to State, local, tribal and territorial (SLTT) and private sector partners and developing intelligence from those partners for the Department and the IC. Without DHS I&A intelligence officers, analysts, and collection managers in fusion centers, we lack that connectivity to the IC. DHS I&A is statutorily directed to be the executive agent for the coordination of DHS and Federal engagement and support to fusion centers, if they are not in a fusion center, we have reduced connectivity to DHS and its component agencies.

I&A is supposed to lead intelligence sharing with their partners through constant and direct engagement in the field, strategic information sharing forums, and robust analytic production tailored to SLTT needs, and technology platforms to enhance collaboration. If the I&A personnel are not at the fusion center, they do not have direct engagement or the ability to tailor analytic products for SLTT needs.

Deployed I&A personnel are responsible for the day to day and emergency functions of:

- Supporting a fusion center's ability to conduct intelligence collection and analysis within their local environment.
- Building the fusion centers and SLLT partners' intelligence sharing capacity.
- Supporting the fusion center's response to emergent incidents.
- Enabling partners to consider national intelligence implications for their jurisdiction and provide local context.

The DHS I&A personnel also have access to DHS systems with data that are critical to fusion centers. Without the personnel on-site, the fusion centers lack access to the critical information that they need to identify terrorism suspects and suspects engaged in other criminal activity,

2. Has I&A traditionally been receptive to feedback from fusion centers when it comes to deploying I&A resources to fusion centers and allocating I&A personnel?

   The National Network of Fusion Centers has struggled with DHS I&A to have their personnel deployed to fusion centers. DHS I&A had experienced a personnel cap that limited their deployment of personnel while the number of fusion centers was expanding. This has meant that some fusion centers have been without any DHS I&A personnel for years and very few that have a full cadre of needed personnel that may include intelligence officers, regional intelligence analysts, reports officers, and collection operations managers. We have regular conversations with DHS I&A on the need for the deployment of personnel, but their ability to recruit, train, and deploy personnel has been painfully slow. They have been receptive to our feedback, but they have not been as responsive as we would like them to be.

3. You also note that I&A should enhance training opportunities for analysts in fusion centers. What kind of training, if any, is currently taking place? And why do you feel more training is necessary?

   Fusion centers currently lack advanced analytical training and specialized training in topics such as cyber risk analysis. Without advanced training we will not be able to develop the cadre of analysts that we need to protect the nation. The Attorney General's Federal Advisory Committee on the topics of justice information sharing and criminal intelligence, GLOBAL and CICC, produced the Analyst Professional Development Roadmap that identifies the intermediate and advanced-level training.

   "Training for an intermediate-level analyst should focus on increasing the understanding and applicability of the analytic process. Training for an advanced-level analyst should focus on refining the analyst's ability to fully implement the analytic process, as well as attendance at instructor techniques training and, at a minimum, project management training. Analysts also should participate in specialized training focused on the law enforcement and homeland security areas of emphasis.

   Training standards for the intermediate and advanced levels are identified in the Minimum Standards for Intermediate Level Analytic Training Courses and Minimum Standards for Advanced-Level Analytic Training Courses." (Please see Appendix B, starting on page 18, and Appendix C, starting on page 25, of the Analyst Professional Development Roadmap for more details.

   The courses below are the FEMA approved courses and the underlined courses are provided through DHS.

   - DHS Basic Intelligence and Threat Analysis Course (BITAC) (DHS-008-PREV)
   - DHS Critical Thinking and Analytic Methods (CTAM) (AWR-231)
   - DHS Introduction to Risk Analysis Course
   - DHS Intermediate Risk Analysis Course

- DHS Principles of Intelligence Writing and Briefing (PIWB) (PER-301)
- Foundations in Intelligence Analysis Training (FIAT) (WV-001-PREV)
- Fundamentals of Suspicious Activity Reporting Analysis (DHS-034-PREV)
- Intelligence Analyst Professional Development Program (IAPDP) – Texas (DHS-032-PREV)
- Intermediate Fusion Center Analyst Training: Analysis and Terrorism Prevention (CA-026-PREV)
- Intermediate Fusion Center Analyst Training: Strategic Analysis and Oral Briefings (CA-025-PREV)
- Law Enforcement Analyst Program (FL-002-PREV)
- ODNI Analysis 101 (DHS-007-PREV)
- Suspicious Activity Reporting: The Analytic Role (DHS-035-PREV)
- Terrorism Intelligence Analysis (CA-018-PREV)

4. On this committee, we've heard from various stakeholders who have been the victims of cyber-attacks, including private-sector companies, schools, and hospitals. How are fusion centers positioned to address these growing cyber threats, especially those that impact local governments or organizations?

   Fusion centers with trained cyber personnel are in the best position to assist private-sector companies, schools, hospitals, and local government organizations with threat prevention, mitigation strategies, and response to cyber-attacks and cyber threats. As the focal points for outreach, training, reporting of major incidents, and response coordination our nation's fusion centers are in the best position to support their local communities through our Cyber Intelligence Network (CIN). The CIN's mission is to support the free and rapid exchange of cyber intelligence. The CIN was developed by the National Fusion Center Association (NFCA) to create a virtual community of over seven hundred (700+) cyber analysts and cyber investigators across the country dedicated to responding to cyber incidents, sharing cyber intelligence, and producing relevant, actionable, and timely analytic products on cyber threats. The CIN operates the Cyber Situational Awareness Room through the Homeland Security Information Networks' Adobe Connect platform that connects all its members and allows them to share near real-time threat information 24/7.

   Through the CIN, cyber analysts:

   - Share information rapidly,
   - Coordinate and prevent the duplication of efforts, and
   - Connect with each other, so analysts know who their counterparts are nationwide and can rely on them when needed.

   The CIN has also developed the Cyber Liaison Officer (CLO) training course that was designed to improve law enforcement officers' ability to identify the elements of a cyber crime and report that information to their fusion center.

Fusion center personnel are also leveraging their involvement as members of the FBI's Cyber Task Forces to support the cyber investigations, assist with law enforcement/DHS deconfliction, and provide the mitigation support that is outside the scope of the FBI's responsibilities.

Post-Hearing Questions for the Record
Submitted to Faiza Patel
From Senator Josh Hawley

"Examining the Role of the Department of Homeland Security's Office of Intelligence and Analysis"
May 18, 2021

1. You write in your own testimony how "overt collection methods" generally used by the Office of Intelligence & Analysis still raise First Amendment and privacy concerns, despite the fact that these data collection methods might seem innocuous. Can you explain why that is the case?

   Answer:

   The "overt collection methods" that I&A is authorized to use can encompass a range of activities, from agents gathering information at public gatherings to accessing information on the Internet. The latter includes, of course, social media, which is a principal forum for exchanging ideas and political organizing.

   As the investigations guide of the Federal Bureau of Investigation recognizes, "[o]nline information, even if publicly available, may still be protected by the First Amendment."[1] When a government agency collects social media information, it has the ability to create detailed dossiers of Americans' views, including political matters that lie at the heart of First Amendment protections, as well as their social networks and even where they are located and the places they go. Social media can reveal the most intimate aspects of our lives: whether a person is gay or straight, whether she is a gun owner or a supporter of Planned Parenthood, or whether she goes to the mosque on Fridays or to church on Sundays.

   While we do not yet know the full scope of I&A's efforts, it is worth noting that the risks increase when vast swaths of information are swept up, combined with other sources of information, and subjected to algorithmic analysis.

[1] FED. BUREAU OF INVESTIGATIONS, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE, https://www.brennancenter.org/sites/default/files/2021-06/FOIA%20doc%201.pdf (last visited Jul. 1, 2021) (obtained via FOIA); *see also* L.A. POLICE DEP'T, SOCIAL MEDIA USER GUIDE 4 (2015), https://ia801000.us.archive.org/15/items/LosAngelesPoliceDepartmentSocialMediaPolicies/2015_03_12_lapd_chief_charlie_beck_lapd_social_media_guide_OCOP_Notice_03-12-2015.pdf ("Social media sites are a platform for people to express themselves, including political and religious beliefs, or views on government. The Department expressly recognizes the right of public expression. Employees should not interfere with the public's right to free speech, with the exception of those categories of speech that are not constitutionally protected (i.e., bomb threats)." (citation omitted)).

2. On May 10th it was reported that DHS was implementing a new strategy to analyze intelligence from public social media posts to build a type of warning system to detect violent events based on "narratives" they see online. These plans were confirmed by various DHS officials, including Secretary Mayorkas, over the past several months. What is your view of this government monitoring of social media?

   Answer:

   Social media is a tempting trove of information for security agencies, which have been engaged in efforts to mine it for years. At times, social media can reveal planning for criminal activity, as was the case leading up to the January 6th attack on the Capitol.[2] But monitoring social media for "narratives" casts an extremely broad net that will undoubtedly capture reams of political speech that is unrelated to planned violence.

   The individuals and groups who attacked the Capitol may share certain "narratives" – for example, with regard to the 2020 election. Regardless of what one may think of these narratives, they are commonly shared by millions of Americans and cannot by themselves serve as a basis for identifying potentially violent actors. DHS officials have repeatedly stated that they intend to focus on violence, not ideology, but they have conceded that it is difficult to parse out violent actors from those who are simply venting online, and the Department has yet to explain how it intends to make these critical distinctions.

   Notably, earlier DHS pilot programs for monitoring social media were unsuccessful in identifying threats to national security—even where they were checking on known individuals rather than trying to extrapolate the possibility of violence from online chatter.

   In 2016, DHS piloted several social media monitoring programs, one run by Immigration and Customs Enforcement (ICE) and five by United States Citizenship and Immigration Services (USCIS). A February 2017 DHS inspector general audit of these pilot programs found that the department had not measured their effectiveness, rendering them an inadequate basis on which to build broader initiatives.[3]

   Even more damning are USCIS's own evaluations of its social media monitoring programs, which showed them to be largely ineffective. According to a brief prepared by DHS for the incoming administration at the end of 2016, for three out of the four programs used to vet refugees, "the information in the accounts did not yield clear, articulable links to national

[2] *See, e.g.*, Sheera Frankel, *The Storming of Capitol Hill Was Organized on Social Media*, N.Y. TIMES (Jan. 6, 2021), https://www.nytimes.com/2021/01/06/us/politics/protesters-storm-capitol-hill-building.html; Cammy Pedroja, *Parler Warned FBI More than 50 Times Before Capital Riot, Rep. Carolyn Mahoney Says*, NEWSWEEK (Jun. 15, 2021), https://www.newsweek.com/rep-carolyn-maloney-says-parler-sent-warnings-over-50-times-ahead-capitol-riots-1601034.

[3] *See* OFFICE OF INSPECTOR GENERAL, U.S. DEP'T OF HOMELAND SEC'Y, DHS' PILOTS FOR SOCIAL MEDIA SCREENING NEED INCREASED RIGOR TO ENSURE SCALABILITY AND LONG-TERM SUCCESS TIMES 2 (2017), https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf.

security concerns, even for those applicants who were found to pose a potential national security threat based on other security screening results."[4] Out of the 12,000 refugee applicants and 1,500 immigration benefit applicants screened, USCIS found social media information helpful only in "a small number of cases," and even in those the data "had limited impact on the processing of those cases—specifically in developing additional lines of inquiry."[5]

The key takeaway from the pilot programs was that it was hard to determine "with any level of certainty" the "authenticity, veracity, [or] social context" of the data, as well as whether there were "indicators of fraud, public safety, or national security concern."[6]

Most recently, the White House Office of Information and Regulatory Affairs (OIRA) rejected a DHS proposal to collect social media identifiers from a range of travelers seeking to come to the United States because the agency had not "adequately demonstrated the practical utility of collecting this information."[7] OIRA instructed DHS that if it submitted a similar proposal in the future, "it must demonstrate the practical utility of collecting it and demonstrate that such utility outweighs the costs - both monetary and social - of doing so."

3. Generally speaking, do you believe this type of warning system risks chilling free speech or other First Amendment-protected activities?

   Answer:

   Yes. There is ample empirical evidence that the possibility of government monitoring reduces people's willingness to freely express themselves online.[8]

---

[4] U.S. CITIZENSHIP & IMMIGRATION SERV., BRIEFING BOOK 181 (2016), https://www.dhs.gov/sites/default/files/publications/USCIS%20Presidential%20Transition%20Records.pdf.

[5] *Id* at 183.

[6] *Id.*

[7] Office of Information and Regulatory Affairs, *View Generic ICR*—OIRA Conclusion, REGINFO.GOV, https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202007-1601-001 (last visited Jul. 1, 2021).

[8] *See, e.g.*, FDR GROUP & PEN AM. CTR, CHILLING EFFECTS: NSA SURVEILLANCE DRIVES US WRITERS TO SELF-CENSOR 6 (2013), https://pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling%20Effects%20w%20Color%20cover-UPDATED.pdf [https://perma.cc/5TFK-Q8MF] (finding that 28% of surveyed writers had curtailed social media activities because of government surveillance); Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH L.J. 117, 147–48 (2016) (finding an immediate 30% decrease in security-sensitive Wikipedia searches by U.S. Internet users following the revelations by Edward Snowden of extensive government surveillance); Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNALISM & MASS COMM. Q. 1, 8–10 (2016) (finding that survey participants were less likely to voice minority opinions online after being primed about government surveillance, though not less likely to voice majority opinions); Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* 4–5 (Feb. 17, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564 (finding a 4% decrease in Google searches for terms that users perceived might get them into trouble following the Snowden revelations, with larger decreases in English-speaking countries traditionally considered U.S. allies and less accustomed to surveillance than in

4. What does I&A need to do to remove concerns that they are too focused on keeping tabs on what Americans are saying online rather than identifying criminals?

   Answer:

   The following steps are recommended as ways to mitigate concerns about the use of social media monitoring.

   a. Policy Publication. I&A should publish a policy that sets out the rules it will follow for monitoring social media.[9] The policy should be developed in consultation with, and approved by, DHS's Civil Rights and Civil Liberties (CRCL) Officer and its Privacy Officer and should cover, at a minimum:

   - Purpose of monitoring: The policy should set out the purposes for which I&A plans to monitor social media and what steps it will take to ensure that its collection and use of social media is narrowly tailored to these purposes. I&A should maintain for a minimum of three years records documenting the purpose of each social media search, including searches of individuals and groups, as well as key words and any automated alerts, and the identity of the official responsible for each search.
   - Vendor contracts: The CRCL and Privacy Officers should review any arrangement between I&A and vendors of social media monitoring tools. All contracts with outside vendors should be made public.
   - Record retention and segregation: Any results of social media monitoring should be kept in a separate database and not integrated into DHS's systems unless related to criminal activity. Social media monitoring results should only remain in this stand-alone repository for the minimum period necessary.

---

countries conventionally treated as intelligence targets); Jonathon W. Penney, *Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study*, 6 INTERNET POL'Y REV. 1, 12 (2017) (finding that 60% of survey participants were less likely to share personally created material online due to government surveillance, whereas only 34% were less likely to share content due to an anti-cyberbullying statute); Elizabeth Stoycheff et al, *Privacy and the Panopticon: Online Mass Surveillance's Deterrence and Chilling Effects*, 21 NEW MEDIA & SOC'Y 602, 608–11 (2019) (finding that study participants who read an Associates Press article about government surveillance of online activities became less likely to be politically active online); Mark Rosso, A.B.M. Nasir & Mohsen Farhardloo, *Chilling Effects and the Stock Market Response to the Snowden Revelations*, 22 NEW MEDIA & SOC'Y 1976, 1982 (2020) (finding 605% increase in use of privacy-oriented search engine DuckDuckGo following Snowden revelations); Kristine Eck et al, *Evade and Deceive? Citizen Responses to Surveillance*, J. POL. (forthcoming 2021) (finding that 29% of Japanese research participants were more likely to exit a website after receiving a cookie warning specifically reminding them of the possibility of government surveillance compared to 21% of participants who received a more generic warning).

[9] I&A's "authorized intelligence activities" are exempt from DHS's Privacy Policy for Operational Use of Social Media, which provides the framework for most of the Department's use of social media. *See* U.S. DEP'T OF HOMELAND SEC'Y, PRIVACY POLICY FOR OPERATIONAL USE OF SOCIAL MEDIA 1 (2012), https://www.dhs.gov/sites/default/files/publications/Instruction_110-01-001_Privacy_Policy_for_Operational_Use_of_Social_Media_0.pdf.

- Dissemination of data: Social media information should only be disclosed to agencies outside DHS if it is related to criminal activity for which that agency has enforcement authority.
- Use of covert social media accounts: The policy should include an explicit prohibition on the use of covert and undercover accounts.
- Prohibition on targeting of constitutionally protected activity or protected characteristics: Explicit prohibition on the use of social media monitoring that is based, to any extent, on First Amendment protected speech or activity, race, religion, gender, sexual orientation, or immigration status. When, however, statements advocate unlawful activity, or indicate an apparent intent to engage in acts of violence, collection of data from social media may be warranted, unless it is apparent, from the circumstances or the context in which the statements are made, that there is no prospect of harm.

b. Audit and Evaluation

- The CRCL and Privacy Officers should conduct regular audits of I&A's social media monitoring to ensure that it is narrowly tailored to the expressed purpose, and to identify any civil rights or civil liberties violations. The audit should be provided to DHS leadership, as well as the homeland security committees of the Senate and House and to the Privacy and Civil Liberties Oversight Board (PCLOB). It should be made public; if redactions are necessary, they should be limited to the minimum amount necessary.
- I&A should, in consultation with the CRCL and Privacy Officers and PCLOB, develop metrics for evaluating the use of social media information and should publish annual reports measuring the program against these metrics. The metrics should be public. The reports should also be public; if redactions are necessary, they should be limited to the minimum amount necessary.

c. Congressional Oversight. The Senate and House homeland security committees should hold annual hearings to review I&A's use of social media.

○