BRENNAN CENTER FOR JUSTICE

DHS AT 20: AN AGENDA FOR REFORM

Ending Fusion Center Abuses

A Roadmap for Robust Federal Oversight

By Michael German, Rachel Levinson-Waldman, and Kaylana Mueller-Hsia

PUBLISHED DECEMBER 15, 2022

For almost two decades, the Department of Homeland Security (DHS) has supported the development of a national network of 80 fusion centers. Operated by states and localities, fusion centers incorporate federal, state, and local law enforcement personnel, first responders, and select private-sector representatives to collect, analyze, and distribute intelligence. While the federal government initially promoted them as hubs for sharing counterterrorism information, fusion centers quickly expanded their missions to include any crimes or hazards.

DHS provides these centers with funding, personnel, and access to federal intelligence, but it has failed to ensure that they have used these resources appropriately. As a result, fusion centers have long produced flawed analysis, abused their authorities to monitor people engaged in First Amendment–protected activities, and leaked sensitive law enforcement information. This domestic intelligence model has undermined Americans' privacy, civil rights, and civil liberties.

Fusion centers have repeatedly targeted minority communities and protest movements under the guise of counterterrorism or public safety. In their early years, they often singled out American Muslims for unwarranted scrutiny. Their bulletins have regularly painted racial and environmental justice activists as menacing threats. Fusion center reports are widely disseminated to local police and federal law enforcement, likely contributing to their heavy-handed responses to these protests in recent years. The participation of private companies, including some that have been the subjects of protests, in fusion centers raises the possibility that these operations sometimes serve private interests rather than public safety.

Fusion centers continue to be susceptible to abuse as protest movements react to events, creating new targets for unwarranted scrutiny. For example, fusion centers have amplified FBI and DHS threat warnings that falsely lump pro-choice activists together with abortion foes as potential "abortion-related violent extremists," even though only anti-abortion militants have a history of engaging in deadly violence.[1] As states criminalize abortion, investigations of those seeking, providing, or even just supporting access to reproductive services will fit within fusion centers' "all crimes" remit,[2] making it likely that fusion centers will heed law enforcement requests for assistance.

At the same time, there is little to suggest that fusion centers have provided meaningful assistance to federal counterterrorism efforts. And even as they have broadened their missions beyond counterterrorism, there is no evidence that they have contributed substantially to reducing or solving serious crime. They do, however, facilitate broad, unregulated information sharing among a variety of public and private entities with little oversight or public accountability, which poses a serious security liability that was realized when hackers breached a fusion center contractor in 2020, exposing hundreds of thousands of sensitive records from the FBI, DHS, and other law enforcement agencies.

As the 20th anniversary of the creation of DHS approaches, the Brennan Center has undertaken a comprehensive review of the department's efforts to carry out its primary mission of keeping the country safe from terrorism. Our April 2022 report, *A Course Correction for Homeland Security: Curbing Counterterrorism Abuses*, identified structural and operational problems endemic to DHS-sponsored fusion centers.[3] This report expands on these critiques and proposes solutions through the lens of federal funding, support, and oversight. While fusion centers are run by state or local agencies, they continue to receive significant federal investments. The federal government has an obligation to guard against the misuse of the resources, systems, and personnel it provides, and to ensure that Americans' constitutional rights are not infringed upon by the improper collection, retention, and dissemination of personally identifiable information of persons not reasonably suspected of criminal activity.

Accordingly, the secretary of homeland security should take immediate action to ensure that DHS grants to fusion centers are transparent and used for their intended counterterrorism purpose. The secretary should also require regular audits of fusion centers to ensure that data is protected against unauthorized disclosure, and that DHS resources are not used in violation of constitutional rights. Congress should establish a special inspector general to audit the national network of fusion centers to detect waste, fraud, abuse, and illegality, and should use the results of this audit to establish a permanent, independent federal oversight body to ensure that future violations of any laws, regulations, or policies are discovered and remedied in a timely manner. These reforms will help to ensure that fusion centers' capabilities and resources are not abused, and that Americans' rights to freedom of speech and association are preserved.

Mission Versus Reality

No single piece of legislation established the national network of fusion centers, defined its mission, or authorized it to operate as a decentralized domestic intelligence collection mechanism feeding the federal intelligence community with information gathered from every American neighborhood. The network operates in secret, without a clear charter, and under ambiguous lines of authority. It includes not only federal, state, and local law enforcement, but also other public and private entities that have no authority to collect or disseminate intelligence about Americans. The public has little access to information regarding what their local fusion centers do in their communities or even who works there. No federal entity accepts responsibility for overseeing them, leaving the network essentially ungoverned.

Expanding Missions

The federal government supported the development of the national network as a means for sharing counterterrorism information between federal law enforcement, military, and intelligence agencies; state and local law enforcement and emergency response services; and select private-sector entities. Most fusion centers were established in the decade following the 9/11 terrorist attacks on the theory that gathering information from a multitude of sources and sharing it broadly would help law enforcement and intelligence agencies predict and prevent terrorist attacks.[4]

Operated mainly by state and local governments, fusion centers receive substantial support from the federal government in the form of DHS and Department of Justice (DOJ) grant funding, access to federal counterterrorism and military intelligence data systems, and personnel deployed from DHS and the FBI.[5] They are staffed primarily by state and local law enforcement, but also include representatives from emergency management and public health agencies, the National Guard, and locally chosen private-sector participants and contractors.[6] DHS began serving as the primary federal liaison to fusion centers in 2007.[7]

To encourage greater participation by entities that did not feel their local terrorism threat justified their involvement, fusion centers quickly expanded the purposes of their intelligence collection activities, first to "all crimes" and then, as they recruited more non–law enforcement agencies and private-sector participants, to "all hazards."[8] This shift is reflected in their mission statements, which often make no mention of terrorism but instead are expansive enough to encompass nearly any activity the fusion center chooses to undertake.[9] Such a broad remit makes it difficult for fusion centers to develop reliable metrics to measure their effectiveness and all but impossible for overseers to determine whether a fusion center's actions are necessary or appropriate.

The funding model has changed as well. Initially developed with federal dollars, fusion centers are now mainly supported through state and local budgets. According to the most recent data published by DHS, in 2017, fusion centers received about a third of their funding from federal grants.[10] Federal auditors have complained, however, that

the way DHS and DOJ grants are distributed to law enforcement makes it difficult to determine how much federal funding fusion centers actually receive and how they use it.[11]

There is also no publicly available information detailing how fusion centers allocate their spending between counterterrorism, general crimes, and hazards. In a 2017 DHS survey, 94 percent of fusion centers said that counterterrorism was among their top five priorities, with general crime, narcotics, cybersecurity, and critical infrastructure rounding out the list.[12] According to that same report, however, only 16 percent of fusion center analysts are counterterrorism specialists, which suggests that counterterrorism is a relatively smaller part of their work.[13]

Cracking Down on Dissent

The blurry boundaries and shifting contours of their missions have given fusion centers ample room to abuse their authorities. Over the last two decades, leaked materials have shown fusion centers tracking protestors and casting peaceful activities as potential threats. Their targets have included racial justice and environmental advocates, right-wing activists, and third-party political candidates.[14]

In 2020, fusion centers regularly tracked the overwhelmingly nonviolent racial justice protests organized across the country in response to the police killings of George Floyd and Breonna Taylor. Though violence and property damage did occur amid some protests, fusion centers issued bulletins that were poorly sourced, sensationalized, and unable to point to specific threat information. These bulletins — often citing rumors or disinformation spread by anonymous social media posters or right-wing media sites — rarely identified individuals suspected of specific criminal activities. Rather, they routinely insinuated that the protestors were collectively responsible for any crimes committed during demonstrations and broadly labeled them as anarchists or "antifa" (shorthand for anti-fascists), echoing language that President Donald Trump used to demonize protesters.[15] Press reports and leaked documents reveal how fusion centers around the country hyped the threat posed by protesters:

- The Minnesota fusion center "fed a constant stream of unverified and ultimately bogus threats to officers" during the unrest in Minneapolis, according to the *Minnesota Reformer*, "while failing to identify more credible risks." For example, the center modified information from an FBI report documenting a source's warning of a possible "Antifa" car bomb attack against the National Guard, removing language reflecting the analyst's skepticism regarding its credibility and painting the threat as definitive rather than speculative.[16] No such attack took place.

- The Northern California fusion center issued multiple warnings about Black Lives Matter rallies in the region. The bulletins, which were sent to some 14,000 police officers, did not include any specific threat information, but nevertheless painted the rallies as dangerous, stating that "[s]ome of these events involve criminal activities such as planned looting, vandalism and threats of violence."[17]

- The Austin, Texas, fusion center combed social media for announcements of events hosted by Black Lives Matter organizers, creating intelligence reports about events as innocuous as a Juneteenth celebration, a meditation circle, and candlelight vigils for victims of police violence. It shared these reports with local, state, and federal law enforcement agencies, as well as with the Central Intelligence Agency and Immigration and Customs Enforcement.[18]

- The Maine fusion center tracked racial justice protests and disseminated online conspiracy theories and disinformation exaggerating the potential for violence at demonstrations.[19] For example, the center sent out alerts from DHS and the FBI in June 2020 warning police departments that piles of bricks were being placed around the country, which the source for the report claimed was a "tactic . . . used by Antifa to fuel violent opportunists."[20] The source was a far-right social media account that disseminated pro-Trump conspiracy theories.[21] In another alert, the fusion center warned that a TikTok video posted by a teenager, consisting entirely of other people's tweets, provided "tactics, techniques and procedures on how to interfere with the US National Guard during riots."[22]

- The national fusion center network distributed false threat warnings regarding "antifa arsonists" starting wildfires in the western United States and "anarchist extremists" planning an "International Sabotage Day."[23] These warnings proliferated through the network despite some internal efforts to debunk them, misdirecting scarce law enforcement and emergency response resources during natural disasters.[24]

Environmental advocacy groups, such as those seeking to block the construction of pipelines over Native American lands, are often the targets of fusion center scrutiny as well. According to a lawsuit filed by activists and organizers in Oregon, the state's fusion center has, "for years, engaged in and facilitated the surveillance of environmental advocacy groups, community organizations, and Native American tribes opposing the proposed $10 billion fossil fuel pipeline and export terminal known as Jordan Cove LNG."[25] In emails obtained by the *Guardian* in 2019, the local sheriff's office reported tracking attendance at a rally for the fusion center "as promised," despite a "lack of criminal nexus."[26] Fusion center analysts also submitted

reports on environmental advocates and local business owners who interrupted a 2018 chamber of commerce meeting to censure the chamber for accepting donations from an oil company.[27]

The North Dakota fusion center played a similar role in collecting and disseminating intelligence about protestors challenging the construction of the Dakota Access Pipeline in 2016. The center issued threat assessments based on information compiled from state and local police and social media, flagging citizen journalism organizations and advocates for Native American communities as "groups of interest."[28] The overwhelming majority of information described nonviolent demonstrations with no link to criminal activity.

Early signs suggest that fusion centers and law enforcement may similarly overreact to pro-choice protestors as they mobilize on the streets and on social media in the wake of the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*.[35] A Virginia fusion center report, for instance, observed that "groups from both sides of the issue" were organizing protests following the May 2022 leak of the draft *Dobbs* opinion and warned that "some may become violent," without clarifying that anti-abortion extremists have committed the vast majority of abortion-related violence.[36] Fusion center publications touting a speculative threat from pro-choice activists run the risk of magnifying a law enforcement response by agents already poised to provoke violence against protesters. After the *Dobbs* decision leaked, for example, DHS Federal Protective Service officers in Los Angeles instigated a hostile confrontation with protesters at an orderly reproductive rights demonstration blocks away from the federal courthouse where they have jurisdiction.[37]

Moreover, police in states that criminalize abortion are likely to leverage their fusion centers' access to a broad array of data, including federal counterterrorism systems, to gather evidence and intelligence necessary to enforce these anti-abortion laws. Since fusion centers operate in a national network, personnel in states where abortion remains legal may be tasked with assisting out-of-state criminal investigations seeking to develop evidence for abortion-related prosecutions.[38]

Fusion centers are not alone in targeting protestors and minority communities. The FBI, DHS, and police departments have done the same. But fusion centers facilitate and amplify this abuse because, as detailed in the next section, they are designed to enable the unfettered collection and broad dissemination of information about the activities of Americans who are not suspected of any criminal activity.

Private Priorities

>> **Fusion center** monitoring of environmental protests demonstrates the risks of private-sector participation in these ventures. In theory, private partners could provide useful counterterrorism information to the government or use information provided by the government to mitigate threats. In practice, their participation can distort fusion centers' public safety mission in service of corporate interests. According to the Oregon environmental activists' lawsuit, the state fusion center "facilitated the creation of, and worked closely alongside, a taskforce that included a dedicated unit" within the sheriff's office that was "funded entirely by Pembina, the private fossil fuel company" that was seeking to build the pipeline.[29] The Oregon fusion center also "cooperated and coordinated" with "a private public relations firm retained by Pembina to monitor opposition to the project and turn public sentiment against the organizations and individuals opposing [the pipeline]."[30]

Similarly, the law enforcement response to the 2016 Dakota Access Pipeline protests — which was marked by excessive, indiscriminate police violence and mass arrests — was coordinated through a task force that included not only the North Dakota fusion center and federal, state, and local law enforcement agencies but also TigerSwan, an unlicensed private security contractor with experience in Iraq and Afghanistan that was working for the pipeline company.[31] TigerSwan operatives infiltrated protest groups and developed detailed dossiers on individual protestors.[32] It shared sensationalized threat reports with law enforcement, labeling the pipeline protests an "insurgency" that needed to be defeated, and often highlighted the presence of Palestinian Americans and other "Islamic individuals" in the protestors' camp to suggest that Middle Eastern terrorist groups may have been working with the protesters.[33]

These are not isolated events. Fusion centers in Oklahoma, Texas, and Nebraska have had similar intelligence-sharing arrangements with fossil fuel companies focused on monitoring and subverting environmental activists' protest activities.[34]

Data Systems Ripe for Exploitation

Fusion center personnel have access to vast government and private-sector data systems and information-sharing platforms. How they use these systems is shielded from public view. Fusion center proponents at DHS and DOJ diluted or subverted long-standing restraints on law enforcement intelligence collection as part of their efforts to establish fusion centers as local intelligence hubs and combine them into a national network. The effect was to create an enormous and unaccountable domestic intelligence enterprise that now operates in every U.S. community, threatening Americans' privacy and fundamental freedoms without justification, proper legal process, or independent oversight.

Access to Expansive Information Sources

Fusion center personnel have access to massive amounts of data about the activities of ordinary Americans not suspected of criminal activities. In addition to the information systems and databases owned and controlled by their home agencies, fusion center participants can also access information from a range of other government and private data systems, whether directly through subscriptions with data brokers or as a function of sitting next to a colleague with access. While some of this information might be useful for criminal investigations, it can all too easily be abused.[39]

Neither DHS nor the fusion center network publicly discloses all the data systems that fusion center personnel have access to, but a review of some of the most prominent ones gives a sense of the scope of information available to fusion centers:

- The Homeland Security Information Network (HSIN) was established by DHS to facilitate information sharing among a multitude of government agencies and private partners involved in "identifying and preventing terrorism" and "incident management activities," from terrorist attacks to natural disasters.[40] According to its 2020 annual report, nearly 150,000 people are registered to use HSIN.[41] There are virtually no limits on the types of information that can be disseminated through HSIN, which may include personally identifiable information.[42] Law enforcement, emergency management agencies, and the National Guard used HSIN to monitor the summer 2020 protests against police violence in the Washington, DC, area, for instance, while the Oklahoma fusion center leveraged the system "for real-time situational awareness and information sharing" in response to "civil unrest and protests" that same year.[43]

- Law Enforcement Online (LEO) is managed by the FBI to provide a secure means to communicate and share unclassified (though potentially sensitive) information.[44] Users can upload all types of personally identifiable information, including financial data and medical histories, as well as individuals' "photos, all types of physical characteristics, and activities."[45] As of 2012, the service had almost 60,000 active users from criminal justice agencies, the intelligence community, the military, agencies charged with protecting critical infrastructure, and select private-sector representatives.[46]

- The National Data Exchange (N-DEx), also managed by the FBI, is an online investigative information-sharing system with more than 90,000 registered users from criminal justice agencies at all levels of government as well some private security agencies, such as railroad and campus police.[47] As of 2015, N-DEx reportedly held over 180 million records relating to 1 billion people, places, and events.[48] In addition to information about people convicted or suspected of crimes, the database contains information about witnesses and "anyone else who may be identified in criminal justice information."[49]

- The Regional Intelligence Sharing Systems (RISS) program is a DOJ-funded "family" of six regional intelligence systems that are meant to support law enforcement efforts against all types of crimes.[50] Its 157,000 authorized users are from law enforcement and criminal justice agencies. The system provides intelligence analysis, digital forensics, and audio/video enhancement and allows access to specialized investigative databases.[51]

- The Law Enforcement Information Exchange (LInX), created by the U.S. Navy's civilian law enforcement component, the Naval Criminal Investigative Service, is used by some 2,000 law enforcement agencies.[52] In addition to criminal incident data such as arrests and outstanding warrants, LInX includes noncriminal information, such as data from field interviews, traffic stops, parking tickets, and automated license plate readers.[53] As of 2015, this data warehouse reportedly contained over 570 million event records.[54]

RISS, N-DEx, and LInX operate under a federal regulation — discussed in further detail below — that prohibits criminal intelligence systems from collecting, maintaining, or disseminating intelligence about individuals unless there is "reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity."[55] The regulation restricts access to information for official law enforcement purposes and requires users to seek permission from the providing agency before using any data in an affidavit or criminal proceeding.

Select fusion center personnel with federal security clearances also have access to classified systems, such as the Defense Department's Secure Internet Protocol Router Network (SIPRNet).[56] This system, which operates as the military's classified internet, was the source of the 725,000 documents that were leaked by former U.S. Army intelligence analyst Chelsea Manning.[57] DHS has also developed its own classified system, the Homeland Security Data Network (HSDN). Documentation suggests that as of 2014, access to HSDN was extended to fusion centers.[58]

The multiplicity of data-sharing platforms inevitably leads to redundancy, contributing to information overload that overwhelms intelligence analysis and impairs effective threat response.[59] For instance, information from an FBI bulletin shared through LEO could also be shared through RISS, and later disseminated over HSIN in a fusion center report or included in an investigative report documented in N-DEx.

With so many interrelated platforms, erroneous, irrelevant, or misleading information shared by one user can be accessed by thousands of others, with no opportunity or ability to prevent the flawed intelligence from spreading through these overlapping systems. Some fusion center leaders have disavowed any responsibility for evaluating the veracity of information they disseminate, with one stating, "[i]f we set as a threshold that we are going to independently verify every piece of information that goes out, then we would be sharing almost no information."[60]

The restrictions on access or use of data in some of these systems (e.g., law enforcement–restricted data in RISS, LInX, and N-DEx, or classified information in SIPRNet) can too easily be circumvented, and the fusion center architecture makes the spillage of restricted or classified data to unauthorized persons for improper purposes more likely.[61] By placing law enforcement officials alongside non–law enforcement personnel and security clearance holders alongside uncleared partners, and tasking them with a common mission, fusion centers break down the traditional arm's-length relationships between these entities and undermine the legal processes designed to protect Americans' privacy rights. Without independent oversight of how fusion centers use the data they retrieve from these systems, abuses are likely to go undiscovered. Internal audits of any one platform are unlikely to detect all the ways that fusion centers use the information they access, since the various personnel have access to multiple systems.

Furthermore, not all information shared by fusion centers is disseminated through these platforms. In a 2016 survey, fusion center personnel indicated that they often share information through emails, phone calls, or in-person meetings rather than through these automated systems.[62] These offline information-sharing methods make it even more difficult to regulate how fusion center personnel use information extracted from federal intelligence systems.

Many fusion centers also purchase access to data sets collected by private-sector data brokers like LexisNexis and credit reporting agencies like TransUnion,[63] and have contracted with data analytics firms like Palantir and facial recognition companies such as Tygart Technology and Clearview AI.[64] There is hardly any federal regulation regarding how fusion centers contract to obtain these types of information and use these technologies, which can reveal intimate details of Americans' lives. Indeed, the information gathered by these brokers and firms is far more likely to pertain to innocent persons than to criminals.[65] The federal government does not vet these contractors, who may gain access to law enforcement sources, methods, data requirements, and often sensitive data itself, adding to the fusion center network's security vulnerabilities.

Without strong rules restricting improper use, independent oversight capable of uncovering abuse, and public accountability, the "need to share" culture promoted by fusion center proponents creates unacceptable risks to Americans' civil rights and civil liberties. Moreover, protecting individual privacy is not just a hallmark of a free society, it is essential to genuine security.[66] The vast rivers of information about Americans that flow through fusion centers do not resolve vulnerabilities; they create new ones.

Creating New Security Risks

>> **Fusion centers** have proved themselves to be inadequate guardians of the security of the sensitive information in their systems. In 2020, hacktivists exploited a security vulnerability at a fusion center contractor to obtain 269 gigabytes of sensitive information from 251 different law enforcement agencies, as well as the FBI, DHS, and the National Guard, spanning a 24-year period from 1996 to 2020.[67] The leaked data, dubbed "BlueLeaks" in the media, included personal information about 700,000 law enforcement officers, as well as witnesses, victims, and suspects. It also exposed a trove of biased, inappropriate, and erroneous intelligence products and law enforcement training materials coursing through the fusion center network. Some of these documents reveal the abuses discussed in this report.

Untethered Data Collection Standards

State and local law enforcement intelligence units have long abused their power to suppress labor organizing, hound protest movements, and intimidate political opponents.[68] To curb this pattern of abuse, in 1980, the Justice Department established a regulation limiting the kinds of information that state and local law enforcement agencies could collect and distribute via shared criminal intelligence systems receiving federal funding through the Omnibus Crime Control and Safe Streets Act of 1968. The Criminal Intelligence Systems Operating Policies, codified at 28 C.F.R. Part 23, prohibits participating agencies from collecting and maintaining information concerning individuals in the absence of reasonable suspicion that they are involved in criminal conduct and that the information is relevant to that activity. The regulation further prohibits participating agencies from collecting information about "the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity." It also restricts access to this information to individuals who have a "need to know and a right to know the information in the performance of a law enforcement activity." And it limits retention of information within criminal intelligence systems, requiring them to purge information after five years.[69]

The reasonable suspicion standard established in 28 C.F.R. Part 23 is not particularly arduous: it is defined simply as facts sufficient to give a trained investigator "a basis to believe there is a reasonable possibility that an individual or organization is involved in a definable criminal activity."[70] Law enforcement officers were already familiar with this "reasonable suspicion" standard, which the Supreme Court imposed in *Terry v. Ohio* (1968) for stop-and-frisks.[71] State and local law enforcement embraced the same standard for intelligence collection as a means to protect against constitutional violations as well as to prevent the accumulation of useless, irrelevant information polluting their systems, and many agencies adopted identical requirements in their own regulations and policies.[72]

After the 9/11 terrorist attacks, however, federal officials sought to undermine the regulation so that fusion centers could collect and disseminate counterterrorism leads they received through the "If You See Something, Say Something" campaign. In 2008, the Justice Department attempted to amend 28 C.F.R. Part 23 to allow for this broader type of intelligence sharing. Its effort failed, however, in the face of opposition by civil rights groups and even associations representing law enforcement intelligence officials.[73]

At the same time, the Office of the Director of National Intelligence was developing a new federal system called the Information Sharing Environment (ISE), which it hoped to populate with suspicious activity reports (SARs) received from members of the public or local law enforcement and processed through fusion centers for dissemination to the federal government.[74] The ISE defined SARs as "official documentation of observed behavior that may be indicative of intelligence gathering or preoperational planning related to terrorism, criminal [*sic*], or other illicit intention."[75] This was a broad definition in light of the wide variety of activities that could be perceived as "preoperational planning" or related to an "illicit intention." The FBI soon established a parallel system for collecting these reports called eGuardian.[76] Meanwhile, DHS publicly promoted the "If You See Something, Say Something" campaign and provided training to fusion center personnel and the public.[77]

Working together, the ISE program manager, the FBI, and DHS implemented the Nationwide Suspicious Activity Reporting Initiative (NSI), which enlisted fusion centers as the primary conduit to receive SARs from the local level and vet them for dissemination to the ISE and eGuardian.[78] Training materials distributed by DHS identified innocuous, commonplace activities like taking photographs, asking questions, and using binoculars as reportable behaviors.[79] Several law enforcement agencies and fusion center leaders balked at participating in these initiatives, however, because the SAR standards that ISE and eGuardian employed did not meet the "reasonable suspicion" standard required by 28 C.F.R. Part 23 or, in many cases, their own policies.[80]

In an effort to coax these agencies to participate in the NSI, the ISE program manager amended the ISE-SAR functional standard to require that documents fed into the system be "reasonably indicative of criminal activity associated with terrorism."[81] This language appeared to be roughly equivalent to the "reasonable suspicion" requirement of 28 C.F.R. Part 23, particularly as the amended standard specifically referenced *Terry*.[82] But in practice, the ISE standard was quickly undermined, as the FBI promoted eGuardian's lower submission requirements to encourage faster growth.[83] Then, Justice Department officials quietly instructed state and local law enforcement to interpret the ISE's "reasonably indicative" language as more permissive than the "reasonable suspicion" standard of 28 C.F.R. Part 23, so that ISE and eGuardian would harmonize in applying a weaker SAR standard.[84]

Had SARs been required to comply with 28 C.F.R. Part 23, they also would have been subject to its prohibitions on the targeting of First Amendment–protected activity and its limits on information sharing for non–law enforcement purposes. In 2013, DHS's Office for Civil Rights and Civil Liberties (CRCL) recommended that fusion centers adopt policies "comparable in scope and effectiveness to 28 C.F.R. Part 23" in recognition of fusion centers' potential "infringement of First Amendment protections."[85]

The failure to apply such restrictions predictably resulted in fusion centers' submission of SARs based on ideological and racial biases.[86] These reports often covered protest movements and minority communities, particularly American Muslims. A recent review of reports from the Chicago-area fusion center found a number of SARs describing men as suspicious based in part on their ethnic origin.[87] Among the issues that the Chicago Police Department ordered its officers to report to the fusion center was "information concerning strikes, labor-management incidents or union controversies."[88] And an analysis of SARs submitted by Mall of America security officers and local police in Minnesota over five years found that 65 percent of the reports involved people of color.[89]

DHS claimed that approximately a third of the 100,000 SARs submitted to the NSI between 2010 and 2017 had a "nexus to terrorism" and were uploaded to the ISE or eGuardian.[90] But "nexus to terrorism" is a flexible term, particularly given DHS's track record of treating protestors, journalists, and attorneys as potential terrorists.[91] One fusion center director told researchers that he would categorize any SAR that has "anything" to do with "foreign nationals" as a potentially serious indicator of terrorism. An analyst observed that information about fraud or marijuana would be considered terrorism-related if "the money's going to freaking somewhere in the Middle East with two guys from Saudi Arabia, that type of thing."[92] It is therefore no surprise that only 2.3 percent of those 100,000 reports furthered an FBI investigation or involved someone on the terrorist watch list (both of which themselves have low standards).[93]

DHS has done little to mitigate these issues, leaving fusion centers to operate largely unchecked.[94] The agency's Office of Intelligence and Analysis (I&A) does conduct annual audits, but those audits rely on fusion centers' self-reports and focus on policy implementation rather than substantively examining fusion centers' operations and intelligence products to ensure compliance with laws, regulations, and policies.[95] DHS lists as the first goal of its annual fusion center assessment to "[c]ommunicate the fusion centers' value in contributing to national information sharing and homeland security outcomes," making clear that the purpose is to promote fusion centers rather than to critically evaluate them.[96]

Nor have states picked up the slack.[97] The first comprehensive congressional study of fusion centers, conducted by a subcommittee of the Senate Committee on Homeland Security and Governmental Affairs in 2012, found significant inconsistencies in states' compliance with the federal requirement that they audit expenditures of grant funds and determined that states frequently failed to track fusion center spending separate from that of other programs.[98] A 2017 DHS inspector general report indicated that the problem has persisted: due to the way states administer federal law enforcement grants, DHS still could not accurately track its grant spending to fusion centers to determine how much federal money they receive and spend on counterterrorism.[99]

In sum, fusion centers have virtually unchecked access to vast rivers of data, which they have exploited to target protest movements and other disfavored groups. Moreover, as discussed below, there is little evidence that they have been effective in protecting the communities they serve from terrorism or other serious crime.

Unimpressive Results

Fusion centers' contributions to combating terrorism have been scant. The 2012 Senate study criticized fusion centers for wasting counterterrorism resources and infringing on civil liberties. The committee staff reviewed more than 80,000 pages of intelligence reports, emails, and audits; undertook a nationwide survey of fusion centers; and interviewed dozens of DHS staff and local and state officials.[100] The final report concluded that the intelligence produced by DHS officers deployed to fusion centers was "oftentimes shoddy, rarely timely, sometimes endangering citizens' civil liberties and Privacy Act protections, occasionally taken from already-published public sources, and more often than not unrelated to terrorism."[101] It found that DHS support for fusion centers "yielded little, if any, benefit to Federal counterterrorism intelligence efforts."[102] Furthermore, DHS failed to illustrate a single "clear example in which a fusion center provided intelligence which helped disrupt a terrorist plot."[103]

In the decade since, DHS has made few efforts to address the criticisms in the report or to implement its recommendations. Public knowledge of fusion center abuses relies almost entirely on leaks, investigative reporting, and researchers using open records laws to pry information free rather than evaluations produced by official oversight bodies.

Even when the fusion center network has gotten the intelligence right and warned of an attack, it has failed to galvanize an effective law enforcement response. Fusion centers reportedly alerted federal law enforcement to social media posts indicating that far-right militants were preparing to engage in violence at the U.S. Capitol on January 6, 2021.[104] FBI and DHS leadership ignored these warnings, however, along with other prior alarms raised by lawmakers, former law enforcement and national security officials, social media companies, terrorism researchers, and the *Washington Post*.[105] It is not clear whether the FBI and DHS failed to heed the fusion centers' reporting because these agencies had become accustomed to discounting the faulty intelligence that the centers often produce or because bias blinded them to the threat.

There is also little evidence that fusion centers have aided law enforcement in addressing general crime problems,

despite shifting their missions to cover "all crimes" and "all hazards." While the number of fusion centers has expanded and their capabilities have increased over the last two decades, their intelligence collection, information-sharing, data analysis, and case support efforts have not demonstrably helped law enforcement become more efficient or effective at solving the most serious types of crimes. Most violent crime in the United States still goes unsolved. The clearance rate for murders was just over 50 percent in 2020, down from rates as high as 70 percent in the 1980s, before any of these information-sharing systems existed.[106] Just as the 2012 Senate investigation determined that fusion centers' declared counterterrorism successes were disproven upon examination, law enforcement officials have disputed their claimed successes in solving crimes.[107] A San Jose Police Department spokesperson, for example, recently publicly contradicted a local fusion center's claim of having assisted in the arrest of a man threatening to shoot up a shopping mall. The fusion center's director later acknowledged that it is difficult to determine a fusion center's efficacy, noting, "It's really hard to connect a specific report to an arrest or specific conviction."[108]

Nor have fusion centers had much apparent effect on crime rates. Parsing what causes crime to rise or fall is a difficult matter, but that did not stop the Chicago fusion center's director from claiming that the center's revolutionary methods were responsible for a drop in homicides in the city from 2007 (when the center was established) to 2010.[109] Yet the murder rate in Chicago rose significantly over the following years, even as the fusion center continued to operate, reaching a 25-year high of 797 homicides in 2021.[110] Chicago police made arrests in just 26 percent of these cases.[111]

Finally, the widespread collection of SARs can swamp fusion centers with irrelevant reports. One fusion center official reported that an "overwhelming majority" of incoming SARs were unfounded.[112] Fusion center analysts responding to a George Washington University survey described SARs as "white noise" that impedes effective intelligence analysis.[113]

The lax standards for fusion centers' collection and dissemination of information about Americans not reasonably suspected of criminal activity are at best an ineffective counterterrorism tool. At worst, they perpetuate biased policing practices and exhaust law enforcement resources that could more effectively be deployed to address serious criminal activity.

Recommendations

In less than two decades, fusion centers have strayed far from their initial anti-terrorism mission and activities, continuing to receive millions in federal support even as oversight mechanisms have failed to curb abuses.

State and local governments have the authority to determine whether the benefits of maintaining their fusion centers are worth the costs, particularly as they take on a larger share of the financial burden. And where particular fusion centers have a documented record of abuses, elected officials should be responsive to their constituents' concerns and demand greater accountability. Local advocates from Massachusetts to Texas to California have called for closing fusion centers.[114] In Maine, a bill to eliminate fusion center funding passed through the state house of representatives in 2021 but failed in the state senate.[115]

For its part, the federal government must ensure that the significant resources it devotes to fusion centers and the access it provides to powerful intelligence systems achieve their stated purpose, and that fusion center personnel using these resources comply with all applicable laws, regulations, and policies designed to protect Americans' constitutional rights and individual privacy.

This report's recommendations fall into two categories: steps that the secretary of homeland security can take immediately and those that require congressional action. Taken together, these measures will reduce redundancy and error, strengthen civil rights and civil liberties protections, and increase transparency so that abuses can be quickly discovered and remediated. These new oversight mechanisms should reinforce the requirements of 28 C.F.R. Part 23 to ensure that fusion centers comply with both the purpose and intent of the regulation for all law enforcement information-sharing systems.[116]

Recommendations for the Secretary of Homeland Security

The secretary of homeland security should take the following actions to strengthen oversight of fusion centers' use of DHS grant funds, personnel, and information-sharing systems.

>> Increase the transparency and accountability of DHS grant funding.

The secretary should mandate that DHS grant programs clearly articulate their federal homeland security purpose and ensure that all spending is traceable to its end use. Further, DHS should reconfigure its audits and assessments of fusion centers, including the Fusion Center Performance Program and the annual fusion center assessment. DHS audits and assessments should

- track DHS funds to ensure that they are used for their stated purpose, in a manner that accomplishes the stated goals of the grant, and in compliance with all applicable laws, regulations, and policies;
- focus on uncovering evidence of waste, fraud, or abuse;

- evaluate the quality (rather than quantity) of fusion center reports produced in whole or in part with DHS resources, assessing accuracy, timeliness, and relevance to law enforcement or DHS missions;

- evaluate whether — and the extent to which — fusion centers are following laws, regulations, and policies designed to protect privacy, civil rights, and civil liberties rather than just checking whether fusion centers have fulfilled the administrative task of adopting such policies;

- identify all non–law enforcement government agencies and private entities that participate in fusion centers (including contractors and vendors) and describe their role and functions within the fusion center, as well as whether they receive DHS funds or access to DHS systems, other law enforcement systems, or nonpublic DHS threat, intelligence, or situational awareness reporting; and

- identify all private data brokers and technology companies whose data and services are either contracted by fusion centers or accessible to federal employees assigned to fusion centers, and describe the nature of the data or services.

The secretary should regularly release detailed public reports documenting the results of these audits and assessments.

>> Evaluate civil rights and civil liberties implications.

The secretary should require the DHS Office for Civil Rights and Civil Liberties to regularly evaluate individual fusion centers receiving DHS resources to identify harms to civil rights and civil liberties. The office should receive appropriate staffing and other resources to enable this review, and compliance on the part of the fusion centers should be a condition for continued federal grant funding. These evaluations should be scheduled so that each fusion center receiving DHS resources is evaluated at least once every three years. These evaluations should be designed to examine whether

- fusion center products, including bulletins, threat warnings, situational reports, SARs, and other substantively similar products, comply with all appropriate constitutional requirements, laws, regulations, and policies and do not demonstrate bias on the basis of race, ethnicity, religion, political viewpoint, or First Amendment activities;

- activities of all fusion center personnel are properly overseen to ensure compliance with constitutional requirements, laws, regulations, and policies;

- laws, regulations, and policies governing federal information-sharing systems accessible to fusion center personnel are properly followed, particularly to ensure that criminal intelligence and any other information collected with law enforcement authorities is properly segregated from non–law enforcement personnel, and that information provided to law enforcement is properly evaluated for reasonable suspicion of criminal activity before being shared; and

- subscriptions to private information-sharing tools and contracts to obtain data or services comply with constitutional limits and follow all laws, regulations, and policies, as do the methods for collection, analysis, and retention of the data or services provided.

>> Evaluate database use.

The secretary should require the DHS Privacy Office to evaluate fusion center data practices and information-sharing systems to ensure that all laws, regulations, and policies designed to protect individuals' data from unauthorized disclosure are properly followed, and that the data is properly secured from hackers or hostile foreign intelligence services. The secretary should ensure that the office has sufficient staffing and resources to enable this process, which should include evaluating

- the security of personally identifiable information in all federal, state, and local government information-sharing systems accessible to fusion center personnel;

- the practices of all private entities and non–law enforcement personnel operating within fusion centers to ensure that their access to criminal intelligence and law enforcement information is properly limited to protect individuals' data from unauthorized disclosure for non–law enforcement purposes; and

- data systems provided by private contractors, analysts, and technology providers to ensure that these contractors have been properly vetted for security purposes, and that all personally identifiable information collected by fusion centers or transferred over these systems is secure from unauthorized disclosure.

Recommendations for Congress

Congress should take the following actions to investigate waste, fraud, and abuse within the national network of fusion centers.

>> Appoint a special inspector general.

Congress should establish a special inspector general (SIG) for the national network of fusion centers, with a two-year term, to investigate fusion center operations. The SIG should be empowered to identify any waste, fraud, or abuse involving resources originating from any federal department or agency, and should assess whether fusion center personnel are engaged in illegality or in violations of constitutional rights or federal regulations in the performance of their duties. The attorney general, director of national intelligence, secretary of homeland security, secretary of defense, and inspectors general from DHS, DOJ, the Department of Defense, and the intelligence community should be directed to support the SIG as necessary by providing access to documents or personnel at their respective agencies.

The investigation should be designed to determine whether

- federal funds intended to support fusion centers are properly disbursed, cabined to their intended federal purposes, and properly accounted for;
- fusion center activities supported with federal funds are effective in meeting appropriate federal goals;
- fusion center activities, reports, or personnel violate any laws, regulations, or policies, particularly identifying infringements on First Amendment speech and associational rights and Fourteenth Amendment equal protection rights;
- federal personnel assigned to fusion centers are engaged in any illegal or improper conduct;
- personally identifiable information in federal systems accessible to fusion center personnel is properly protected from misuse and unauthorized disclosure;
- classified information, criminal intelligence, and other nonpublic law enforcement information is properly segregated to prevent access by non–law enforcement fusion center personnel;
- the National SAR Initiative has been a cost-effective method of threat reporting considering the volume of investigative hours spent responding to false leads, the standards for submitting SARs to the ISE or eGuardian are followed in practice, and these standards ensure that SARs are timely, accurate, and useful in identifying criminal activity related to terrorism and do not infringe on First Amendment rights or the privacy of individuals not reasonably suspected of criminal activity;
- private fusion center participants and contractors are properly vetted for security purposes and properly segregated from classified information, criminal intelligence, and nonpublic law enforcement records;
- selection of private entities to participate in fusion centers or receive nonpublic fusion center reports is made in a transparent and equitable manner; and
- participation of private entities undermines individual rights and privacy of individuals whose data is collected, analyzed, or disseminated by fusion centers, or enables the targeting of critics of any private entity by law enforcement, intelligence agencies, or private security.

The SIG should issue a report to Congress after one year, highlighting any violations of law, waste, or misuse of federal resources that the investigation identifies, as well as any violations of regulations and policies. A second report at the end of the SIG's term should evaluate whether fusion centers implemented the requested reforms or otherwise resolved the issues raised during the SIG's investigation. These reports may be augmented by interim reports as Congress or the SIG deems necessary. The reports should also provide recommendations regarding how the federal government should regulate fusion centers to prevent waste, fraud, abuse, and infringements on constitutional rights, including recommendations regarding the establishment of a permanent oversight mechanism to ensure that future waste, fraud, and abuse occurring within the fusion center network is discovered and properly addressed in a timely manner.

>> Establish an independent federal oversight office.

Congress should establish a permanent independent federal oversight office charged with implementing the reforms recommended by the DHS audits, the Privacy Office and CRCL evaluations, and the SIG reports described above. If Congress is slow to act, the president could establish an oversight office by executive order.[117]

The oversight office's effectiveness will depend on its independence and the expertise of its staff. Congress should require that the attorney general, secretary of homeland security, and secretary of defense coordinate and cooperate with the oversight office. The office should make direct reports to Congress, and interim reports should be available to members of Congress to view upon request. The office should be led by individuals selected based on experience and ability rather than

political affiliation. Expertise in legal requirements regarding the protection of privacy and civil rights and liberties is essential.

The oversight office should be given the authority to access information and interview personnel from each fusion center. This access must include relevant databases, archives, personnel, and partner agencies and companies, including private-sector participants and contractors, regardless of individuals' affiliation with other federal, state, or local government entities. Fusion centers should be required to provide this access via a designated point person as a condition of receiving federal grants. Oversight office staff must be able to attain the appropriate security clearances to obtain information without delay and conduct uninhibited conversations. Fusion centers' noncompliance with requests to access their staff or information should be grounds for penalties such as limiting federal funding or access to federal information-sharing systems.

Congress should ensure that the oversight office is adequately resourced to conduct robust oversight. The oversight office must also have support from the states that have legislative control over individual fusion centers. Congress can accomplish this requirement by making acceptance of the oversight office's access and authority a condition of continued receipt of federal grant funding and access to federal information-sharing systems.

The oversight office must have the authority to require that fusion centers take corrective action if it identifies civil rights violations, discrimination, unreliable intelligence products, misuse of federal funds — including for non-counterterrorism purposes — or other operational failures. Corrective measures may include increased auditing, suspension of access to federal information-sharing systems, removal of past intelligence products from federal information-sharing systems, and suspension of federal funding.

Conclusion

DHS has played a major role in developing fusion centers as hubs for domestic intelligence collection, but it has failed to conduct the oversight necessary to protect privacy and civil rights and to ensure that security resources are used responsibly and effectively. Errors, abuses, and security lapses over the last two decades are well-documented, but reform remains elusive, leaving the public less secure. Americans should not have to worry that exercising their First Amendment rights, whether speaking out online or protesting on the street, will result in an anonymous fusion center analyst labeling them a potential terrorist in federal intelligence networks. Congress and the secretary of homeland security must ensure that DHS fulfills its responsibilities to defend constitutional rights and to prevent federal law enforcement and security resources from being misused to collect, maintain, or disseminate information that is false, misleading, or related to individuals or groups who are not reasonably suspected of criminal activity.

Endnotes

1 Federal Bureau of Investigation (hereinafter FBI) and Department of Homeland Security (hereinafter DHS), *Strategic Intelligence Assessment and Data on Domestic Terrorism*, May 2021, 7, https://www.fbi.gov/file-repository/fbi-dhs-domestic-terrorism-strategic-report.pdf/view; and Jana Winter, "Law Enforcement Prepares for Potential Violence, Unrest Surrounding Roe Decision," Yahoo News, May 4, 2022, https://news.yahoo.com/exclusive-law-enforcement-prepares-for-potential-violence-unrest-after-roe-decision-204137717.html.

2 Permanent Subcomm. on Investigations, S. Comm. on Homeland Security and Governmental Affairs, *Federal Support for and Involvement in State and Local Fusion Centers* (hereinafter *Federal Support for Fusion Centers*), October 3, 2012, 94–96, https://www.hsgac.senate.gov/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf.

3 Faiza Patel, Rachel Levinson-Waldman, and Harsha Panduranga, *A Course Correction for Homeland Security: Curbing Counterterrorism Abuses*, Brennan Center for Justice, April 20, 2022, https://www.brennancenter.org/our-work/research-reports/course-correction-homeland-security.

4 Marilyn Peterson, *Intelligence-Led Policing: The New Intelligence Architecture*, Bureau of Justice Assistance, Department of Justice, September 2005, 5–13, https://www.ojp.gov/pdffiles1/bja/210681.pdf.

5 Permanent Subcomm. on Investigations, *Federal Support for Fusion Centers*, 10–17; and Government Accountability Office (hereinafter GAO), *Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers* (hereinafter *Federal Efforts Are Helping to Alleviate Fusion Center Challenges*), October 30, 2007, https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-08-35/html/GAOREPORTS-GAO-08-35.htm.

6 DHS, *2018 National Network of Fusion Centers Final Report* (hereinafter *2018 Fusion Centers Final Report*), 2018, 2–4, https://www.dhs.gov/sites/default/files/publications/2018_national_network_of_fusion_centers_final_report.pdf.

7 Permanent Subcomm. on Investigations, *Federal Support for Fusion Centers*, 13–14.

8 Permanent Subcomm. on Investigations, *Federal Support for Fusion Centers*, 93–96.

9 For example, the mission of the West Virginia Fusion Center is "to anticipate, identify, and prevent criminal activity and all other hazards and to responsibly distribute that intelligence to its stakeholders while both protecting the rights of its citizens and guarding the rights and integrity of law enforcement and private industry," while the Florida Fusion Center aims "to protect citizens, visitors, resources, and critical infrastructure of Florida by enhancing information sharing, intelligence, capabilities, and preparedness operations for all local, state, and federal agencies." The North Texas Fusion Center emphasizes the involvement of private industry, describing its mission as "protect[ing] the citizens of North Texas by creating a synergistic environment among governmental and corporate stakeholders." See West Virginia Fusion Center, "Mission & Vision," accessed November 19, 2022, https://fusioncenter.wv.gov/pages/Mission.aspx; Florida Department of Law Enforcement, "The Florida Fusion Center," accessed November 19, 2022, http://www.fdle.state.fl.us/FFC.aspx; and Collin County, Texas, "North Texas Fusion Center," accessed November 19, 2022, https://www.collincountytx.gov/sheriff/fusion_center/Pages/default.aspx.

10 In 2017, fusion centers received some $63.1 million in federal grants. The bulk of this support ($53.6 million) came from DHS — particularly from the Homeland Security Grant Program (HSGP), which is meant to assist in "preventing, protecting against, mitigating, responding to and recovering from acts of terrorism and other threats." Federal Emergency Management Agency (hereinafter FEMA), "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2022 Homeland Security Grant Program," DHS, May 13, 2022, https://www.fema.gov/grants/preparedness/homeland-security/fy-22-nofo. Within DHS distributions, fusion centers receive funding through the FEMA-managed HSGP, primarily through one of two subgrant programs: Urban Area Security Initiative (UASI) grants and State Homeland Security Program (SHSP) grants. Funding is contingent on a number of requirements, including completing the annual fusion center assessment managed by the Office of Intelligence and Analysis, conducting a compliance review and audit of publicly available privacy, civil rights, and civil liberties policies, and providing a biannual program performance report to FEMA. DHS, "Homeland Security Grant Program (HSGP)," accessed November 19, 2022, https://www.dhs.gov/homeland-security-grant-program-hsgp; and FEMA, *FEMA Preparedness Grants Manual*, DHS, February 2021, A-24, A-25, https://www.fema.gov/sites/default/files/documents/FEMA_2021-Preparedness-Grants-Manual_02-19-2021.pdf. The remaining federal grants were awarded by the DOJ's Community Oriented Policing Services Office and Bureau of Justice Assistance and the Drug Enforcement Agency's High Intensity Drug Trafficking Areas program. See DHS, *2017 National Network of Fusion Centers Final Report* (hereinafter *2017 Fusion Centers Final Report*), October 2018, 15, https://www.dhs.gov/sites/default/files/publications/2017_National_Network_of_Fusion_Centers_Final%20Report.pdf. Of the nonfederal grants, $210.9 million came from state and local sources, with an additional $4.4 million from tribal, territorial, and private-sector grants. DHS, *2017 Fusion Centers Final Report*, 15. Fusion centers also benefit from "direct" federal expenditures — to the tune of $44.3 million in 2017. That money seems to reflect the deployment of federal employees, largely from DHS and DOJ, to fusion centers as supplemental analysts. There were 297 such employees in 2017, but we do not know how many come from counterterrorism-focused offices within the federal government. See DHS, *2017 Fusion Centers Final Report*, 15; GAO, *Federal Efforts Are Helping to Alleviate Fusion Center Challenges*; and Permanent Subcomm. on Investigations, *Federal Support for Fusion Centers*, 20. In 2018, the overall amounts contributed by federal grant programs ($75.2 million) and by states and localities ($214.9 million) were somewhat higher, but there is no publicly available breakdown of the amounts contributed by various federal agencies. DHS, *2018 Fusion Centers Final Report*, 2.

11 DHS Office of Inspector General, Intelligence Community Office of Inspector General, and DOJ Office of Inspector General (hereinafter, collectively, OIG), *Review of Domestic Sharing of Counterterrorism Information*, March 2017, 44, https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-49-Mar17.pdf; and Peterson, *Intelligence-Led Policing*.

12 DHS, *2017 Fusion Centers Final Report*, 17. Although DHS published a similar report in 2018, we have relied on the 2017 report because it contains more detailed information. There are some variations in the percentage of fusion centers identifying certain matters as priorities, but those do not affect the overall picture.

13 DHS, *2017 Fusion Centers Final Report*, 11.

14 Joshua Rhett Miller, "'Fusion Centers' Expand Criteria to Identify Militia Members," Fox News, December 24, 2015, https://www.foxnews.com/politics/fusion-centers-expand-criteria-to-identify-militia-members.

15 Ryan Devereaux, "Leaked Documents Show Police Knew Far-Right Extremists Were the Real Threat at Protests, Not 'Antifa,'" *Intercept*, July 15, 2020, https://theintercept.com/2020/07/15/george-floyd-protests-police-far-right-antifa.

16 Logan Carroll, "Leaked Documents: Intelligence Wing of

Law Enforcement Struggled to Fulfill Its Mission During George Floyd Protests," *Minnesota Reformer*, July 8, 2020, https://minnesotareformer.com/2020/07/08/leaked-documents-intelligence-wing-of-law-enforcement-struggled-to-fulfill-its-mission-during-george-floyd-protests.

17 Micah Lee, "How Northern California's Police Intelligence Center Tracked Protests," *Intercept*, August 17, 2020, https://theintercept.com/2020/08/17/blueleaks-california-ncric-black-lives-matter-protesters.

18 Mara Hvistendahl, "Austin Fusion Center Spied on Nonpolitical Cultural Events," *Intercept*, November 30, 2020, https://theintercept.com/2020/11/30/austin-fusion-center-surveillance-black-lives-matter-cultural-events.

19 Mike Tipping, "Data Breach Exposes Activities of Maine's Secretive Police Intelligence Agency," *Beacon* (Maine People's Alliance), June 26, 2020, https://mainebeacon.com/data-breach-exposes-activities-of-maines-secretive-police-intelligence-agency.

20 Office of Intelligence and Analysis (hereinafter I&A), "Open Source Intelligence Report (OSIR)," DHS, June 2, 2020, https://www.documentcloud.org/documents/20643306-maine-information-and-analysis-center-alert; and Nathan Bernard and Caleb Horton, "Teenager or Terrorist?," *Mainer*, July 29, 2020, https://mainernews.com/teenager-or-terrorist.

21 Bernard and Horton, "Teenager or Terrorist?"

22 Bernard and Horton, "Teenager or Terrorist?"

23 Jason Wilson, "Officials Baselessly Linked 'Antifa' to Arson Before Wildfires, Documents Show," *Guardian*, September 19, 2020, https://www.theguardian.com/us-news/2020/sep/19/police-antifa-arson-wildfire-conspiracy-theories.

24 Sam Levin, "How California Police Chased a Nonexistent 'Antifa Bus,'" *Guardian*, August 23, 2021, https://www.theguardian.com/us-news/2021/aug/23/revealed-california-police-antifa-misinformation.

25 Farrell-Smith v. Oregon Dep't of Justice, No. 21CV47809 (Or. Cir. Ct. December 14, 2021), complaint ¶ 48, https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/61bb7484b5d3234af35ca694/1639675023280/2021-12-14+Oregon+Complaint+FILESTAMPED.pdf. See also Will Parrish and Jason Wilson, "Anti-Terror Center Helped Police Track Environmental Activists," *Guardian,* October 2, 2019, https://www.theguardian.com/us-news/2019/oct/02/oregon-pipelines-protests-monitoring-police-anti-terror-unit.

26 *Farrell-Smith*, complaint ¶ 51; and Parrish and Wilson, "Anti-Terror Center Helped Police."

27 *Farrell-Smith*, complaint ¶¶ 53–54.

28 Curtis Waltman, "DAPL Fusion Center Reports Illustrate Everything Wrong with Fusion Centers," MuckRock, August 9, 2017, https://www.muckrock.com/news/archives/2017/aug/09/dapl-threat-assessment-ii; and MuckRock, "DAPL Protest Threat Assessments," accessed November 19, 2022, https://www.muckrock.com/foi/north-dakota-232/dapl-protest-threat-assessments-40376/#file-143404 (including in its list of references the "Michigan State Police" and "Morton County Intel Tip #201").

29 *Farrell-Smith*, complaint ¶ 49.

30 *Farrell-Smith*, complaint ¶ 55.

31 Alleen Brown, Will Parrish, and Alice Speri, "Standing Rock Documents Expose Inner Workings of 'Surveillance-Industrial Complex,'" *Intercept*, June 3, 2017, https://theintercept.com/2017/06/03/standing-rock-documents-expose-inner-workings-of-surveillance-industrial-complex.

32 Alleen Brown, "In the Mercenaries' Own Words: Documents Detailing TigerSwan Infiltration of Standing Rock," *Intercept*, November 15, 2020, https://theintercept.com/2020/11/15/standing-rock-tigerswan-infiltrator-documents.

33 Alleen Brown, Will Parrish, and Alice Speri, "Leaked Documents Reveal Counterterrorism Tactics Used at Standing Rock to 'Defeat Pipeline Insurgencies,'" *Intercept*, May 27, 2017, https://theintercept.com/2017/05/27/leaked-documents-reveal-security-firms-counterterrorism-tactics-at-standing-rock-to-defeat-pipeline-insurgencies.

34 Adam Federman, "Undercover Agents Infiltrated Tar Sands Resistance Camp to Break Up Planned Protest," *Earth Island Journal*, August 12, 2013, https://www.earthisland.org/journal/index.php/articles/entry/undercover_agents_infiltrated_tar_sands_resistance_camp_to_break_up_planned; and Adam Federman, "TransCanada Is Spying on Keystone XL Opponents," *Earth Island Journal*, June 20, 2013, https://www.earthisland.org/journal/index.php/articles/entry/transcanada_is_spying_on_keystone_xl_opponents.

35 Dobbs v. Jackson Women's Health Organization, 142 S. Ct. 2228 (2022); and Darragh Roche, "Homeland Security Visits Woman over Her Tweet About Roe v. Wade Reversal," *Newsweek*, July 2, 2022, https://www.newsweek.com/homeland-security-visits-woman-over-her-tweet-about-roe-v-wade-reversal-1721236.

36 Virginia Fusion Center, "Leaked SCOTUS Document May Inspire Abortion Related Civil Unrest and Violence Incidents," May 2022, https://www.documentcloud.org/documents/22017783-vfc-scotus.

37 Kevin Rector, "Why Did Federal Police Square Off with Abortion Rights Protesters in L.A. Streets?," *Los Angeles Times*, May 5, 2022, https://www.latimes.com/california/story/2022-05-05/why-were-federal-police-squaring-off-with-abortion-rights-protesters-in-l-a-s-streets.

38 Jake Laperruque, "Cracking Down on Federal Aid for Reproductive Health Surveillance: Fusion Centers," Center for Democracy and Technology, October 5, 2022, https://cdt.org/insights/cracking-down-on-federal-aid-for-reproductive-health-surveillance-fusion-centers; and Lily Hay Newman, "The Surveillance State Is Primed for Criminalized Abortion," *Wired*, May 24, 2022, https://www.wired.com/story/surveillance-police-roe-v-wade-abortion. In September 2022, to avert this eventuality, California passed the first law to prevent in-state law enforcement officers and tech companies from assisting out-of-state criminal investigations into abortion services that are lawful under California law. Cal. Health & Safety Code §§ 103005, 123462, 123467–123469 (West 2022).

39 On law enforcement's historical repression of protest movements, see, e.g., Frank Donner, *Protectors of Privilege: Red Squads and Police Repression in Urban America* (Berkeley: University of California Press, 1990).

40 Mary Ellen Callahan, *Privacy Impact Assessment for the HSIN 3.0 Shared Spaces: On the Sensitive but Unclassified Network*, DHS, July 25, 2012, 1–2, https://www.dhs.gov/sites/default/files/publications/privacy_pia_ops_hsin_sharedspace_07252012.pdf; and FEMA, *National Incident Management System*, DHS, October 2017, https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf.

41 Homeland Security Information Network (hereinafter 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.

42 Callahan, *Privacy Impact Assessment for HSIN 3.0 Shared Spaces*, 1, 3–4. See, e.g., Office of Inspector General, *Actions Related to an I&A Intelligence Product Deviated from Standard Procedures (Redacted)*, DHS, April 26, 2022, 5, 16, https://www.oig.dhs.gov/sites/default/files/assets/2022-05/OIG-22-41-Apr22-Redacted.pdf (noting that unclassified intelligence products from I&A that are approved for dissemination are posted onto HSIN).

43 HSIN, *2020 Annual Report: Delivering Mission Success*, 1, 16–17.

44 Erin M. Prest, *Privacy Impact Assessment for the Law Enforcement Online (LEO) Services* (hereinafter *PIA for LEO*), DOJ, July 16, 2019, 2, 19, https://www.fbi.gov/file-repository/pia-leo-services.pdf/view.

45 Prest, *PIA for LEO*, 5.

46 FBI, *Information Sharing and Safeguarding Report 2012*, DOJ, 2012, https://www.fbi.gov/stats-services/publications/national-information-sharing-strategy-1; and Prest, *PIA for LEO*, 2, 6, 7.

47 Erin M. Prest, *Privacy Impact Assessment for the National Data Exchange (N-DEx) System* (hereinafter *PIA for N-DEx*), DOJ, August 29, 2018, 2–3, https://www.fbi.gov/file-repository/pia-national-data-exchange-n-dex-system.pdf/view.

48 John S. Hollywood and Zev Winkelman, *Improving Information-Sharing Across Law Enforcement: Why Can't We Know?*, RAND Corporation, 2015, 5, https://www.ojp.gov/pdffiles1/nij/grants/249187.pdf.

49 Prest, *PIA for N-DEx*, 3.

50 Regional Information Sharing Systems (RISS) Program, "About the RISS Program: A Proven Resource for Law Enforcement," accessed November 19, 2022, https://www.riss.net/about-us; and Hollywood and Winkelman, *Improving Information-Sharing Across Law Enforcement*, 10.

51 RISS, "Regional Information Sharing Systems (RISS) Program," last updated May 2022, https://www.riss.net/wp-content/uploads/2022/06/RISS-Overview-Brochure-2022.pdf.

52 Law Enforcement Information Exchange (hereinafter LInX), "Introduction and Overview," accessed November 19, 2022, https://www.linxnc.us/Linx/WebHelp/overview.htm; and Naval Criminal Investigative Service (hereinafter NCIS), "LInX/D-Dex," accessed November 19, 2022, https://www.ncis.navy.mil/Mission/Partnership-Initiatives/LInX-D-Dex.

53 NCIS, "Law Enforcement Information Exchange (LInX) Program Briefing" (PowerPoint presentation, November 2007, slides 7, 13), https://www.mwcog.org/file.aspx?A=CUxX2Acv9k2DtAiVvto8nJ2la7P7j/EAXbYC1tsEOsI=; and NCIS, "Law Enforcement Information Exchange (LInX)" (PowerPoint presentation, Justice and Public Safety Appropriation Subcommittee, March 11, 2015, slides 4, 10), https://cjin.nc.gov/infoSharing/Presentations/LInX%20Presentation%20JPS%20Sub-Committee%202-18-2015%20Final.pdf.

54 NCIS, "Law Enforcement Information Exchange (LInX)," March 11, 2015, slide 11.

55 28 C.F.R. § 23.20(a).

56 DHS, "DHS Announces New Information-Sharing Tool to Help Fusion Centers Combat Terrorism," press release, September 14, 2009, https://www.dhs.gov/news/2009/09/14/new-information-sharing-tool-fusion-centers-announced.

57 Dell Cameron, "Assange Charges Finally Reveal Why Chelsea Manning Is Sitting in Jail," *Gizmodo*, April 11, 2019, https://gizmodo.com/assange-charges-finally-reveal-why-chelsea-manning-is-s-1833972958; and Kim Zetter and Kevin Poulsen, "U.S. Intelligence Analyst Arrested in WikiLeaks Video Probe," *Wired*, June 6, 2010, https://www.wired.com/2010/06/leak.

58 DHS, "IT Program Assessment: DHS — Homeland Secure Data Network (HSDN)," accessed November 19, 2022, https://www.dhs.gov/xlibrary/assets/mgmt/itpa-dhs-hsdn2012.pdf.

59 See, e.g., Robert Mandel, *Global Data Shock: Strategic Ambiguity, Deception, and Surprise in an Age of Information Overload* (Stanford, CA: Stanford University Press, 2019); and Tara Seals, "Threat Intelligence Strategies Suffer from Data Overload," Info Security Group, accessed November 19, 2022, https://www.infosecurity-magazine.com/news/threat-intelligence-strategies.

60 Bernard and Horton, "Teenager or Terrorist?"

61 Federal systems are also covered by the Privacy Act of 1974, Pub. L. 93–579, which imposes restrictions on how the federal government collects, uses, and discloses personally identifying information and grants certain rights to individuals whose data is collected. The Privacy Act contains several broad exemptions, including for law enforcement specifically, but law enforcement agencies must still follow fair information practices, including in complying with the Privacy Act's disclosure requirements, by ensuring the "accuracy, completeness, timeliness, and relevance of records" and establishing rules to safeguard the security of the data. See Electronic Privacy Information Center, "The Privacy Act of 1974," accessed November 19, 2022, https://epic.org/the-privacy-act-of-1974.

62 Jeremy G. Carter et al., "Law Enforcement Fusion Centers: Cultivating an Information Sharing Environment While Safeguarding Privacy," *Journal of Police and Criminal Psychology* 32 (2017): 23, https://scholarworks.iupui.edu/bitstream/handle/1805/11245/Carter_2016_law.pdf;sequence=1.

63 See *Digital Dragnets: Examining the Government's Access to Your Personal Data, Hearing Before the H. Comm. on the Judiciary*, 117th Cong. (2022), 7 (statement of Sarah Lamdan, professor of law, City University of New York Law School), https://docs.house.gov/meetings/JU/JU00/20220719/115009/HHRG-117-JU00-Wstate-LamdanS-20220719.pdf; and Chris Cushing et al., *MIAC [Maine Information and Analysis Center] Shadow Report: Reporting on MIAC Auditing Processes Supplemental to the DPS Report*, April 1, 2022, 34, https://mainebeacon.com/wp-content/uploads/2022/03/MIAC-Shadow-Report.pdf.

64 Caroline Haskins, "This Is Palantir's Top-Secret User Manual for Cops," *Vice*, July 12, 2019, https://www.vice.com/en/article/9kx4z8/revealed-this-is-palantirs-top-secret-user-manual-for-cops (describing use of Palantir by a Northern California fusion center); Stephen Mayhew, "Fusion Intelligence Center Implements Tygart Facial Recognition Software," BiometricUpdate.com, October 16, 2014, https://www.biometricupdate.com/201410/fusion-intelligence-center-implements-tygart-facial-recognition-software; and Ryan Mac, Caroline Haskins, and Logan McDonald, "Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA," BuzzFeed News, February 27, 2020, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

65 *Digital Dragnets, Hearing Before the H. Comm. on the Judiciary* (2022), 5–7 (statement of Elizabeth Goitein, Liberty and National Security Program, Brennan Center for Justice), https://docs.house.gov/meetings/JU/JU00/20220719/115009/HHRG-117-JU00-Wstate-GoiteinE-20220719.pdf.

66 See, e.g., President's Review Group on Intelligence and Communication Technologies, "Liberty and Security for a Changing World," December 12, 2013, 14, 15, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

67 Micah Lee, "Hack of 251 Law Enforcement Websites Exposes Personal Data of 700,000 Cops," *Intercept*, June 15, 2020, https://theintercept.com/2020/07/15/blueleaks-anonymous-ddos-law-enforcement-hack; and Brian Krebs, "'BlueLeaks' Exposes Files from Hundreds of Police Departments," *Krebs on Security* (blog), June 22, 2020, https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments.

68 Donner, *Protectors of Privilege*.

69 28 C.F.R. § 23.20(a)–(h).

70 28 C.F.R. § 23.20(c).

71 Terry v. Ohio, 392 U.S. 1 (1968).

72 See, e.g., Association of Law Enforcement Intelligence Units, "History, Purpose, and Operations," revised August 19, 2009, http://leiu.org/sites/default/files/History%2C%20Purpose%2C%20and%20Operations.pdf.

73 See, e.g., comments by the Association of Law Enforcement Intelligence Units and the Criminal Intelligence Coordinating Council on proposed modifications to 28 C.F.R. Part 23 (Russell M. Porter, general chair, Association of Law Enforcement Intelligence Units, to Michael Dever, policy adviser, Bureau of Justice Assistance, DOJ, September 1, 2008, https://www.regulations.gov/comment/OJP-2008-0002-0010; and Russell M. Porter chair, Criminal Intelligence Coordinating Council, to Michael Dever, policy adviser, Bureau of Justice Assistance, DOJ, September 2, 2008, https://www.regulations.gov/comment/OJP-2008-0002-0016).

74 GAO, *Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress*, June 2008, https://www.gao.gov/assets/gao-08-492.pdf.

75 "Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)" (PowerPoint, undated, slide 3), accessed November 19, 2022, https://info.publicintelligence.net/SARsuspiciousactivityreporting.pdf.

76 FBI, "Connecting the Dots Using New FBI Technology," DOJ, September 19, 2008, https://archives.fbi.gov/archives/news/stories/2008/september/eguardian_091908.

77 DHS, "If You See Something, Say Something® Campaign Overview," last updated May 17, 2022, https://www.dhs.gov/publication/if-you-see-something-say-something%E2%84%A2-campaign-overview.

78 "Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)," slides 2, 4.

79 Nationwide SAR Initiative, "Suspicious Activity Reporting Indicators and Examples," revised March 2018, https://www.dhs.gov/sites/default/files/publications/18_0531_NSI_SAR-Indicators-Examples.pdf.

80 American Civil Liberties Union (hereinafter ACLU), "Documents Reveal Lack of Privacy Safeguards and Guidance in Government's 'Suspicious Activity Report' System," October 29, 2013, https://www.aclu.org/sites/default/files/assets/eye_on_fbi_-_sars.pdf.

81 DHS, *Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR)* (hereinafter *ISE Functional Standard*), February 2015, 3, https://www.dhs.gov/sites/default/files/publications/15_0223_NSI_ISE-Functional-Standard-SAR.pdf.

82 DHS, *ISE Functional Standard*, 11; and ACLU, "More About Suspicious Activity Reporting," accessed November 19, 2022, https://www.aclu.org/other/more-about-suspicious-activity-reporting.

83 FBI, "Connecting the Dots"; ACLU, "More About Suspicious Activity Reporting"; and Nusrat Choudhury, "Where's the Suspicion in Government's 'Suspicious Activity' Reports?," ACLU, October 30, 2013, https://www.aclu.org/news/national-security/wheres-suspicion-governments-suspicious-activity.

84 ACLU, "Documents Reveal Lack of Privacy Safeguards"; and email from David Lewis, "Re: The definition of SARs," September 13, 2010, https://www.aclu.org/files/assets/aclueg000394.pdf.

85 Tamara Kessler, *Civil Rights/Civil Liberties Impact Assessment: DHS Support to the National Network of Fusion Centers*, DHS, March 1, 2013, 9, https://www.dhs.gov/sites/default/files/publications/DHS%20Support%20to%20National%20Network_0_0.pdf.

86 ACLU, "Documents Reveal Lack of Privacy Safeguards"; and Julia Harumi Mass, "The Government Is Spying on You: ACLU Releases New Evidence of Overly Broad Surveillance of Everyday Activities," ACLU of Northern California, September 19, 2013, https://www.aclunc.org/blog/government-spying-you-aclu-releases-new-evidence-overly-broad-surveillance-everyday-activities.

87 Open the Government, *The Cost of Fear: Long-Cited Abuses Persist at U.S. Government-Funded Post-9/11 Fusion Centers*, March 26, 2020, https://web.archive.org/web/20220608165512/https://www.openthegovernment.org/dhs-fusion-centers-full-report/.

88 Joel Handley, "Who Do You Protect, Who Do You Surveil?," *In These Times*, April 6, 2015, https://inthesetimes.com/article/who-do-you-protect-who-do-you-surveil.

89 Priscilla M. Regan, Torin Monahan, and Krista Craven, "Constructing the Suspicious: Data Production, Circulation, and Interpretation by DHS Fusion Centers," *Administration & Society* 47, no. 6 (2015): 749, https://publicsurveillance.com/papers/FC_Admin-Society.pdf.

90 *Sixteen Years After 9/11: Assessing Suspicious Activity Reporting Efforts*, *Hearing Before the Subcomm. on Counterterrorism and Intelligence, H. Comm. on Homeland Security*, 115th Cong. (2017) (written testimony of Robin Taylor, acting deputy secretary of intelligence operations, I&A), https://www.dhs.gov/news/2017/09/13/written-testimony-ia-house-homeland-security-subcommittee-counterterrorism-and-0.

91 Eileen A.J. Connelly, "Homeland Security Collected Intel on US Citizens During Portland Protests," *New York Post*, October 2, 2021, https://nypost.com/2021/10/02/dhs-collected-intel-on-us-citizens-during-portland-protests-report; and Salvador Hernandez, "The US Compiled a Secret List of Journalists, Attorneys, and Activists to Question at the Border," BuzzFeed News, March 7, 2019, https://www.buzzfeednews.com/article/salvadorhernandez/government-list-journalists-border-immigration-question.

92 Regan, Monahan, and Craven, "Constructing the Suspicious," 745.

93 *Sixteen Years After 9/11, Hearing Before the H. Comm. on Homeland Security* (2017) (written testimony of Robin Taylor). See also Patel, Levinson-Waldman, and Panduranga, *Course Correction*, 6–7 and accompanying notes.

94 Patel, Levinson-Waldman, and Panduranga, *Course Correction*, 5–7. I&A does conduct an annual audit of fusion centers. This audit relies on self-reported information from fusion centers, however, and tends toward celebrating operational metrics rather than seriously considering the efficacy of fusion centers or their impact on civil rights, civil liberties, and privacy. Thus, while we recommended in our *Course Correction* report that I&A be charged with ensuring that fusion centers have appropriate rules and procedures in place to protect against bias, we conclude that a combination of internal oversight (from the Privacy and CRCL offices) and external oversight (from the special inspector general and the federal oversight office) will be more effective.

95 DHS, *2018 Fusion Centers Final Report*, 1.

96 DHS, "Annual Fusion Center Assessment and Gap Mitigation Activities," last updated December 16, 2021, https://www.dhs.gov/annual-fusion-center-assessment-and-gap-mitigation-activities.

97 Patel, Levinson-Waldman, and Panduranga, *Course Correction*, 6.

98 Permanent Subcomm. on Investigations, *Federal Support for Fusion Centers*, 70.

99 OIG, *Review of Domestic Sharing of Counterterrorism Information*, 42–47.

100 Permanent Subcomm. on Investigations, *Federal Support for Fusion Centers*, 1, 8, 27.

101 Permanent Subcomm. on Investigations, *Federal Support for Fusion Centers*, 1.

102 Permanent Subcomm. on Investigations, *Federal Support for Fusion Centers*, 27.

103 Permanent Subcomm. on Investigations, *Federal Support for Fusion Centers*, 83.

104 Hannah Allam et al., "Red Flags," *Washington Post*, October 31, 2021, https://www.washingtonpost.com/politics/interactive/2021/warnings-jan-6-insurrection/; and Rachael Levy, Dan Frosch, and Sadie Gurman, "Capitol Riot Warnings Weren't Acted On as System Failed," *Wall Street Journal*, February 8, 2021, https://www.wsj.com/articles/capitol-riot-warnings-werent-acted-on-as-system-failed-11612787596.

105 Craig Timberg and Drew Harwell, "Pro-Trump Forums Erupt with Violent Threats Ahead of Wednesday's Rally Against the 2020 Election," *Washington Post*, January 5, 2021, https://www.washingtonpost.com/technology/2021/01/05/parler-telegram-violence-dc-protests; and Erik Dahl, "January 6th Intelligence Failure Timeline," *Just Security*, June 7, 2022, https://www.justsecurity.org/81806/january-6-intelligence-and-warning-timeline.

106 Weihua Li and Jamiles Lartey, "As Murders Spiked, Police Solved About Half in 2020," Marshall Project, January 12, 2022, https://www.themarshallproject.org/2022/01/12/as-murders-spiked-police-solved-about-half-in-2020. The FBI modified the way it collects and presents crime data in 2021 and it warns against year-to-year

comparisons, but previous annual reports consistently indicated violent crime clearance rates of less than 50 percent of violent crimes reported to police. See FBI, *Crime in the United States* (annual publication), DOJ, accessed November 19, 2022, https://www.fbi.gov/services/cjis/ucr/publications. Research also indicates that less than half of violent crimes are reported to police. See, e.g., John Gramlich, "Most Violent and Property Crimes in the U.S. Go Unsolved," Pew Research Center, March 1, 2017, https://www.pewresearch.org/fact-tank/2017/03/01/most-violent-and-property-crimes-in-the-u-s-go-unsolved.

107 See Permanent Subcomm. on Investigations, *Federal Support for Fusion Centers*, 26–60.

108 See, e.g., Cyrus Farivar, "20 Years After 9/11, 'Fusion Centers' Have Done Little to Combat Terrorism," NBC News, September 10, 2021, https://www.nbcnews.com/business/business-news/20-years-after-9-11-fusion-centers-have-done-little-n1278949.

109 Blake Harris, "Chicago Fusion Center Gives Police New Criminal Investigation Tools," *Government Technology*, July 27, 2010, https://www.govtech.com/public-safety/chicago-fusion-center-gives-police-new.html. On the proposition that it is difficult to assess what causes crime rates to decline, see Oliver Roeder, Lauren-Brooke Eisen, and Julia Bowling, *What Caused the Crime Decline?*, Brennan Center for Justice, February 12, 2015, https://www.brennancenter.org/our-work/research-reports/what-caused-crime-decline.

110 Monique Beals, "Chicago's 797 Homicides in 2021 Highest in 25 Years, Most of Any US City," *Hill*, January 1, 2022, https://thehill.com/homenews/state-watch/587891-chicagos-797-homicides-in-2021-highest-in-25-years; and Tom Schuba et al., "As Violent Crime in Chicago Soared, Arrests Fell to Historic Lows," *Chicago Sun-Times*, July 15, 2022, https://chicago.suntimes.com/2022/7/15/23216341/violent-crime-soared-arrests-historic-lows-chicago-police-department-david-brown-lori-lightfoot.

111 Andy Grimm, "Half of Murder Cases Considered 'Solved' by Chicago Police in 2021 Didn't Lead to Charges," *Chicago Sun-Times*, March 31, 2022, https://chicago.suntimes.com/crime/2022/3/31/22996487/cpd-police-department-clearance-murder-solved-rate-david-brown-kim-foxx-prosecutor-charges.

112 Regan, Monahan, and Craven, "Constructing the Suspicious," 741.

113 ACLU, "More About Fusion Centers," accessed November 19, 2022, https://www.aclu.org/other/more-about-fusion-centers.

114 Operation Defuse, "About Fusion Center," accessed November 19, 2022, https://www.operationdefuse.com/about-fusion-center; Lauren Chambers, "Break Up with the BRIC: Unpacking the Boston Regional Intelligence Center Budget," ACLU of Massachusetts, accessed November 19, 2022, https://data.aclum.org/2020/07/22/break-up-with-the-bric-unpacking-the-boston-regional-intelligence-center-budget; and Stop LAPD Spying Coalition, "Shut Down the Spy Centers!," April 12, 2014, https://stoplapdspying.org/shut-down-the-spy-centers.

115 Nick Linder, "Maine Senate Votes to Keep Controversial 'Fusion Center,'" Maine Wire, June 21, 2021, https://www.themainewire.com/2021/06/maine-senate-votes-to-keep-controversial-fusion-center.

116 See, e.g., Michael Price, *National Security and Local Police*, Brennan Center for Justice, December 10, 2013, 39, https://www.brennancenter.org/our-work/research-reports/national-security-and-local-police.

117 The Information Security Oversight Office was established by executive order in 1978 and may provide a useful model. National Archives, "History of the Information Security Oversight Office (ISOO)," accessed November 19, 2022, https://www.archives.gov/isoo/about/history.html.

ABOUT THE AUTHORS

▶ **Michael German** is a fellow with the Brennan Center's Liberty and National Security Program. He served for 16 years as a special agent with the Federal Bureau of Investigation before becoming a civil rights lobbyist with the American Civil Liberties Union. He has taught courses on terrorism and civil liberties at the FBI National Academy, National Defense University, and John Jay College of Criminal Justice. German is the author of *Thinking Like a Terrorist: Insights of a Former FBI Undercover Agent* (2007) and *Disrupt, Discredit, and Divide: How the New FBI Damages Democracy* (2020). He holds a BA from Wake Forest University and a JD from Northwestern University Law School.

▶ **Rachel Levinson-Waldman** is managing director of the Brennan Center's Liberty and National Security Program, where she works to shed light on the government's use of surveillance technologies and authorities and its collection and use of data for law enforcement and intelligence purposes. Levinson-Waldman has authored articles and reports on topics including DHS's counterterrorism initiatives, the government's use of social media, and Fourth Amendment implications of public space surveillance. She has written and provided expert input for publications including the *Guardian*, the *Washington Post*, *Wired*, the *Atlantic*, and the *New Republic*. She holds a BA in religion from Williams College and a JD from the University of Chicago Law School.

▶ **Kaylana Mueller-Hsia** is a Fulbright researcher in Jakarta, where she is studying the use of digital evidence in investigations conducted by Indonesia's National Commission on Human Rights. Previously, she was a research and program associate with the Brennan Center's Liberty and National Security Program. Prior to joining the Brennan Center, Mueller-Hsia served as a technology policy adviser in the mayor's office in San Jose, California, where she advocated for expanding digital access in underserved communities and strengthening municipal privacy protections. She holds a BA from Stanford University.

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.

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.

Many people contributed to the development of this report. The authors are grateful to Faiza Patel, Liza Goitein, Spencer Reynolds, and Kirstin Dunham for their expert insight and feedback, and to Alia Shahzad, José Gutiérrez, Benjamin Waldman, and Marisa Lowe for their research, fact-checking, and proofreading. The authors would also like to thank Michael Waldman and John Kowal for their guidance and support. Julian Brookes, Zachary Laub, Brian Palmer, Janet Romero-Bahari, Stephanie Sykes, and Alden Wallace provided valuable input and prepared this report for publication.

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