BRENNAN CENTER FOR JUSTICE

DHS AT 20: AN AGENDA FOR REFORM

A New Vision for Domestic Intelligence

Fixing Overbroad Mandates and Flimsy Safeguards

By Spencer Reynolds and Faiza Patel

PUBLISHED MARCH 30, 2023

Built from 22 agencies with disparate missions, the Department of Homeland Security (DHS) routinely gathers intelligence to guide its strategic and operational activities.[1] But in the two decades since its inception, scores of incidents have undermined the legitimacy of its intelligence programs.

Congress and the department's own general counsel and inspector general, among others, have shown that DHS intelligence officers abused their counterterrorism authorities to suppress racial justice protests after the murder of George Floyd at the hands of a police officer.[2] In support of the Trump administration's goals to undermine the Black Lives Matter movement and spin an election-season story of anarchy, DHS sent intelligence officers to Portland, Oregon, to surveil protestors, create dossiers on dissidents, and enable U.S. Border Patrol special forces to whisk demonstrators away in unmarked vehicles. DHS's Office of Intelligence and Analysis (I&A) also surveilled prominent national security journalists and issued intelligence reports on their tweets. This political targeting was enabled by expansive intelligence authorities and a lack of meaningful checks on discretion.

While investigations into the department's response to the Portland protests provide a rare, detailed look at its operations, the concerns they raise are hardly limited to a single administration. Throughout its history, I&A has generated poorly sourced analysis heavily reliant on social media and on conjecture and caricature to draw sweeping conclusions. Its intelligence products are widely circulated to tens of thousands of police and other government officials nationwide, influencing their threat evaluations and responses to protests and social movements.

Other parts of DHS also raise concerns.[3] U.S. Customs and Border Protection (CBP) has used high-tech surveillance tools to target its critics. U.S. Immigration and Customs Enforcement (ICE) has monitored protestors. These programs, along with those run by other DHS components, operate with an opaque patchwork of rules that has proved both inadequate to counter abuses and resistant to transparency.

The time has come to rethink DHS intelligence operations and build safeguards that permit the department to provide its leadership with the information it needs while protecting civil rights and civil liberties. This report charts a course for doing so. It focuses initially on I&A, explaining how the office has veered from its counterterrorism mission into tracking social and political movements, often distributing shoddy information and

analysis. It then turns to other parts of DHS's intelligence infrastructure, highlighting significant operations run by CBP and ICE as well as situational awareness initiatives, which have often targeted Americans exercising their First Amendment rights. Finally, it explains why the departmental oversight bodies created by Congress to protect civil rights and liberties consistently fail to prevent intelligence abuses at DHS.

The report concludes with concrete recommendations to end the department's practice of broadcasting unreliable reports, implement better guardrails to protect civil rights and civil liberties, and create a robust and unified oversight structure. The secretary of homeland security should undertake these changes now, and Congress should codify reforms to ensure that limits on DHS endure across administrations.

The Office of Intelligence and Analysis

The Office of Intelligence and Analysis is DHS's head-quarters intelligence office. A member of the U.S. Intelligence Community, it collects, analyzes, and disseminates information to support departmental and national missions, which include countering international and domestic terrorism, foreign intelligence threats, international criminal drug activities, and threats to "critical infrastructure and key resources," along with addressing major disasters and national public health emergencies.[4] I&A also serves the ad hoc information demands of DHS leadership.[5] Its approximately 700 employees are mostly based in Washington, DC, with approximately 100 deployed to fusion centers around the country.[6] For fiscal year 2023, I&A shared a budget of more than $316 million with the Office of Homeland Security Situational Awareness, another headquarters office.[7]

The Homeland Security Act of 2002 established I&A, and a 2008 executive order authorizes the office to collect publicly available (or "open source") information. As the internet and social media — and the tools to mine them for insights into individuals — have ballooned, security agencies have prioritized this type of surveillance. I&A is also authorized to undertake overt collection from human sources, an authority it frequently uses to obtain data from other government personnel.[8] This authority also enables I&A to purchase data from private vendors, expanding the scope of its programs.[9]

The office serves as a hub for transmitting information from other DHS components and the 17 other federal agencies that make up the Intelligence Community to state and local police and funneling information back from them. In addition to informing the department's own programs, I&A's reports are disseminated to tens of thousands of law enforcement, intelligence, and private-sector recipients around the country, influencing resource allocation, assisting with the development of targets and priorities, and providing justification for policing and other security actions (including, for example, additional surveillance and information sharing).[10]

I&A's work, at times influenced by a quota system that "encourages collectors to over-report," has been marked by quantity over quality.[11] The office has widely circulated unverified raw intelligence based on ambiguous social media posts, and it regularly targets protest movements. Multiple internal surveys cited in a recent *Politico* article show that I&A staff were concerned about the legality of some activities and worried that articulating these concerns would result in retaliation.[12] I&A's intelligence analysis often relies on thin sourcing and faulty assumptions, making unsupported logical leaps, entrenching bias, and caricaturing marginalized communities and social movements. Less is known about how I&A employs overt collection, but it appears to use this authority to gather information not obtainable from public sources. The *Politico* exposé, however, documents I&A's practice of questioning people in detention without notifying their attorneys, a practice that was partially suspended last year because I&A's own staff worried it was illegal.[13]

Unverified Raw Intelligence

Since 2018, I&A has produced and disseminated an average of 1,100 open source intelligence reports (OSIRs) each year.[14] These reports, consisting of raw intelligence, are meant to warn Intelligence Community agencies and other government recipients about emerging threats.[15] Raw intelligence refers to data points that have not yet been thoroughly examined and evaluated by an analyst, which Intelligence Community agencies use to develop analytic products and identify trends.[16] Such material is generally unverified and can be unreliable, however, and the thousands of state and local law enforcement agencies that also receive OSIRs often lack the expertise to interpret them.

Although the OSIRs circulated by I&A frequently acknowledge the tenuous nature of the information they contain, they also often carry alarming labels — such as "extremist incites violence" — suggesting serious threats.[17] Moreover, OSIRs are based almost entirely on social media posts. As I&A's leadership has acknowledged, it is exceedingly difficult to identify real threats within a pool of millions of posts that are context-dependent, subject to interpretation, often ambiguous, and frequently anonymous.[18] I&A's staff members too say that "they struggle with determining whether a statement is hyperbole or reportable as an actual threat."[19]

Intelligence agencies defend this open source collection work as nonanalytic, saying that its purpose is to provide

raw material to analysts who can contextualize it. Indeed, I&A defended its broad dissemination of hundreds of OSIRs during the 2020 racial justice protests by pointing to caveats in the reports stating that they comprised "raw, unevaluated intelligence" and were "for lead purposes" only.[20] Such caveats are easily skipped over and likely serve as boilerplate justifications for broad dissemination rather than meaningful protections against misuse. When circulating intelligence to a wide audience, a domestic intelligence agency should not divest itself of the responsibility to ensure that it is providing credible and reliable information.

Through official investigations and press coverage, considerable information has emerged about I&A's activities during the 2020 racial justice protests, especially in Portland. Between May 25 and August 24, 2020, the office issued 366 OSIRs.[21] Yet a 2022 DHS inspector general report found that I&A "does not have comprehensive policies and procedures to ensure [that] its employees effectively collect [open source intelligence] and adhere to privacy protections."[22] A 2021 review by the DHS Office of the General Counsel (OGC) documented deep problems as well, ranging from pressure to generate this type of intelligence in support of the Trump administration's political goals to a lack of understanding of the difference between protected speech and threats.[23] The general counsel went so far as to recommend that I&A shift away from the type of short-term threat reporting found in OSIRs to refocus on support to intelligence analysts.[24]

One June 2020 OSIR illustrates how I&A spreads unsubstantiated information. Citing an anonymous social media user, the office issued a report claiming that anarchist extremists (a category that intelligence and law enforcement agencies treat as equivalent to terrorists) across the country had "staged piles of bricks . . . to fuel violent opportunists in major cities."[25] Whereas journalists easily and promptly discredited the claim, I&A apparently conducted no such due diligence.[26] The office ignored indications of the source's bias (other content in the post suggested opposition to the protests), did not question whether the photographs supported the assertions (there is no indication that they did), and failed to consider context such as the source's other social media posts or apparent location. The OSIR used Intelligence Community rhetoric (calling the bricks a "tactic, technique, and procedure") to suggest a terrorist threat. This report was distributed across the federal government and to thousands of police officers, bearing the imprimatur of homeland security specialists. This type of warning could easily encourage its recipients to police social movements more aggressively than they would otherwise.

I&A also surveilled journalists during the 2020 racial justice protests. The office circulated three OSIRs summarizing tweets written by a *New York Times* reporter and the editor in chief of a legal blog. These documents, ostensibly "provided for intelligence and lead purposes," reported that the journalists had published leaked, unclassified documents about DHS operations in Portland.[27] Why I&A or police would need information about journalists is difficult to envision; such reporting serves no legitimate purpose.

While the Portland protests did at times result in property damage and even physical confrontations between law enforcement and protestors, these types of incidents are a matter for local authorities, not a threat to national security requiring counterterrorism measures.[28] It seems the barrage of DHS reports about Portland was designed mainly to support the Trump administration's narrative that the racial justice protests were hijacked by "violent opportunists" sowing anarchy — a message the president and his cabinet members parroted across the airwaves — and to justify the deployment of more than 750 federal officers, including Border Patrol special forces.[29]

Dossiers on Protestors

>> I&A authored dossiers on people cited or arrested (including for nonviolent infractions) at protests in Portland. The total number of these dossiers, known colloquially as "baseball cards," is not known, but DHS investigators reviewed at least 43.[30]

To create the dossiers, I&A ran protestors' names through government travel and immigration systems, commercial data sets, and some systems the government would not publicly reveal. Among other sensitive data, the dossiers included protestors' passport numbers and immigration statuses. Using its social media tools, I&A swept up the names of protestors' friends and followers, possibly numbering in the "hundreds, if not thousands," and tracked their interests.[31] The dossiers were provided to DHS political leadership, the Federal Protective Service (a uniformed police division that secures federal property), at least one federal prosecutor, and potentially state and local government agencies.[32] Such information helps agencies with personnel on the ground target specific protestors, impede demonstrators' ability to mobilize, and generate leads for arrest.

I&A's reliance on sensitive intelligence systems to investigate detained Americans was hardly an aberration. According to I&A's then head, the office had done it "thousands" of times before.[33]

Sen. Ron Wyden characterized I&A's record during the protests as one of "stunning incompetence, mismanagement, and abuse of power . . . in order to politicize and inflame conflict in Portland." In a report issued in October 2021, Wyden castigated DHS intelligence officials as lacking "basic knowledge of their authority, what constituted real threats, and when it was appropriate to investigate Americans who were suspected of no crime at all."[34]

Beyond the flagrant overreach, this type of threat reporting is hardly useful. The OGC investigation noted that the FBI had complained about the "crap" that I&A was reporting as threats and concluded that there is "at best, anecdotal evidence" that OSIRs and the like are valuable to state and local law enforcement or the FBI.[35] Furthermore, OSIRs have little use in informing finished intelligence products such as those discussed in the next section. According to the OGC report, finished intelligence products in fiscal years 2019 and 2020 referenced less than 10 percent of OSIRs.[36]

Flawed Intelligence Analysis

In addition to circulating open source intelligence, I&A regularly authors and disseminates analytic intelligence reports, which are known by various names, including intelligence assessments, intelligence notes, field analysis reports, and finished intelligence. According to Intelligence Community standards, these reports are meant to piece together information from various sources, weighing their credibility and reaching judgments about their reliability to help decision-makers come to operational, policy, and strategic conclusions.[37]

To evaluate I&A's intelligence analysis, we reviewed more than 25 reports that have become publicly available because they were either released pursuant to Freedom of Information Act requests or leaked to the press. Much of the analysis is flawed. Several of the reports depict protest movements as terrorist threats and cast unwarranted suspicion on Muslim communities. Many are rife with speculation and unfounded assumptions, and some stray well beyond matters relating to national security.

In 2020, for example, as the Trump administration cracked down on racial justice protests, I&A released the OSIR describing "uncorroborated reports of bricks being pre-staged" at protests around the country. As described above, I&A apparently did nothing to verify this information, which turned out to be false.[38] The office instead recycled the information from the raw intelligence report into an analytic product, giving it further unwarranted credibility. The analytic product also listed "indicators" of potential rioting or violence among activists, including monitoring of law enforcement communications, travel and online planning by nonlocals, scouting of protest sites, concealment of identities, and encouragement of participants to protest in locations less populated with police.[39] None of these activities is indicative of criminal activity. But by framing them as suspicious, I&A invited police to investigate them.[40]

Several reports are highly speculative. For example, a 2013 assessment suggested that anti-gentrification "anarchist extremists" were targeting "urban development sites" based on three incidents in two states and Canada in which unknown persons set fire to or claimed credit for destroying construction sites.[41] The report acknowledged that the incidents were "unconnected" to one another, but it nonetheless extrapolated a terrorist threat. It also warned that such attacks may be preceded by "lower level criminal activity or mischief" or graffiti such as "Gentrification Kills" (which appeared in "several areas of Seattle" during the two years prior to the arson).[42] The case studies hardly supported I&A's suggestions that anti-gentrification activists were moving toward violence — which it portrayed as extremism — or that petty vandalism presages arson.[43]

A June 2018 I&A counterterrorism note released amid public outrage about the Trump administration's family separation policy reported an "increase in doxing incidents" based on the release by unknown persons of DHS facility locations and unspecified personal information about officials.[44] The two-page note found that the posting of this information "may lead to extremist violence by individuals vehemently opposed to purported or perceived DHS actions." I&A made this sweeping conclusion even though the report itself conceded that such threats have "historically been non-specific and aspirational in nature, and thus do not necessarily result in actualized physical violence." Rather than actual intelligence analysis, the report seems to have been intended to bolster the administration's narrative that supposed "antifa" (antifascists) were threatening government personnel and to build support for crackdowns on protestors.[45]

In these and other reports, the connection to terrorism or other federal homeland security matters is often tenuous. For example, so-called sovereign citizens, who reject government authority, often commit white-collar crimes, such as tax evasion and document fraud, and sometimes come into conflict with state and local law enforcement as a result.[46] Looking at 24 events over four years, a 2015 I&A paper found a "sporadic pattern" of violence between self-identified sovereign citizens and police during traffic stops and service of warrants, along with threats of retaliation for these actions. The paper included an extensive discussion of sovereign citizen ideology, which is embraced by a far larger number of people who have never participated in violence or criminal activities.[47] While local police are rightly concerned with protecting their safety in their interactions with criminals of all kinds, the connection between holding sovereign citizen beliefs and perpetrating terrorism is less direct than the intelligence suggests, and the federal counterterrorism interest in these matters is dubious.

Moreover, intelligence reports are often of poor quality. Even DHS's own acting secretary described an I&A intelligence assessment on foreign influence in elections from July 2020 as "written at the Fifth Grade level. . . . There were sentences that did not make sense. There was no cohesive argument. It lacked citations and context. It simply did not meet the standards of work product that I expect."[48] Such reports should not be driving federal, state, or local law enforcement efforts.

Misused Overt Collection

I&A has broad authority to collect information from human sources, including agents representing law enforcement entities, and to contract with private-sector data brokers.[49] So long as an I&A officer claims to be furthering a national or departmental mission, states a government affiliation, and comports with the other rules described below, it appears that no human sources or private vendors are off-limits. Similarly, no rules limit the type of information that I&A officers can acquire from other agencies (e.g., interview notes, law enforcement database entries, data from seized electronic devices, or copies of the devices themselves).[50] The same goes for contractors, from whom I&A can purchase collected raw intelligence, analytic findings, and other materials — far more than it could acquire on its own from publicly available information or human sources.

Two examples illustrate how I&A can bypass traditional safeguards through overt collection. First, through its Overt Human Intelligence Collection Program, which was initiated in 2016, it can question people in detention. Interviewees included people awaiting trial as well as those in immigration detention; apparently interviews of people awaiting trial who have been read their Miranda rights were paused in 2022.[51] I&A is not required to notify the detainee's attorney, which is the normal practice for law enforcement agents. I&A has acknowledged carrying out such questioning in Portland with the cooperation of local police, arguing that it did so with the consent of detained persons.[52] Such an argument is severely undermined by the inherently coercive conditions of detention. I&A does not appear to have procedures in place for documenting how it obtained consent, nor does it have any other safeguards for detained persons' constitutional rights. This collection method also undermines constitutional protections against police overreach by giving them a backdoor to information about defendants and investigative targets that they could not otherwise obtain.

Second, though I&A is generally not permitted to examine the contents of travelers' or others' cell phones, it can obtain information from both Americans' and foreigners' electronic devices from other agencies. In fiscal year 2020 alone, I&A officers used their overt collection authority to obtain from CBP information from more than 400 electronic devices, such as cell phones and laptops, "extracted" by officers scrolling through or copying them at ports of entry.[53] I&A then used this information to create or update more than 500 entries in the Intelligence Community's vast central terrorism database.[54] I&A's guidelines do not require officers to ensure that such information was properly acquired at the outset.

I&A can also offer technical assistance to partner agencies, thereby gaining access to devices' content. During the DHS response in Portland, for instance, I&A's field operations division apparently offered to the local government, which had retained arrested protestors' cell phones, to take and "exploit" these devices.[55]

Little information is publicly available about the extent to which I&A obtains and uses information via overt collection,[56] but its eagerness to deploy these methods in Portland suggests that it relies on them routinely.

I&A's Broad Mandate and Flimsy Safeguards

In the waning days of the Obama administration, I&A promulgated attorney general–approved intelligence oversight guidelines as required by Executive Order 12333, which established presidential policy for the Intelligence Community. The broad mandate and flimsy safeguards reflected in these January 2017 guidelines, along with DHS-wide policy proclamations and a lack of unified oversight, have enabled overreach and abuses.[57]

Expansive Missions

Under the 2017 guidelines, each of I&A's intelligence activities must further one or more national or departmental missions. These missions are sizable: they span international and domestic terrorism, hostile activities by foreign powers, international criminal drug activities, and risks to critical infrastructure and key resources (that is, those that are "essential to the minimal operations of the economy and government"). I&A is also directed to provide intelligence to help counter undefined "other threats to homeland security." Although I&A has apparently chosen to limit this catchall to threats of a certain "severity and magnitude" or those that it deems "significant," this restriction is so vague and discretionary as to hardly constitute a limitation.[58] Moreover, the provision of intelligence requested by the secretary or other DHS leadership is itself considered a departmental mission.

While these missions relate to real and serious threats, their breadth also means that they can serve as cover for a wide range of illegitimate government activities. Because intelligence gathering is generally a secretive enterprise, the public only rarely gets a glimpse of how these authorities are interpreted. Guidance issued by I&A in the summer of 2020, however, shows how broadly

these authorities have been construed. This "job aid" was meant to enable I&A officers to monitor protests against monuments (including Confederate ones) regardless of whether they fell under federal purview. Relying on a proclamation issued by President Trump, the guidance allowed officers to collect information about constitutionally protected demonstrations and speech if it would inform an "overall assessment" about potential threats to monuments. The guidance appears to assert that doing so would protect against terrorism and other threats to homeland security, despite no evidence that damage to statues would ever pose such a risk.[59]

I&A's overbroad interpretations of its mandate are not limited to the Trump administration. Today, DHS parses and judges "narratives" that it asserts drive white supremacist violence.[60] In two recent National Terrorism Advisory System bulletins, for instance, the department described a number of grievances expressed online as "false or misleading," including those reflecting the view that the government is "unwilling or unable to secure the U.S.-Mexico border" and opposition to Covid-19 mitigation policies.[61]

Such messaging risks exacerbating the tensions in political discourse by caricaturing tens of millions of Americans as potential terrorists.[62] Moreover, the approach can — and under polarized political circumstances likely will — be turned against Americans critical of government policy on race or immigration, casting their views as inherently dangerous and deserving of an aggressive law enforcement response. When ideology is treated as a marker of dangerousness, those in positions of authority decide which ideologies and speech they consider threatening.

Elastic "Reasonable Belief" Standard

The 2017 guidelines require that I&A officers operate on the basis of a "reasonable belief" that the information they are seeking to collect furthers one or more broad national or departmental missions.[63] DHS defines reasonable belief as a "belief based on facts and circumstances such that a reasonable person would hold that belief."[64] The department appears not to have further interpreted the provision, only explaining in guidance to intelligence officers that reasonable belief must be supported "with facts and circumstances you can articulate," that hunches and intuitions are insufficient, and that officers may rely on their "own experience, training, and knowledge."[65] The guidelines further require only that the basis for reasonable belief "can" be articulated — not that it must be — suggesting that there may be no documentation for many decisions made by I&A personnel.[66]

Reasonable belief is a vague standard, lacking clarity and leaving compliance to the discretion of intelligence officers. Reviews of I&A's work, such as the OGC report on Portland, make clear that its officers tend not to exercise this discretion well, targeting protestors and journalists, relying on specious indicators and speculation, and drawing sweeping conclusions about terrorism. Other Intelligence Community agencies, such as offices of the Department of Defense, use a similarly vague reasonable belief standard.[67] I&A stands out as particularly risky, however, because it operates domestically, regularly targets Americans, and issues its intelligence to a huge national audience for the purpose of influencing policing and security activities. The low reasonable belief standard does little to ensure that this audience receives reliable, accurate, and unbiased intelligence.

The guidelines seem to impose additional hurdles for I&A to maintain information in DHS databases and disseminate it in reports.[68] But such decisions are all premised on slight variations of the standard for collection, and they ultimately come down to whether collecting or disseminating the information furthers a national or departmental mission. The appearance of multiple layers of protection against overreach is by and large illusory.

For example, I&A officers may seek to collect Facebook posts from someone organizing a protest on the theory that the posts will help assess the risk of domestic terrorism, given that violence sometimes breaks out at these types of events. Officers may then add those posts or information derived from them to DHS raw intelligence materials and circulate them to I&A's many thousands of recipients so long as they believe that doing so furthers the mission to counter domestic terrorism, or another I&A mission.[69] All of this seems permissible under the 2017 guidelines, even though violence at protests rarely rises to the level of terrorism. So, in effect, I&A can gather, keep, and circulate information about First Amendment–protected activity.

The 2017 guidelines also purport to include special protections governing the retention of information about U.S. persons (mainly citizens and lawful permanent residents),[70] requiring that the information fit within certain categories. Yet these categories are typically permissive (for example, publicly available information) or reflect nothing more than the mission of a DHS component (such as border security or protecting critical infrastructure and key resources) that I&A is already separately authorized to support.[71] An officer who says that information is useful for a mission can usually also say that it fits into an information category, meaning that it can be used by I&A and retained permanently in DHS databases.

The guidelines' additional protections for disseminating information that refers to U.S. persons are similarly weak. The information must fit into one of several permanent retention categories (that is, it must serve one of DHS's or I&A's missions); the recipient must be a government agency, a foreign government, or a "private sector entity or individual with responsibilities relating to

homeland security," which describes an enormous set of recipients; and the officer seeking to disseminate the information must have a reasonable belief that the recipient could use it to further some intelligence, counterterrorism, law enforcement, or other homeland security–related function, which, given the breadth of these terms, also poses at best a minimal check.[72]

Other supposed safeguards in the guidelines also do little to constrain I&A. The requirement that officers use the least intrusive collection techniques feasible has minimal bearing on publicly available information, and feasibility is a functionally meaningless standard because it is left to officers' discretion.[73] The guidelines also require the masking of information about U.S. persons, but this too does not apply to publicly available information.[74] For other information, revealing U.S. persons' identity is permitted if doing so "would materially assist the intended recipient in using or understanding the disseminated intelligence or information." Given that I&A distributes its intelligence products to tens of thousands of law enforcement and private-sector recipients, often via broadly accessible web portals, any serious effort to consider the appropriateness of each recipient seems unlikely.[75]

Toothless Constitutional Protections

Domestic intelligence operations can serve as vehicles for monitoring and suppressing the First Amendment–protected activities that are fundamental to a functioning democracy. I&A's 2017 guidelines do not contain sufficiently robust rules to prevent this type of abuse, and other DHS guidelines seem not to apply.

The guidelines prohibit collecting intelligence for the "sole purpose" of monitoring First Amendment–protected activities.[76] But this is ultimately an empty protection: officers whose sole purpose is to monitor protected activity already lack a legitimate purpose because they would not be pursuing an authorized mission. Moreover, it is all too easy for I&A officers to point to an additional purpose or simply claim one of the broad national security missions. The guidelines offer scant protection once such a predicate is stated.

Implementation has also fallen short. The OGC review of I&A's activities in Portland found that all of the personnel who collected information on "current and emerging threats" demonstrated "major gaps" in their understanding of the scope of collection affecting First Amendment issues pursuant to the 2017 guidelines.[77]

DHS headquarters policy hardly offers protection either. In 2019, acting Secretary of Homeland Security Kevin McAleenan issued a memorandum purportedly forbidding the use of First Amendment–protected material.[78] But exceptions set forth in the memorandum mean that it does little to constrain I&A. The use of First Amendment–protected material is allowed when the department has "express statutory authorization."[79] "Express" does not mean explicit, however: the memorandum explains that a statute would be regarded as expressly authorizing the use of First Amendment–protected material if it "references activities that are relevant to a determination concerning an individual." Because intent is relevant to whether an act is considered to be terrorism, and First Amendment–protected material can indicate intent, the memorandum effectively excludes a swath of I&A's activities from the general prohibition against the use of such materials.[80]

In addition, the memorandum permits the use of First Amendment–protected material if doing so is "pertinent to and within the scope of an authorized criminal, civil, or administrative law enforcement activity."[81] Although I&A does not directly undertake law enforcement activities, its work can easily be considered "pertinent to" such activity because it provides intelligence to law enforcement agencies.

The 2017 guidelines also bar "intelligence activities based solely on an individual's or group's race, ethnicity, gender, religion, sexual orientation, gender identity, country of birth, or nationality." As with the First Amendment rule, I&A officers can easily find pretexts or proxies to avoid this stricture. The guidelines explicitly permit intelligence activities on the basis of a "reasonable belief" that considering a protected trait in conjunction with "other information" (which the guidelines fail to specify) furthers a mission.[82]

Other DHS Intelligence Programs

While I&A has faced the greatest recent scrutiny, other parts of DHS also carry out questionable intelligence operations. The Homeland Security Act recognizes a category of DHS "intelligence components," defined as parts of DHS that execute intelligence functions.[83] Although the law does not identify specific intelligence components, it states that they are broadly responsible for sharing information and supporting the intelligence mission led by the DHS undersecretary for intelligence and analysis.[84] The components carrying out these functions have some rules in place for particular operations or types of activities but no comprehensive, overarching framework akin to I&A's intelligence oversight guidelines or the FBI's *Domestic Investigations and Operations Guide* seems to exist.[85] Even though these guidance documents often fall short, they at least offer guideposts for the constitutional concerns raised by domestic intelligence collection.

Few public documents or press reports convey the full extent of components' programs, and the rules under

which they operate are opaque. This section highlights significant CBP and ICE initiatives for which there is substantial public information about abuses, as well as DHS situational awareness programs that permit broad monitoring of speech with few constraints.

CBP and ICE

At CBP, Congress established an Office of Intelligence but has given it little specific guidance. The office is mandated to formulate a "cohesive intelligence enterprise" in service of CBP's mission to police the border and trade. It maintains a presence at CBP's National Targeting Center in Virginia and claims to review more than 1,000 Intelligence Community products daily.[86] In consultation with the head of I&A, the office also establishes "intelligence-sharing relationships" with other government agencies.[87] CBP's commissioner is authorized to charge the office with additional intelligence responsibilities.[88]

CBP's expansive border security authorities cover terrorist travel and transnational crime and the enforcement of immigration and trade laws.[89] Federal regulation construes the "border" where CBP operates broadly to mean any land within 100 miles of the country's coast or land borders, a region that is estimated to cover some 200 million people and several states in their entirety.[90] Near the southern border in particular, CBP operates a thicket of surveillance towers, aircraft, sensors, and radars that track the movements of people, vehicles, and animals who cross the border or simply are near it.[91]

CBP uses this surveillance system — often in opaque ways — in support of its missions.[92] It has also turned these tools against its critics. In 2017, amid protests in San Diego against prototypes for President Trump's border wall, CBP stationed a movable surveillance tower to monitor political opposition, citing the demonstrations as a threat to its work. The tower, which was equipped with high-definition night-vision cameras, thermal sensors, and radar to track people and cars, remained in place for eight months.[93]

In 2019, using social media surveillance and other techniques, CBP created a list of immigration activists and aid workers, along with detailed dossiers about them.[94] Counterterrorism agents carried out extensive interviews with people on the list when they traveled through U.S. airports, pulling many of them into CBP offices for invasive conversations about their political leanings, work, and families. The information was shared with the Mexican government, which revoked several of the activists' visas.[95]

In Minneapolis in 2020, CBP redirected a Predator drone, commonly used in foreign military operations and for immigration enforcement along the border, to monitor protests against police brutality in the wake of George Floyd's murder.[96] Elsewhere, CBP has used drones to monitor the homes of pipeline protestors.[97]

More recently, CBP has monitored right-wing groups planning to commemorate the January 6, 2021, attack on the Capitol, despite the absence of any link to border security and its own conclusion that these events appeared to be nonviolent.[98]

As CBP's counterpart for enforcing immigration laws inside the United States, ICE also conducts intelligence operations. Its investigative arm, Homeland Security Investigations (HSI), includes an intelligence office that supports ICE's asserted authority to enforce "more than 400 federal statutes" across a range of topics including national security, public safety, immigration enforcement,

Operation Whistle Pig

>> Operation Whistle Pig, a CBP initiative that Yahoo News exposed in 2022, shows how DHS's lack of comprehensive policies and procedures can facilitate illegitimate activities.[99] In mid-2017, CBP officer Jeffrey Rambo started investigating a well-regarded national security reporter, Ali Watkins.[100] Rambo claimed that his interest in Watkins started as an effort to cultivate her and several other journalists for a CBP investigation into forced labor. He ran their names through an assortment of DHS databases. Based on Watkins' travel history — which Rambo had no justification to access — he noticed that she was traveling with a congressional security official, whom he suspected was leaking information to her. Rambo met Watkins at a bar, where he grilled her about the intimate details of her life and confirmed his suspicions.

An inspector general investigation into the operation found that CBP agents also tracked and likely analyzed congressional staffers' travel. Even members of Congress were routinely vetted, and some were apparently found to be "linked to people on the Terrorism Screening Database." Given the low standard for placement in the database and the prevalence of errors, this is unsurprising. But the fact that a CBP agent could run these types of queries without reason surely is.[101]

This highly invasive domestic intelligence operation was completely unrelated to CBP's mission, and it seems that no rules constrained agents. Watkins suffered professional and reputational harm, and the congressional security official was sentenced to prison for lying to the FBI during the investigation. The lack of regulations ultimately proved to be Rambo's salvation, though: the government declined to prosecute him in the absence of "CBP policies and procedures concerning Rambo's duties."[102]

and transnational crime.[103] Other parts of ICE operate an expansive information collection program, acquiring driver's license, child welfare, and utility information from state and local governments, and even buying location information from data brokers — a practice that academics and advocates have increasingly criticized as a violation of Fourth Amendment protections and a way to evade limits on government action.[104] Like CBP, ICE has also in effect pursued a family separation policy at the border, drawing on data mining tools to create "profiles of immigrant children and their family members" that are used to identify, locate, and investigate families of undocumented immigrant children.[105]

Also like CBP, ICE has turned its intelligence capabilities on Americans who oppose its operations. When advocacy organizations demonstrated in 2017 near an immigration detention center in Georgia, ICE tracked them online and in person. Its officers described one of the groups as a "known adversary" and considered blocking another organization's access to people detained at the facility in retaliation for its protest activity.[106] In 2018, ICE tracked "anti-Trump," anti-deportation, and anti–white supremacist protests in New York.[107] And it used intelligence from a private contractor to monitor hundreds of protests nationwide against the family separation policy.[108]

Situational Awareness

Many DHS components also engage in around-the-clock surveillance of social and other media via situational awareness programs. Our review of publicly available government documents identified at least 12 overlapping programs for tracking what Americans are saying online. Two significant examples are discussed here.

The National Operations Center (NOC) is tasked by Congress to provide the "entire" government and private sector with situational awareness, or information that "can form the basis for incident management decision-making and steady-state activity."[109] The NOC tracks and reports on political events and speech. It has issued multiple bulletins describing the 2020 racial justice protests and related vandalism and public opinion.[110] Yet despite its constant surveillance of the internet, the NOC issued no warnings leading up to or during the January 6 attack on the Capitol, instead reportedly telling the Pentagon that there were "no major incidents of illegal activity" after rioters had already breached Capitol barricades.[111]

The Federal Emergency Management Agency (FEMA) also maintains a situational awareness initiative that routinely monitors First Amendment–protected activity. Although FEMA's primary mission concerns disaster preparedness and response, the agency tracks a range of broad and innocuous terms on social media (such as *agriculture*, *authorities*, *China*, and *cops*) and monitors a wide swath of media including the right-wing news aggregator Drudge Report and WikiLeaks, which lack any apparent connection to a disaster preparedness mission.[112] Like the NOC, FEMA has monitored protests, including demonstrations in Ferguson, Missouri, and Philadelphia, and has tracked Black Lives Matter activists in Washington, DC.[113]

These intelligence programs regularly veer into monitoring First Amendment–protected activity in part because oversight mechanisms are too weak to prevent abuses.

Oversight

Given the scope of DHS's intelligence programs, robust oversight is critical to prevent abuses, unearth errors, give Congress and departmental leadership visibility into agency activities, and ensure a streamlined and efficient use of personnel and resources. Instead, the department's sprawling intelligence enterprise is subject to little coherent scrutiny.

Two DHS-wide oversight offices — the Office for Civil Rights and Civil Liberties (CRCL) and the Privacy Office — are meant to keep a check on the department's activities, including its intelligence programs. In addition, the Office of the General Counsel is charged with interpreting legal authorities and restrictions that affect intelligence operations. Finally, I&A also has a separate internal Intelligence Oversight Office.[114] These offices, however, are often neutered for reasons ranging from structural shortcomings to turf battles to operational incentives that reward aggressive intelligence activities.

Civil Rights and Civil Liberties Oversight

CRCL and the Privacy Office have failed to live up to their broad congressional mandates to ensure respect for constitutional and statutory rights.[115] Reports by DHS's general counsel and inspector general show that CRCL in particular is regularly sidelined by operational components and senior leadership. Even when consulted, CRCL's role is often limited.[116] In a contest between I&A's interest in expansive intelligence collection and CRCL's efforts to protect civil rights and civil liberties, the latter almost invariably loses.

CRCL's role in reviewing finished intelligence assessments has fluctuated over time, seemingly driven by political pressures.[117] In addition, according to the DHS inspector general's report, there are no

> formal intelligence oversight and legal reviews of OSIRs before they are disseminated. In the past, raw intelligence, including OSIRs, received a formal pre-dissemination review, but the volume of raw intelligence made the requirement unmanageable. In May 2021, I&A tried to add more oversight of raw

> intelligence by encouraging collectors to seek prepublication guidance for OSIRs and increasing collection staff's access to an intelligence officer. However, prepublication review is not required, leaving [open source collection operations] subject to noncompliance with important guidance such as privacy protection guidelines.[118]

At this time, according to I&A's head of intelligence operations, CRCL is not in the review chain for I&A's raw intelligence reports but rather is in an "audit" posture. The official was not aware of any audits by CRCL.[119]

When it comes to component intelligence programs, CRCL seems to exercise minimal oversight, although it does field complaints. Our examination of the office's reports to Congress and other publicly available documentation has not revealed any publicly visible CRCL review of component intelligence efforts.

Privacy Oversight

Compared with CRCL, the Privacy Office has better entry points for oversight. Legal requirements for oversight and compliance documentation, such as privacy impact assessments, provide an opportunity for the Privacy Office to implement guardrails for intelligence efforts that involve data systems, both at I&A and elsewhere in DHS. However, this documentation often fails to fully address privacy concerns, suggesting that the office's influence is limited.[120]

The Privacy Office is also set up to have better insight into component programs, because each component has a privacy officer who is meant to perform their oversight activities in coordination with the chief privacy officer. This provides headquarters Privacy Office staff a window into intelligence programs across the department. But component privacy officers report to those responsible for operational activities, so operational imperatives can easily override any concerns they raise.[121] Ultimately, while good privacy policy should be central to safeguards at DHS, privacy documentation appears no more protective in the components than at headquarters.

Legal Advice and Counsel

While CRCL and the Privacy Office provide policy guidance, the Office of the General Counsel interprets and offers advice regarding I&A's legal authorities.[122] Yet, as one of the authors of this report experienced firsthand, OGC attorneys assigned to I&A have limited influence due to the permissiveness of the legal regime. Further, the general counsel's accounting of I&A's actions to suppress racial justice demonstrations in 2020, authored at the secretary's direction, described how multiple layers of I&A management disregarded serious concerns expressed by the office's legal and policy counsel and were hostile to basic questioning and fact-finding.[123] According to the report, the head of the social media surveillance team even instructed staff not to take questions to the attorneys designated to provide them with guidance.[124]

When it comes to the components, OGC faces an additional hurdle: only its headquarters office appears to have a unit dedicated to intelligence law, and component lawyers are poorly equipped to keep up with intelligence programs operating far from headquarters in regions such as the southern border.[125] Given the challenges faced by attorneys seeking to hold I&A to its legal authorities, it seems unlikely that the general counsel's office has significant influence on the intelligence programs run by the likes of CBP and ICE. As CBP's Operation Whistle Pig shows, some of the department's most aggressive programs may operate without any legal guidance.

Intelligence Oversight Officer

In addition to the DHS-wide controls set out above, I&A also has an intelligence oversight officer who is charged with implementing its oversight guidelines.[126] The intelligence oversight officer is responsible for training the office's personnel about the guidelines, conducting preliminary inquiries into potential violations, and reporting the findings of those inquiries to internal offices such as OGC, CRCL, and Privacy. However, with just seven staff members as of the latest public reporting, the oversight officer is hardly in a position to properly oversee I&A's vast intelligence output.[127]

The oversight officer reports to the undersecretary for I&A, who is not required to heed the officer's advice.[128] This structure disincentivizes robust oversight, especially in situations where controls are most needed. DHS's general counsel barely mentions the oversight officer in its review of I&A's Portland operations, suggesting that the role is of limited relevance during I&A's toughest moments. In any event, it is hard to believe that the same I&A leadership that — as the investigations into Portland have shown — has stymied DHS oversight offices and ignored concerns raised by the people charged with intelligence collection would heed concerns raised by internal subordinate oversight staff.[129]

Recommendations

DHS has a broad mandate. Its decision-makers need a lot of information to execute their jobs effectively. But many of the operations carried out by I&A and other DHS intelligence programs stray too far from their lawful missions and instead sweep up information about First Amendment–protected activities. These operations are enabled by expansive authorities that

internal rules and oversight have failed to contain. The time has come to focus these oversight efforts and build more robust safeguards against overreach. We offer four sets of recommendations for reform; the first three are directed to the secretary of homeland security and the last to Congress.

Recommendations for the Secretary of Homeland Security

>> Direct I&A to end its practice of circulating unverified raw intelligence.

The secretary should dismantle the OSIR reporting system. For I&A's other uses of social media information, the secretary should direct the office to document and publicly disclose the empirical foundations for its informational assessments, the relationships it establishes between users, and other conclusions it draws.

>> Revise the 2017 I&A guidelines to better protect constitutional rights and ensure transparent and effective intelligence practices.

I&A's current guidelines should be amended to meaningfully safeguard the exercise of its intelligence mandate. The secretary, working with the attorney general, should amend them as follows:

- **Substantiate collection activities.** The requirement that I&A personnel have a reasonable belief that collection furthers their broad missions should be amended to require I&A personnel to record in writing their specific justifications for accessing and collecting information, including any search terms used. I&A must also ensure that its information systems can be audited for compliance with its own guidelines and other DHS policies. It should audit these systems as directed by the new oversight office discussed below.

- **Prevent misuse of overt collection authority.** The guidelines should extend the prohibition on I&A tasking other government agencies with collecting information on its behalf to implicit tasking, a practice also known as "sensitizing" (e.g., when I&A personnel relay their interest in certain types of information to personnel from other agencies). Protections against abuse in I&A's overt collection activities should be strengthened in the guidelines, which should incorporate prohibitions on interviewing detained individuals or persons subject to ongoing government investigation.

- **Clarify implied consent.** The guidelines give I&A great latitude in collecting, using, and retaining information obtained with consent, which can be implied by "adequate notice" and when "adequate policy has been published or otherwise articulated." They should clarify the department's understanding of implied consent and the various scenarios in which I&A can permissibly rely on it for intelligence collection. This means that I&A should commit to complying with social media platforms' terms of service, which generally prohibit scraping and surveillance, as it conducts its open source collection.

- **Substantiate dissemination decisions.** The guidelines require that each instance of intelligence dissemination be supported by a reasonable belief that it furthers a mission. Yet I&A's dissemination of intelligence via platforms accessible to tens of thousands of federal, state, and local personnel suggests that it does not make these determinations on the appropriate case-by-case basis. The guidelines should require that I&A officers document their justifications prior to making intelligence available to any recipient to ensure that only recipients who can use it appropriately and responsibly receive it.

- **Strengthen protections for U.S. persons information.** The guidelines should provide that I&A personnel must in all cases anonymize information about U.S. persons prior to dissemination, replacing it with a generic marking identifying the individual simply as a U.S. person (e.g., USPER1 and USPER2).[130]

- **Account for bulk data transfers.** The secretary should order an accounting of the extent and type of bulk data transfers undertaken by I&A and ensure that the public and Congress understand these transfers, as well as the other means of information sharing identified in section three of the guidelines. These transfers involve large quantities of data, the majority of which may not have any intelligence value, and may not even have been assessed for the extent of Americans' information contained therein. The secretary should transmit this accounting to the congressional homeland security and intelligence committees, and as much as possible should be made public.

- **Ensure effective protection of constitutional rights.** Current rules that prohibit I&A from undertaking an activity for the sole purpose of burdening constitutional rights are ineffective and should be strengthened. For a start, the guidelines should explicitly recognize — as the FBI has — that "online information, even if publicly available, may be protected by the First Amendment."[131]

>> Create a unified and empowered office to conduct intelligence oversight.

Critical deficiencies in intelligence oversight must be rectified. A new Oversight Office could do so by covering the full range of DHS's intelligence programs, centralizing oversight authority so that offices no longer report to

officials they are meant to oversee and signaling DHS leadership's commitment to preserving the legitimacy of the department's domestic intelligence programs.

The secretary can create this office immediately. Section 872 of the Homeland Security Act authorizes the reorganization of department functions with 60 days' notice to Congress.[132]

To reinforce the authority of the Oversight Office and boost the influence of existing mechanisms, the secretary should also establish an intelligence policy and review committee with representatives from CRCL, Privacy, OGC, I&A, and the Office of Strategy, Policy, and Plans. The committee should be chaired by the head of the Oversight Office and mandated to provide advice on all matters within the office's jurisdiction. The Oversight Office should obtain the committee's advice on any significant policy disagreements with an operational unit of the department.

Functions of the Oversight Office

Various oversight functions that are currently scattered across the department should be centralized in this office, including the following:

- the functions of I&A's oversight office;
- integrated intelligence oversight across DHS, including in components such as CBP and ICE;
- promulgation of department-wide standards for appropriate intelligence activities (e.g., collection and dissemination of information), enhanced protections of information and persons implicated by intelligence activities, transparency, oversight inquiries, and oversight reporting;
- development of standards for evaluating the efficacy of intelligence programs and the protections they incorporate (e.g., assessing the usefulness of I&A's social media monitoring and how I&A distinguishes between protected speech and association and true threats and incitement);
- standardization, policy development, and coordination of the department's disparate intelligence activities;
- training;
- advising on all proposed intelligence operations;
- enforcement of the matters under its purview through ongoing monitoring and audits of intelligence operations; and
- reporting of intelligence guidelines violations to external entities such as Congress, the Office of the Director of National Intelligence, and the President's Intelligence Advisory Board, and reporting of activities and violations to the public.

When a DHS component disagrees with the Oversight Office's determination about a policy or program, the component should be able to elevate the matter to the deputy secretary, who would be required to consider the input of the oversight officer and the intelligence policy and review committee. Whenever the deputy secretary overrules the intelligence oversight officer, that determination and its justification should be recorded and promptly reported to the congressional intelligence and homeland security committees.

Independence and Access

To fulfill its mandate and to resist capture, the Oversight Office must be independent and properly staffed. To this end, its head should be appointed for a five-year term, removable only for cause. At least half of its staff should have policy or investigative backgrounds (e.g., experience in an inspector general's office; on a congressional committee; in a governmental privacy, civil rights, civil liberties, or legal office; or in a civil society organization).

The secretary should require all DHS offices and components to give the Oversight Office unrestricted access to their records and personnel (including those outside of formally designated intelligence programs) and to participate in its efforts to develop standards and policies. Given the scope of this task, the office should begin with a pilot project focused on I&A. During the pilot project, the Oversight Office should develop practices for information access, investigations, record keeping, and report writing. Incorporating lessons learned from working with I&A, it should then expand its model to all DHS headquarters offices conducting intelligence activities, such as the NOC, and thereafter to component intelligence programs, such as those in CBP or ICE.

To ensure that policy guidance accounts for the evolving nature of intelligence operations, the Oversight Office should monitor implementation on an ongoing basis. Accordingly, it must have near real-time access to intelligence agencies' information and systems. DHS computer systems (which are used for social media surveillance, collection and retention of raw intelligence, development of analytic products, and dissemination) should be accessible by Oversight Office personnel.[133] In addition, the Oversight Office should be authorized to embed personnel into component intelligence programs and to visit intelligence personnel in the field.

Policy Development and Reporting

Within its first 180 days, the Oversight Office should provide the secretary with its accounting of the scope of the department's intelligence activities. This accounting

should identify the offices and components that conduct intelligence activities and the nature and extent of these programs. It should also include a baseline mapping of the policies of and justifications for these programs and any reports or prior investigations into their conduct. A public version of this report should be made available to appropriate inspectors general and congressional oversight committees and should be published on the DHS website. The accounting should be updated periodically.

Building on its initial report, within one year of its creation, the Oversight Office should promulgate DHS-wide intelligence policies, which should cover standards for appropriate access, collection, retention, and dissemination of information. These policies should focus on potential harm to U.S. persons and constitutional standards; permissible uses of intelligence for activities across the department, including to aid law enforcement, screening and vetting, and watch-listing; documentation of intelligence activities, reports, and products, and procedures for their review, including for review of novel or sensitive activities (e.g., those potentially affecting Americans); whistleblower protections and reporting of noncompliance and questionable activities; and data stewardship standards.

Recommendations for Congress

Congress created DHS's domestic intelligence infrastructure, and it must ensure that this perennially fraught undertaking is properly regulated. To start, Congress should pass a legislative charter for the Oversight Office and create an undersecretary-level position for its head to give it the necessary political clout within the department to do its job. In addition, Congress should pass legislation to curb the enormous discretion afforded to DHS intelligence programs, including by defining the scope of "other threats to homeland security" and promulgating guidelines on the scope of I&A support for DHS component missions. It should also codify into law robust protections of the First Amendment and against biased decision-making, and it should limit the full use of appropriated funds through conditions or prerequisites until DHS strengthens internal protections.

Conclusion

Overbroad mandates, flimsy safeguards, and fragmented oversight have allowed overreach and abuses to proliferate across DHS intelligence programs. There is much that the secretary of homeland security can do to put these programs on firmer footing, both by delineating better standards and stronger safeguards and by creating a new centralized Oversight Office that will cover the full range of DHS activities and have the institutional heft to carry out its critical functions. Congress can encourage the department in this direction, both through its own oversight function and by legislating better oversight and rules. Two decades after the creation of DHS, it is time to put insights about the pitfalls and promise of its efforts to use.

Endnotes

1 By intelligence, we mean the accessing, collecting, retaining, analyzing, or disseminating of information by any component of the Department of Homeland Security (regardless of U.S. Intelligence Community membership) to inform operational, policy, or strategic decisions not directly connected to a predicated criminal investigation, including for purposes such as situational awareness (e.g., to identify and keep abreast of breaking events, including emerging crises); threat detection (e.g., to identify potential threats of violence and terrorism, including by specific individuals); tip and lead generation; civil enforcement of immigration laws; and substantively similar purposes.

2 Office of Inspector General (hereinafter OIG), *The Office of Intelligence and Analysis Needs to Improve Its Open Source Intelligence Reporting*, Department of Homeland Security (hereinafter DHS), July 6, 2022, https://www.oig.dhs.gov/sites/default/files/assets/2022-07/OIG-22-50-July22.pdf (hereinafter OIG, *I&A Needs to Improve Its Open Source Intelligence Reporting*); Office of Intelligence and Analysis (hereinafter I&A), *Office of Intelligence and Analysis Operations in Portland*, DHS, April 20, 2021, https://www.wyden.senate.gov/imo/media/doc/I&A%20and%20OGC%20Portland%20Reports.pdf (hereinafter I&A, *I&A Operations in Portland*); and Office of the General Counsel (hereinafter OGC), *Report on DHS Administrative Review into I&A Open Source Collection and Dissemination Activities During Civil Unrest: Portland, Oregon, June Through July 2020*, DHS, January 6, 2021, 13, https://www.wyden.senate.gov/imo/media/doc/I&A%20and%20OGC%20Portland%20Reports.pdf (hereinafter OGC, *Administrative Review into I&A Open Source Collection*). (Heavily redacted versions of I&A's and OGC's reports regarding I&A's activities in Portland were previously released in 2021. In October 2022, Senator Wyden released new versions of the reports, both of which are compiled in one document. The OGC report begins on page 13 of the compiled document; page numbers cited are the document's, not the original report's.)

3 DHS offices are divided into operational and support components. Operational components are agencies such as CBP and ICE, while support components — sometimes referred to as headquarters offices — provide "specific assistance" to DHS operations, including legal, policy, liaison, and intelligence support. These distinctions are largely technical in nature: support components such as I&A run operations and operational components such as CBP have legal and policy subdivisions. DHS, "Organization of the Department of Homeland Security," March 31, 2009, https://www.dhs.gov/sites/default/files/publications/mgmt/human-resources/mgmt-dir_252-01-organization-of-the-dhs_rev-00.pdf.

4 I&A, *Department of Homeland Security, Office of Intelligence and Analysis, Instruction IA-1000: Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines*, DHS, January 19, 2017 (hereinafter I&A, *Intelligence Oversight Program and Guidelines*), app. B, glossary 3–4, https://www.dhs.gov/sites/default/files/publications/office-of-intelligence-and-analysis-intelligence-oversight-program-and-guidelines.pdf. (I&A's *Intelligence Oversight Guidelines* are appended to IA-1000 at page 10 of the document and referred to as appendix B in the main body of the document. However, the *Guidelines* are not labeled as appendix B.)

5 I&A also leads DHS's counterintelligence program, serves as the lead for DHS nominations to the central Terrorist Identities Datamart Environment repository, and is authorized to provide technical knowledge and expert assistance to law enforcement partners. Privacy Office, *Privacy Impact Assessment for the DHS Counterintelligence Program*, DHS/ALL/PIA-086, DHS, August 31, 2020, 1–2, https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhsall086-ciprograms-august2020.pdf; National Counterterrorism Center, Watchlisting Guidance, Office of the Director of National Intelligence, March 2013, 21, § 1.48.4, https://www.eff.org/files/2014/07/24/2013-watchlist-guidance_1.pdf; and Exec. Order No. 12333, § 2.6, 3 C.F.R. 200 (1981). These activities also raise various concerns that are not within the scope of this report. Finally, the office manages the Nationwide Suspicious Activity Reporting Initiative, which we discuss in our report on fusion centers. Michael German, Rachel Levinson-Waldman, and Kaylana Mueller-Hsia, *Ending Fusion Center Abuses: A Roadmap for Robust Federal Oversight*, Brennan Center for Justice, December 15, 2022, 7–8, https://www.brennancenter.org/our-work/policy-solutions/ending-fusion-center-abuses.

6 OIG, *I&A Needs to Improve Its Open Source Intelligence Reporting*, 1; and Government Accountability Office (hereinafter GAO), *Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results*, September 29, 2010, https://www.gao.gov/assets/a310273.html.

7 Consolidated Appropriations Act, 2023, Pub. L. 117-328, § F(I) (2022), https://www.congress.gov/bill/117th-congress/house-bill/2617/text.

8 Exec. Order No. 12333, § 1.7 (i), as amended by Exec. Order No. 13470, § 1.11, 3 C.F.R. 218 (2008); and I&A, *Intelligence Oversight Program and Guidelines*, app. B, glossary 4.

9 For example, I&A has entered into a contract with SITE Intelligence Group to track social media. Publicly available contracting documentation offers little assurance that a contractor will abide by the rules that apply to I&A's intelligence activities or by the department's legal, civil rights, civil liberties, and privacy policies. Office of Procurement Operations, *Justification and Approval for Other Than Full and Open Competition*, Authority 41 U.S.C. 3304(a)(1), J&A no. FY21-00280, DHS, accessed February 13, 2023, https://sam.gov/api/prod/opps/v3/opportunities/resources/files/15b57dedcdb2437ea13701c2192ecb39/download?&status=archived&token=.

10 Among its other methods of disseminating information such as via participation in fusion centers and task forces, I&A maintains a community of interest for intelligence topics on the Homeland Security Information Network (HSIN), which reaches more than 10,000 recipients across all levels of government. DHS, "HSIN-Intel: Partner Products," DHS, accessed February 13, 2023, https://www.dhs.gov/sites/default/files/publications/HSIN-Brochure-HSIN-Intel%20Partner%20Products.pdf. The broader HSIN platform has nearly 150,000 registered users. HSIN, *2020 Annual Report: Delivering Mission Success*, DHS, June 21, 2021, 12, https://www.dhs.gov/sites/default/files/publications/hsin-fy20-annual-report_1.pdf; and German, Levinson-Waldman, and Mueller-Hsia, *Ending Fusion Center Abuses*, 5.

11 OGC, *Administrative Review into I&A Open Source Collection*, 85.

12 Betsy Woodruff Swan, "DHS Has a Program Gathering Domestic Intelligence — and Virtually No One Knows About It," *Politico*, March 6, 2023, https://www.politico.com/news/2023/03/06/dhs-domestic-intelligence-program-00085544.

13 Woodruff Swan, "DHS Has a Program Gathering Domestic Intelligence."

14 OIG, *I&A Needs to Improve Its Open Source Intelligence Reporting*, 2; and I&A, *Office of Intelligence and Analysis Transition Overview*, DHS, 19, https://www.dhs.gov/sites/default/files/publications/I%26A%20PTO%20Records.pdf (describing 2016 collection statistics).

15 I&A, *Department of Homeland Security, Office of Intelligence and Analysis, Policy Instruction IA-900: Official Usage of Publicly Available Information*, DHS, January 13, 2015, 2–3, https://www.aclu.org/sites/default/files/field_document/dhs_policy_re_official_use_of_public_social_media_info_-_01.13.2015.pdf (defining open source, publicly available information, and social media).

16 See Office of the Director of National Intelligence, "How the IC [Intelligence Community] Works," accessed February 13, 2023, https://www.intelligence.gov/how-the-ic-works.

17 Over the years, I&A has consistently labeled OSIRs as unevaluated while asserting that subjects of those OSIRs are "extremists" or involved in terrorism. See, e.g., DHS, "Open Source Intelligence Report (OSIR)," November 1, 2016, 1–2, https://cdn.muckrock.com/foia_files/2017/09/26/2017-IAFO-00333_CD_Response_3.pdf. The endnotes of one I&A analytic product that cites OSIRs illustrate the inflammatory titles often given to this raw intelligence. Counterterrorism Mission Center (hereinafter CTMC), "Terrorists Exploiting COVID-19 Pandemic in an Attempt to Incite Violence," DHS, March 23, 2020, 1, 3, https://www.okhighered.org/state-system/corona/docs/dhs-note-32320.pdf.

18 See, e.g., *Examining the January 6 Attack on the U.S. Capitol, Hearing Before the S. Comm. on Homeland Security and Governmental Affairs and S. Comm. on Rules and Administration*, 117th Cong. (2021) (testimony of Melissa Smislova, acting DHS undersecretary for I&A), 3, https://www.hsgac.senate.gov/imo/media/doc/Testimony-Smislova-2021-03-03.pdf.

19 OIG, *I&A Needs to Improve Its Open Source Intelligence Reporting*, 11.

20 I&A, *I&A Operations in Portland*, 11.

21 OIG, *I&A Identified Threats Prior to January 6, 2021, but Did Not Issue Any Intelligence Products Before the U.S. Capitol Breach*, DHS, March 4, 2022, 20, https://www.oig.dhs.gov/sites/default/files/assets/2022-04/OIG-22-29-Mar22-Redacted.pdf.

22 OIG, *I&A Needs to Improve Its Open Source Intelligence Reporting*, 11.

23 Faiza Patel, Rachel Levinson-Waldman, and Harsha Panduranga, *A Course Correction for Homeland Security: Curbing Counterterrorism Abuses*, Brennan Center for Justice, April 20, 2022, 7–8, https://www.brennancenter.org/our-work/research-reports/course-correction-homeland-security; OGC, *Administrative Review into I&A Open Source Collection*, 64, 69.

24 OGC, *Administrative Review into I&A Open Source Collection*, 83–84.

25 I&A, "Open Source Intelligence Report (OSIR)," DHS, June 2, 2020, https://www.documentcloud.org/documents/6988598-June-2-Tweets-Claiming-Antifa-Is-Planting-Bricks.html (hereinafter I&A, "June 2020 OSIR").

26 Matthew Price and Lorand Bodo, "Viral Rumors About Bricks Meant to Encourage Protest Shown to Be False," NBC News, June 4, 2020, https://www.nbcnews.com/news/us-news/live-blog/2020-06-02-nationwide-protests-over-george-floyd-death-live-n1221821/ncrd1222216.

27 Benjamin Wittes (@benjaminwittes), "Document #2," Twitter, July 31, 2020, https://twitter.com/benjaminwittes/status/1289298151422140416/photo/1; and 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.

28 OIG, *DHS Had Authority to Deploy Federal Law Enforcement Officers to Protect Federal Facilities in Portland, Oregon, but Should Ensure Better Planning and Execution in Future Cross-Component Activities*, DHS, April 16, 2021, 6, https://www.oig.dhs.gov/sites/default/files/assets/2021-04/OIG-21-31-Mar21.pdf.

29 DHS, "Myth vs. Fact: 50+ Nights of Violence, Chaos, and Anarchy in Portland, Oregon," July 27, 2020, https://www.dhs.gov/news/2020/07/27/myth-vs-fact-50-nights-violence-chaos-and-anarchy-portland-oregon; Ronn Blitzer, "Acting DHS Secretary Wolf: Feds Will Take 'Action' Against Protest Hijackers," Fox News, June 7, 2020, https://www.foxnews.com/politics/acting-dhs-sec-wolf-doj-taking-action-against-protest-hijackers (playing clips of Attorney General William Barr and President Trump echoing these themes); and Ed Pilkington, "'These Are His People': Inside the Elite Border Patrol Unit Trump Sent to Portland," *Guardian*, July 27, 2020, https://www.theguardian.com/us-news/2020/jul/27/trump-border-patrol-troops-portland-bortac.

30 OGC, *Administrative Review into I&A Open Source Collection*, 69n430.

31 See Dell Cameron, "Homeland Security Admits It Tried to Manufacture Fake Terrorists for Trump," *Gizmodo*, November 5, 2022, https://gizmodo.com/donald-trump-homeland-security-report-antifa-portland-1849718673.

32 OGC, *Administrative Review into I&A Open Source Collection*, 66.

33 OGC, *Administrative Review into I&A Open Source Collection*, 66n400.

34 Office of Sen. Ron Wyden, "Wyden: New Report Shows Stunning Incompetence and Abuse of Power by Trump DHS in Portland," press release, October 1, 2021, https://www.wyden.senate.gov/news/press-releases/wyden-new-report-shows-stunning-incompetence-and-abuse-of-power-by-trump-dhs-in-portland.

35 OGC, *Administrative Review into I&A Open Source Collection*, 36.

36 OGC, *Administrative Review into I&A Open Source Collection*, 36.

37 Office of the Director of National Intelligence, "Intelligence Community Directive 203: Analytic Standards," January 2, 2015, https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf (describing Intelligence Community standards for analysis, including those related to integrity, weighing credibility, sourcing, logical argumentation, and clarifying assumptions and judgments).

38 CTMC, "Substantive Revision: Some Violent Opportunists Probably Engaging in Organized Activities," DHS, June 2, 2020, 2, https://info.publicintelligence.net/DHS-ViolentOpportunistsCivilDisturbancesRevision.pdf; I&A, "June 2020 OSIR"; and Price and Bodo, "Viral Rumors About Bricks."

39 CTMC, "Substantive Revision," 2.

40 This type of indicator reporting is common for I&A; across administrations, the office has bundled common behaviors as suspicious. Harsha Panduranga, *Community Investment, Not Criminalization: A Call to Abandon the Department of Homeland Security's Violence Prevention Strategy*, Brennan Center for Justice, June 17, 2021, https://www.brennancenter.org/our-work/research-reports/community-investment-not-criminalization.

41 I&A, "Self-Identified Anarchist Extremists Target Urban 'Gentrification' Sites with Arson," DHS, July 23, 2013, 1, https://info.publicintelligence.net/DHS-AnarchistGentrificationArson.pdf.

42 I&A, "Self-Identified Anarchist Extremists," 3.

43 The report also ignores the idea that small acts of vandalism and arson on unoccupied, incomplete housing developments likely do not constitute "terrorism" under the Homeland Security Act definition. That definition requires an act that "is dangerous to human life or potentially destructive of critical infrastructure or key resources" (6 U.S.C. § 101 (2018)). This type of construction site vandalism poses neither.

44 I&A, "Incidents of Doxing of DHS Officials May Lead to Extremist Violence," DHS, June 29, 2018, 1, https://www.documentcloud.org/documents/7002565-June-29-2018-Incidents-of-Doxing-of-DHS.html.

45 I&A, "Incidents of Doxing."

46 Lexipol, "5 Responses to a Sovereign Citizen at a Traffic Stop," February 10, 2015, https://www.police1.com/patrol-issues/articles/5-responses-to-a-sovereign-citizen-at-a-traffic-stop-FZ4ruThuMxTHVgEO.

47 I&A, *Sovereign Citizen Extremist Ideology Will Drive Violence at Home, During Travel, and at Government Facilities*, DHS, February 5, 2015, 1, 3, https://info.publicintelligence.net/DHS-SovereignCitizenIdeology.pdf.

48 OIG, *DHS Actions Related to I&A Intelligence Product Deviated from Standard Procedures (Redacted)*, DHS, April 26, 2022, 12–13, https://www.oig.dhs.gov/sites/default/files/assets/2022-05/OIG-22-41-Apr22-Redacted.pdf.

49 As with many other concepts related to DHS intelligence, "overt" collection is not well-defined. I&A's guidelines suggest that overt collection must be "openly acknowledged by or readily attributable" to the U.S. government," but the guidelines do not appear to require officers to identify themselves as associated with I&A, DHS, or even the U.S. Intelligence Community. I&A, *Intelligence Oversight Program and Guidelines*, app. B, 6, glossary 4.

50 I&A, *Intelligence Oversight Program and Guidelines*, app. B, glossary 4.

51 Woodruff Swan, "DHS Has a Program Gathering Domestic Intelligence."

52 I&A, *I&A Operations in Portland*, 9.

53 DHS, *FY 2022: Budget in Brief*, May 28, 2021, 17, https://www.dhs.gov/sites/default/files/publications/dhs_bib_-_web_version_-_final_508.pdf (hereinafter DHS, *FY 2022 Budget*). At the same time, one center within I&A claims to have developed a "breakthrough technology" to allow it to "evaluate massive volumes of data," a tool that it reports using "daily." DHS, *FY 2022 Budget*, 18.

54 DHS, *FY 2022 Budget*.

55 OGC, *Administrative Review into I&A Open Source Collection*, 72–73. The Portland police declined the offer.

56 Adam Schiff, chairman of the H. Permanent Select Comm. on Intelligence, to Chad Wolf, acting secretary of homeland security, and Horace Jen, acting undersecretary of I&A, August 3, 2020, https://www.brennancenter.org/sites/default/files/2023-03/20200803_chm_letter_to_murphy_wolf_re_civil_liberties.pdf.

57 I&A, *Intelligence Oversight Program and Guidelines*. Executive Order 12333, the presidential directive establishing and describing the U.S. Intelligence Community, requires agencies such as I&A to conduct intelligence activities affecting U.S. persons — a category that includes American citizens and lawful permanent residents — consistent with procedures approved by the attorney general. Part two of the executive order details the required procedures, which I&A calls its intelligence oversight guidelines. I&A, *Intelligence Oversight Program and Guidelines*, app. B, glossary 5.

58 I&A, *Intelligence Oversight Program and Guidelines*, app. B, 15; and 6 U.S.C. § 121(d)(3)(A) (2018).

59 Steve Vladeck and Benjamin Wittes, "DHS Authorizes Domestic Surveillance to Protect Statues and Monuments," *Lawfare* (blog), July 20, 2020, https://www.lawfareblog.com/dhs-authorizes-domestic-surveillance-protect-statues-and-monuments.

60 Lauren O'Malley, "Top DHS Counterterrorism Official Talks About Pressing Threats," National Counterterrorism, Innovation, Technology, and Education Center, University of Omaha, accessed February 13, 2023, https://www.unomaha.edu/ncite/our-stories/john-cohen-keynote.php (describing I&A monitoring of "narratives"). Similarly, DHS has referred to "narratives known to provoke violence" without explaining what that means. Sam Levin, "U.S. Capitol Attack: Is the Government's Expanded Online Surveillance Effective?," *Guardian*, January 7, 2022, https://www.theguardian.com/us-news/2022/jan/07/us-capitol-attack-government-online-surveillance.

61 DHS, "National Terrorism Advisory System Bulletin," June 7, 2022, https://www.dhs.gov/sites/default/files/ntas/alerts/22_0607_S1_NTAS-Bulletin_508.pdf; and DHS, "National Terrorism Advisory System Bulletin," February 7, 2022, https://www.dhs.gov/sites/default/files/ntas/alerts/22_0207_ntas-bulletin.pdf.

62 For more analysis, see a recent article that situates this work in the broader context of the department's counterterrorism efforts. Faiza Patel and Spencer Reynolds, "Oversight Reports Raise Questions About Value of DHS Counterterrorism Efforts," *Just Security* (blog), August 17, 2022, https://www.justsecurity.org/82635/oversight-reports-raise-questions-about-value-of-dhs-counterterrorism-efforts.

63 I&A, *Intelligence Oversight Program and Guidelines*, app. B, 3. The guidelines also require that officers have a reasonable belief that information intentionally collected about U.S. persons will be permanently retainable.

64 I&A, *Intelligence Oversight Program and Guidelines*, app. B, glossary 5.

65 Vladeck and Wittes, "Statues and Monuments."

66 I&A, *Intelligence Oversight Program and Guidelines*, app. B, glossary 5.

67 Office of the Deputy Chief Management Officer, *DoD Manual 5240.01: Procedures Governing the Conduct of DoD Intelligence Activities*, Department of Defense, August 8, 2016, 53, https://dodsioo.defense.gov/Portals/46/DoDM%20%205240.01.pdf?ver=2016-08-11-184834-887.

68 I&A, *Intelligence Oversight Program and Guidelines*, app. B, 15–16.

69 I&A, *Intelligence Oversight Program and Guidelines*, app. B, 3–4, 10–11, 15–16. Across government agencies of all levels and corporate America, tens of thousands (if not more) potential recipients with one of these functions exist. Requiring the recipients to be able to use the information is again a protection that simply reduces to "furthering a mission"; it presumably would not further a mission to send intelligence to a recipient who cannot use it.

70 I&A defines "United States persons" as citizens, lawful permanent residents, unincorporated associations substantially composed of citizens or lawful permanent residents, and corporations incorporated in the United States, except those under foreign government control. I&A, *Intelligence Oversight Program and Guidelines*, app. B, glossary 5.

71 I&A, *Intelligence Oversight Program and Guidelines*, app. B, 3–4, 10–15.

72 I&A, *Intelligence Oversight Program and Guidelines*, app. B, 15–16.

73 I&A, *Intelligence Oversight Program and Guidelines*, app. B, 6 (§ 2.1.2). The guidelines state that obtaining information by consent is also less intrusive, but it is not clear how DHS interprets the consent requirement or the extent to which the requirement relies on ambiguous indicators to presume consent.

74 I&A, *Intelligence Oversight Program and Guidelines*, app. B, 17 (§ 2.3.5). The requirement also does not apply to information obtained with consent. For some time, I&A had a practice of masking publicly available U.S. persons information. The practice was not part of the legal regime of the guidelines, however, which allowed this safeguard to be discarded during the Trump administration. OGC, *Administrative Review into I&A Open Source Collection*, 25, 41–42, 83.

75 See the description of HSIN's intelligence community of interest, which acts as a dissemination platform for much of I&A's work and is accessible to myriad law enforcement agencies with disparate needs and jurisdictions. DHS, "Homeland Security Information Network — Intelligence (HSIN-Intel) Partner Products," September 18, 2014, https://www.hsdl.org/?view&did=759439.

76 I&A, *Intelligence Oversight Program and Guidelines*, app. B, 2.

77 OGC, *Administrative Review into I&A Open Source Collection*, 24, 81.

78 Kevin McAleenan, acting secretary of homeland security, "Information Regarding First Amendment Protected Activities," memorandum, May 17, 2019, https://www.dhs.gov/sites/default/files/2022-06/info_regarding_first_amendment_protected_activities_as1_signed_05.17.2019-508.pdf.

79 McAleenan, "Information Regarding First Amendment Protected Activities," 2.

80 6 U.S.C. § 101(18)(B) (2018) (intent element of the Homeland Security Act definition of "terrorism" used by the department).

81 McAleenan, "Information Regarding First Amendment Protected Activities," 3.

82 For deficiencies in DHS-wide safeguards against profiling, see Harsha Panduranga and Faiza Patel, *Stronger Rules Against Bias: A Proposal for a New DHS Nondiscrimination Policy*, Brennan Center for Justice, September 9, 2022, 2, https://www.brennancenter.org/our-work/policy-solutions/stronger-rules-against-bias.

83 6 U.S.C. § 124d (2010).

84 6 U.S.C. § 124d (2010).

85 For example, a DHS privacy impact assessment describes how U.S. Immigration and Customs Enforcement (ICE) officers may conduct electronic surveillance. Tracy Cormier and Jordan Holz, *Privacy Impact Assessment for the Homeland Security Investigation (HSI) Surveillance Technologies*, DHS/ICE/PIA-061, DHS Privacy Office, January 24, 2022, 3–5, https://www.dhs.gov/sites/default/files/2022-01/privacy-pia-ice061-hsisuveillancetech-january2022_0.pdf. As have many other agencies, U.S. Customs and Border Protection (CBP) has issued a strategic plan that situates its intelligence functions within its broader work. CBP, *U.S Customs and Border Protection Strategy 2021–2026*, December 17, 2020, https://www.cbp.gov/sites/default/files/assets/documents/2020-Dec/CBP-Strategy-2021-2026.pdf.

86 CBP, "About CBP: Operational Support/Enterprise Services," DHS, last modified January 6, 2023, https://www.cbp.gov/about/congressional-resources/operational-supportenterprise-services; and *Department of Homeland Security Intelligence and Border Security: Delivering Operational Intelligence, Hearing Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment, H. Comm. on Homeland Security*, 109th Cong. (2006), https://www.govinfo.gov/content/pkg/CHRG-109hhrg34854/html/CHRG-109hhrg34854.htm.

87 6 U.S.C. § 211(h) (2016).

88 6 U.S.C. § 211(h)(3)(E) (2016).

89 CBP, "About CBP," DHS, last modified March 8, 2023, https://www.cbp.gov/about; and 6 U.S.C. § 211(c) (2018).

90 8 C.F.R. § 287.1 (homeland security regulation implementing the statute and taking expansive view of border zone without justification). This view has been vigorously challenged. ACLU, "Customs and Border Protection's (CBP's) 100-Mile Rule," accessed February 13, 2023, https://www.aclu.org/sites/default/files/field_document/14_9_15_cbp_100-mile_rule_final.pdf (discussing history of interpretation, lack of public justification, and harms).

91 Nick Miroff, "Powered by Artificial Intelligence, 'Autonomous' Border Towers Test Democrats' Support for Surveillance Technology," *Washington Post*, March 11, 2022, https://www.washingtonpost.com/national-security/2022/03/11/mexico-border-surveillance-towers; Peter Aldhous "How Buzzfeed News Revealed Hidden Spy Planes in US Airspace," *Columbia Journalism Review*, August 7, 2017, https://www.cjr.org/watchdog/how-buzzfeed-news-revealed-hidden-spy-planes-in-us-airspace.php; and Laurence Castelli, Douglas Harrison, and Sonia Padilla, *Privacy Impact Assessment for the Border Surveillance System (BSS)*, DHS/CBP/PIA-022, DHS Privacy Office, August 29, 2014, https://www.dhs.gov/sites/default/files/publications/privacy_pia_CBP_BSS_August2014.pdf.

92 We do know that this information ends up in DHS's vast databases. For example, it is included in CBP's Analytical Framework for Intelligence (AFI), which combines information from various sources (e.g., immigration, travel, border crossing, and social media) to reveal highly personal information. AFI's integrated analytical tools rely on this information to inform a number of decisions, including determining admissibility. Mario Medina and Debra L. Danisek, *Privacy Impact Assessment for the Analytical Framework for Intelligence (AFI)*, DHS/CBP/PIA-010(a), DHS Privacy Office, 3–4, https://www.dhs.gov/sites/default/files/2022-10/privacy-pia-cbp010%28a%29-afi-october2022.pdf. CBP also operates data and network analysis programs within the National Targeting Center that draw on various sources of information and intelligence to drive operations and policymaking. GAO, "CBP Aims to Prevent High-Risk Travelers from Boarding U.S.-Bound Flights, but Needs to Evaluate Program Performance," January 24, 2017, https://www.gao.gov/assets/gao-17-216-highlights.pdf.

93 Will Parrish, "The U.S. Border Patrol and an Israeli Military Contractor Are Putting a Native American Reservation Under 'Persistent Surveillance,'" *Intercept*, August 15, 2019, https://theintercept.com/2019/08/25/border-patrol-israel-elbit-surveillance.

94 Tom Jones, Mari Payton, and Bill Feather, "Source: Leaked Documents Show the U.S. Government Tracking Journalists and Immigration Advocates Through a Secret Database," NBC 7 San Diego, March 6, 2019, https://www.nbcsandiego.com/news/local/source-leaked-documents-show-the-us-government-tracking-journalists-and-advocates-through-a-secret-database/3438.

95 Ryan Devereaux, "Faith Under Fire," *Intercept*, March 6, 2022, https://theintercept.com/2022/03/06/cbp-border-surveillance-migrant-caravan.

96 Kris Holt, "CBP Flew a Predator Drone over Minneapolis amid George Floyd Protests," *Forbes*, May 29, 2020, https://www.forbes.com/sites/krisholt/2020/05/29/cbp-predator-drone-minneapolis-george-floyd-aclu/?sh=10b6087d40fa.

97 Yessenia Funes and Dhruv Mehrotra, "CBP Drones Conducted Flyovers Near Homes of Indigenous Pipeline Activists, Flight Records Show," *Gizmodo*, September 18, 2020, https://gizmodo.com/cbp-drones-conducted-flyovers-near-homes-of-indigenous-1845104576.

98 Jana Winter, "CBP Unit That Spied on Journalists and Lawmakers Is Monitoring American Protesters," Yahoo News, January 26, 2022, https://news.yahoo.com/cbp-unit-that-spied-on-journalists-and-lawmakers-is-monitoring-american-protestors-100039195.html.

99 Winter, "CBP Unit That Spied"; Jana Winter, "CBP Launches Review of Secretive Division That Targeted Journalists, Lawmakers and Other Americans," Yahoo News, December 31, 2021, https://news.yahoo.com/cbp-launches-review-secretive-division-that-targeted-journalists-lawmakers-americans-100035634.html; and Jana Winter, "Operation Whistle Pig: Inside the Secret CBP Unit with No Rules That Investigates Americans," Yahoo News, December 11, 2021, https://news.yahoo.com/operation-whistle-pig-inside-the-secret-cbp-unit-with-no-rules-that-investigates-americans-100000147.html.

100 Rambo worked for the Counter Network Division, which sits within CBP's National Targeting Center, an entity that monitors travelers and cargo to find what it calls "global threats." Paul Koscak, "Working Together: Catching Smugglers, Terrorists, and Lawbreakers Works Better Through Partnership," CBP, last modified January 4, 2022, https://www.cbp.gov/frontline/cbp-national-targeting-center; and R. Gil Kerlikowske, "Written Testimony of CBP Commissioner R. Gil Kerlikowske for a House Committee on Appropriations, Subcommittee on Homeland Security Hearing on the U.S. Customs and Border Protection's FY 2017 Budget Request," DHS, March 1, 2016, https://www.dhs.gov/news/2016/03/01/written-testimony-cbp-commissioner-house-appropriations-subcommittee-homeland.

101 Winter, "Operation Whistle Pig."

102 Michael M. Grynbaum, "New York Times Reassigns Reporter in Leak Case," *New York Times*, July 3, 2018, https://www.nytimes.com/2018/07/03/business/media/ali-watkins-times-reporter-memo.html; District of Columbia U.S. Attorney's Office, "Former U.S. Senate Employee Sentenced to Prison Term on False Statements Charge," Department of Justice, December 20, 2018, https://www.justice.gov/usao-dc/pr/former-us-senate-employee-sentenced-prison-term-false-statements-charge; and Winter, "Operation Whistle Pig."

103 ICE, "Fact Sheets," DHS, last modified February 1, 2021, https://www.ice.gov/factsheets. HSI's operations are the subject of a forthcoming report by the Brennan Center.

104 Nina Wang et al., *American Dragnet: Data-Driven Deportation in the 21st Century*, Georgetown Law Center on Privacy and Technology,

May 10, 2022, 2–3, 68, https://www.americandragnet.org/sites/default/files/American_Dragnet_report_English_final.pdf.

105 Immigration and Customs Enforcement, *Unaccompanied Alien Children Human Smuggling Disruption Initiative: Concept of Operations*, DHS, May 5, 2017, https://www.documentcloud.org/documents/5980596-Smuggling-Initiative-ConOP.html. Mijente, "Palantir Played Key Role in Arresting Families for Deportation, Document Shows," May 2, 2019, https://mijente.net/2019/05/palantir-arresting-families.

106 José Olivares and John Washington, "ICE Discussed Punishing Immigrant Advocates for Peaceful Protests," *Intercept*, June 17, 2021, https://theintercept.com/2021/06/17/ice-retaliate-immigrant-advocates-surveillance.

107 Jimmy Tobias, "ICE Has Kept Tabs on 'Anti-Trump' Protesters in New York City," *Nation*, March 6, 2019, https://www.thenation.com/article/archive/ice-immigration-protest-spreadsheet-tracking.

108 Mike Ludwig, "ICE Is Monitoring and Targeting Immigration Activists," *Truthout*, April 30, 2019, https://truthout.org/articles/ice-is-monitoring-and-targeting-immigration-activists.

109 6 U.S.C. § 321d(a) (2018).

110 DHS, "DHS Component Actions Report for Civil Disturbances — Multiple Cities," documents obtained by Freedom of Information Act by Citizens for Responsibility and Ethics in Washington (CREW), June 4, 2020, 7–8, 10, 14, 16–85, https://www.citizensforethics.org/wp-content/uploads/2022/01/2021.08.13-Responsive-Records-2021-HQLI-00009-20-cv-02553-TJK.pdf (DHS National Operations Center and I&A reporting); and Andrew Selsky, "New Report Shows Department of Homeland Security Gathered Intel on Portland Black Lives Matter Protesters," Associated Press, October 28, 2022, https://www.pbs.org/newshour/nation/new-report-shows-department-of-homeland-security-gathered-intel-on-portland-black-lives-matter-protestors. This overreach is not confined to the Trump administration. In 2015, the NOC issued reports about music and community parades in two historically black DC neighborhoods and at a walk to end breast cancer. Ben Mathis-Lilley, "Feds Monitored Breast Cancer Walk to Make Sure Black Lives Matter Riot Didn't Break Out," *Slate*, July 24, 2015, https://slate.com/news-and-politics/2015/07/black-lives-matter-surveillance-department-of-homeland-security-seems-relatively-benign-also-pointless.html.

111 Betsy Woodruff Swan and Lara Seligman, "'No Major Incidents of Illegal Activity': DHS Told Pentagon as Pro-Trump Mob Breached the Capitol," *Politico*, September 28, 2021, https://www.politico.com/news/2021/09/28/dhs-pentagon-jan-6-capitol-riot-514527.

112 Eric M. Leckey, *Privacy Impact Assessment for the FEMA Operational Use of Social Media for Situational Awareness*, DHS/FEMA/PIA-041, DHS Privacy Office, March 10, 2016, 22–24, https://www.dhs.gov/sites/default/files/publications/privacy-pia-FEMA-OUSM-April2016.pdf.

113 Federal Emergency Management Agency, "FEMA Regions I, II and III: Scheduled Protest for April 30–May 3," DHS, 2015, 1, https://www.documentcloud.org/documents/2178937-4-2015-4-30-5-3-fema-protest-report-includes.html; and George Joseph, "Feds Regularly Monitored Black Lives Matter Since Ferguson," *Intercept*, July 24, 2015, https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson.

114 I&A, *Intelligence Oversight Program and Guidelines*, 3.

115 Patel, Levinson-Waldman, and Panduranga, *Course Correction for Homeland Security*. The Homeland Security Act charges CRCL with "oversee[ing] compliance with constitutional, statutory, regulatory, policy, and other requirements relating to the civil rights and civil liberties of individuals affected by the programs and activities of the Department." Homeland Security Act of 2002, Pub. L. No. 107–296, §§ 103, 705, 116 Stat. 2144, 2219 (codified as amended at 6 U.S.C. §§ 113, 345 (2004)). The chief privacy offer, who is appointed by the secretary of homeland security, is charged with "assuring that the use of technologies sustain [*sic*], and do not erode, privacy protections relating to . . . personal information," and has the power to undertake "investigations and reports relating to the administration of the programs and operations of the Department." 6 U.S.C. § 142 (2007). This section focuses primarily on CRCL because it is mandated to protect the rights of Americans whose political activities and associations, journalistic speech, and religious practices are too often the subject of I&A surveillance. The Privacy Office, in contrast, typically works to ensure that data relating to Americans is properly handled in keeping with privacy law and policy, which is less directly implicated by DHS intelligence reporting and analysis of the type we discuss in this paper.

116 See Benjamin Wittes, "How the DHS Intelligence Unit Sidelined the Watchdogs," *Lawfare* (blog), August 6, 2020, https://www.lawfareblog.com/how-dhs-intelligence-unit-sidelined-watchdogs; OGC, *Administrative Review into I&A Open Source Collection*, 38, 40, 68, 79; Patel, Levinson-Waldman, and Panduranga, *Course Correction for Homeland Security*, 17–21; and OIG, *I&A Needs to Improve Its Open Source Intelligence Reporting*, 12–13. And in investigating interference in intelligence by senior DHS leadership, the inspector general assessed the process for oversight office review of I&A intelligence products and found it deficient to protect against abuses. OIG, *DHS Actions Related to I&A Intelligence Product*, 3–6.

117 Patel, Levinson-Waldman, and Panduranga, *Course Correction for Homeland Security*, 17–18.

118 OIG, *I&A Needs to Improve Its Open Source Intelligence Reporting*, 13.

119 Stephanie Dobitsch (deputy undersecretary for intelligence enterprise operations, DHS), conversation with Brennan Center, February 1, 2023. See also Patel, Levinson-Waldman, and Panduranga, *Course Correction for Homeland Security*, 18.

120 Patel, Levinson-Waldman, and Panduranga, *Course Correction for Homeland Security*, 20–21.

121 DHS, "Privacy Office Contacts," last modified August 1, 2022, https://www.dhs.gov/privacy-office-contacts (component privacy offices).

122 DHS, "Office of the General Counsel," last modified September 2, 2022, https://www.dhs.gov/office-general-counsel.

123 OGC, *Administrative Review into I&A Open Source Collection*, 40–41.

124 OGC, *Administrative Review into I&A Open Source Collection*, 38, 40–41, 67–68.

125 DHS, "Office of the General Counsel."

126 I&A, *Intelligence Oversight Program and Guidelines*, 3.

127 OIG, *I&A Needs to Improve Its Open Source Intelligence Reporting*, 10.

128 I&A, "I&A Organizational Alignment," DHS, accessed February 13, 2023, https://www.dhs.gov/sites/default/files/publications/18_0817_ia_organizational-chart.pdf (the Intelligence Oversight Office is referred to as "Privacy and Intelligence Oversight," which the chart indicates reports to the undersecretary and a deputy undersecretary for I&A).

129 OGC, *Administrative Review into I&A Open Source Collection*, 40.

130 Minimization of information about U.S. persons (USPI, or U.S. persons information) must fully account for the ability of recipients of the intelligence to infer from the content and context of the information in the report and minimize information beyond merely a name to ensure that the report has been effectively anonymized. For example, if a social media handle is minimized but the recipient can simply conduct an internet search of a reported social media post and find the username or legal name of a poster, the USPI has not been properly minimized.

131 FBI, *FBI Domestic Investigation and Operations Guide*, app. L, 16, https://www.brennancenter.org/sites/default/files/2022-12/2016%20DIOG%20Excerpt.pdf.

132 6 U.S.C. § 452 (2004). See also Stephen R. Vina, *Homeland Security: Scope of the Secretary's Reorganization Authority*, Congressional Research Service, August 9, 2005, https://sgp.fas.org/crs/homesec/RS21450.pdf; and Gary Kepplinger, general counsel, GAO, to Sen. Robert Byrd and Sen. Thad Cochran, "Department of Homeland Security — Transfer of Support Function for Principal Federal Officials," July 31, 2008, 3, https://www.gao.gov/assets/b-316533.pdf.

133 The DHS Insider Threat Program (ITP) offers a loose model for this type of access. It scrutinizes the DHS workforce for potential threats to its missions and security, including through an extensive "user activity monitoring" program. If a DHS employee uses one of the "trigger" indicators identified by ITP on a computer system, it is recorded and sent to ITP for evaluation to determine whether the employee poses any threat to internal security. The Oversight Office could deploy a similar user activity monitoring approach on DHS intelligence collections systems. Alternatively, the program could work with the chief information officer to gain access to these collection systems in order to review the access and collection in real time. We recommend exploring both models and adopting the one that allows the office the most thorough, timely view of DHS intelligence work. Richard D. McComb, *Privacy Impact Assessment Update for the Insider Threat Program*, DHS/ALL/PIA-052(b), DHS Privacy Office, June 16, 2020, 1, https://www.dhs.gov/sites/default/files/publications/privacy-pia-all-insiderthreatprogram-june2020.pdf.

ABOUT THE AUTHORS

▶ **Spencer Reynolds** is counsel in the Brennan Center's Liberty and National Security Program. Previously, he was senior intelligence counsel in the Office of the General Counsel of the U.S. Department of Homeland Security. At DHS, Reynolds advised on operations and policy related to domestic intelligence, counterterrorism, social media monitoring, and other national security matters.

▶ **Faiza Patel** is a nationally recognized expert on counterterrorism and government surveillance. As senior director of the Brennan Center's Liberty and National Security Program, she has published research on National Security Agency surveillance, social media monitoring, countering violent extremism, and targeting of Muslim communities. Patel has testified before the Senate and House of Representatives on homeland security surveillance. Her writing has been featured in major publications such as the *New York Times*, the *Washington Post*, and the *Los Angeles Times*. She is also a regular contributor to the legal blog *Just Security*, for which she is a member of the board of editors. Previously, she worked as a senior policy officer at the Organisation for the Prohibition of Chemical Weapons in The Hague and served as a law clerk at the International Criminal Tribunal for the former Yugoslavia.

ACKNOWLEDGMENTS

The Brennan Center gratefully acknowledges the Bauman Foundation, CS Fund/Warsh-Mott Legacy, and Media Democracy Fund for their generous support of our work. This is an independent Brennan Center publication; the opinions expressed are those of the authors and do not necessarily reflect the views of our supporters.

The authors express their gratitude for the time and insight of senior officials at the DHS Office of Intelligence and Analysis, namely the undersecretary for intelligence and analysis, deputy undersecretary for intelligence enterprise operations, director of the Current and Emerging Threats Center, and chief of staff. We also thank several government intelligence experts for their sharp, insightful review of drafts of this report.

We are grateful to Rachel Levinson-Waldman for her thoughtful contributions to numerous discussions; Sophie Gillard, José Gutiérrez, and Alia Shahzad for invaluable research and cite-checking; and Marisa Lowe for early research assistance. We also thank Michael German, John Kowal, and Michael Waldman for their support and guidance, and Marcelo Agudo, Julian Brookes, Zachary Laub, Janet Romero-Bahari, and Alden Wallace for their editing and communications assistance.

Finally, we express deep gratitude to those government employees who have taken personal risk to disclose to Congress, investigators, and the media the excesses of some Department of Homeland Security programs. These disclosures — and dogged coverage by journalists of these important stories — have made it possible to write about otherwise opaque topics.

ABOUT THE BRENNAN CENTER'S LIBERTY AND NATIONAL SECURITY PROGRAM

The Brennan Center's Liberty and National Security Program works to advance effective national security policies that respect constitutional values and the rule of law, using research, innovative policy recommendations, litigation, and public advocacy. The program focuses on reining in excessive government secrecy, ensuring that counterterrorism authorities are narrowly targeted to the terrorist threat, and securing adequate oversight and accountability mechanisms.

BRENNAN CENTER FOR JUSTICE

Brennan Center for Justice at New York University School of Law
120 Broadway // 17th Floor // New York, NY 10271
www.brennancenter.org