

## Intelligence, Law Enforcement, and Homeland Security



Gregory F. Treverton, Senior Policy Analyst  
RAND

This piece was prepared for The Century Foundation's Homeland Security Project. Nothing written here is to be construed as necessarily reflecting the views of The Century Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

In a very real sense, it should not be surprising that cooperation between the CIA and the FBI before September 11 was ragged at best: they were created that way. When President Truman formed the CIA, he worried openly about a “Gestapo-like organization,” and so the CIA was barred from law enforcement and domestic activity. The nation's first investigations of the intelligence, in the 1970s, uncovered abuses of the rights of Americans and responded by suggesting, in effect, that the wall between intelligence and law enforcement be raised. So, the FBI and CIA sit astride the fundamental distinctions of the Cold War—distinctions between intelligence and law enforcement, between foreign and domestic, and between public and private. The distinctions, mostly erected for good, practical, and constitutional reasons, run very deep. They did not serve us badly during the Cold War, but they set us up to fail in an era of terror.

Now, reshaping intelligence and law enforcement means not just reshuffling organizations and refashioning their cultures, it means rethinking basic categories of threat and response. The threat is new for a country whose previous experience with domestic terrorism was low-level, isolated incidents—by Puerto Rican nationalists; anti-Turkish, anti-Israeli or antiabortion groups; environmental extremists; or anarchic outcasts such as the Unabomber or Timothy McVeigh. Creating a new Department of Homeland Security (DHS), and giving it a real capacity for intelligence analysis, is a first step in a long process, but it surely is not the last. This paper elaborates on the distinctions that underlie current arrangements. It then looks in more detail at what kind of intelligence homeland security requires and how an assessment bureau in a new Department of Homeland Security might function. It then turns to the larger and longer-term issues connected with collecting and sharing intelligence “with ourselves”—across the Cold War distinctions—in the continuing process of responding to a changed threat.

### THE COLD WAR DISTINCTIONS

Three of the Cold war distinctions—or “oppositions”—were plainly on display before September 11, but three others, more particular to intelligence, also were present.

The first is *law enforcement versus intelligence*. The two are very different worlds, with different missions, operating codes, and standards. Intelligence, what John Le Carre refers to as “pure intelligence,” is oriented toward the future and toward policy. It seeks to inform the making of policy. It seeks to understand new information in light of its existing understanding of complex situations. It lives in a blizzard of uncertainty where the “truth” will never be known for certain. Thus, its standard is

“good enough for government work,” or, as Pentagon officials might put it, good enough for “T-Lam therapy” —that is, cruise missile attacks. Because intelligence strives above all to protect sources and methods, its officials want desperately to stay out of the chain of evidence so they will not have to testify in court.

By contrast, law enforcement is after the fact. Its business is not policy but prosecution, and its method is cases. It strives to put bad guys in jail. Its standard is high, good enough for a court of law. And law enforcement knows that if it is to make a case, it must be prepared to reveal something of how it knows what it knows; at least it is aware that it will face that choice. It has no real history of analysis; indeed, the meaning of the word “intelligence” is different for law enforcement, where it means “tips” to finding and convicting evil-doers more than a mosaic of understanding. Law enforcement and policing also traditionally have been defined in geographical units. Those definitions are, more and more, mismatched to threats, such as terrorism, that respect no geographical boundaries.

The chasm between law enforcement and intelligence was driven home to me early in the Clinton administration. There was evidence that Iraqi intelligence had plotted to kill former President Bush during his post-presidential visit to Kuwait.<sup>1</sup> In the event, the plot never came close to the president, but the Clinton administration faced a decision about whether to retaliate against Iraq for the attempt. In examining the evidence, the administration put together a team combining CIA intelligence analysts with FBI and Justice Department lawyers. The interaction was fascinating, but it showed just how different intelligence and law enforcement are in mission, operating code, and standards. Evidence that, for intelligence, would have been good enough to unleash “T-Lam therapy” was not good enough for our FBI and Justice Department colleagues, so the team looked again and again at forensic evidence and the “signatures” of bomb makers.

The second opposition is *foreign versus domestic* (which also magnifies the intelligence versus law enforcement distinction). American institutions and practices before and during the Cold War drew a sharp distinction between home and abroad. President Truman’s fretting about a “Gestapo-like” organization when he created the Central Intelligence Agency in 1946–47 is a case in point. A generation later, in the mid-1970s, Congress’s first-ever inquiry into intelligence, the Senate Select Committee on Intelligence Activities, headed by then-Senator Frank Church (D-Idaho), investigated abuses of the rights of Americans. The most serious of those abuses, which included the harassing of Martin Luther King along with many American religious and political groups, had emerged from COINTELPRO, a curious mixing by the FBI of law enforcement and intelligence ostensibly for domestic counterintelligence purposes. The Congress’s response was to *raise* the walls between intelligence and law enforcement—for instance, by creating a special court, the Federal Intelligence and Surveillance Court (FISC), to review applications for national security, as opposed to law enforcement, wiretaps and surveillance.

In the 1970s, it was literally true that the directors of the CIA and FBI did not speak to one another. That state of affairs has improved—it hardly could have gotten worse—but still, relations between the two, in handing off spies from one agency to the other, have been ragged. The National Security Agency (NSA) too is barred from law enforcement and from domestic spying, so if the trail of conversations becomes “domestic” —that is, involves a U.S. citizen, corporation, or even resident alien—the trail must end.

These oppositions also have shaped the U.S. military, as it is dominated by foreign and *not* law enforcement concerns. World War II and the Cold War made the military very much “abroad,” very “external” in a way that was different from the interwar period when “domestic” operations, such as

---

<sup>1</sup> See reportage in the *Washington Post*, July 1, 1993, p. A18; and June 29, 1993, p. A14. Philip Heymann, who as deputy attorney general was a participant in the episode, describes it in his elegant and sensible book, *Terrorism and America: A Commonsense Strategy for a Democratic Society* (Cambridge, Mass.: MIT Press, 1998), p. 71ff.

those of the Army Corps of Engineers, were much more visible. *Posse comitatus*, or the ban on military involvement in law enforcement, was a legacy of the military's role in the American West. This could change as a result of a more direct military role in homeland security, including the creation of a Northern Command (NORTHCOM), the new joint command charged with homeland security.

The third opposition is *public versus private*. During the Cold War, national security was a government—federal government—monopoly. To be sure, private companies and citizens played a role, but for most citizens, fighting the Cold War simply meant paying their taxes. That does not seem likely to be so for the campaign against terrorism and for homeland security. Safeguarding critical infrastructures, such as communications or electric power, from terrorist attack means protecting public goods that are mostly in private hands. Across the country, there are three times as many “police” in the private sector as in governments. Thus, private companies will be drawn more deeply into fighting terrorism than they were into fighting communism. The lives of private citizens also will be affected more deeply by antiterrorism efforts, in ways that will range from the inconvenience of waiting in long lines imposed by security procedures at airports to harder questions about whether they will carry national identity cards or let their biometric identifications be taken for special advance screenings as “trusted fliers.”

All three of these oppositions were all too vividly on display in the failure to anticipate September 11. An August 23 CIA cable warned of two bin Laden associates who had entered the United States and two others who were expected to attempt entry. Apparently, the FBI did little with the information and also failed to share it with the Immigration and Naturalization Service (INS) until the INS already had admitted other two into the country. Questioned about its failure to follow up on this cable, one FBI official said, “If the cable says, ‘Don’t let them in the country, and they were already in the country, what’s the point of bringing this up now?’” In any event, the FBI failed to locate Khalid Almihdhar and Nawaf Alhazmi, who hijacked the jet that crashed into the Pentagon on September 11.<sup>2</sup>

A State Department official testified that the FBI had refused for a decade to provide the INS with access to its National Crime Information Center Database, on the argument that the INS is not a “law enforcement” organization. Nevertheless, an internal FBI review concluded that “everything was done that could have been done” to prevent September 11.<sup>3</sup> Before September 11, the “standard FBI line” according to one source who spoke to the *New Yorker* writer Joe Klein was that “Osama bin Laden wasn’t a serious domestic security threat,” presumably because his earlier attacks had been abroad, not at home.<sup>4</sup>

No agency told the Federal Aviation Administration (FAA) to be on the lookout for the four men, apparently because it too was not in the law enforcement business. And the airlines were not informed because they were private, not public. A European official testified to the effect that the United States was not alone in having such oppositions: “those we have been arresting are people we knew about before [September 11] but never thought were particularly dangerous to us inside our national boundaries.”<sup>5</sup>

Meanwhile, the suspected “twentieth hijacker,” Zacarias Moussaoui, had been arrested on August 16 in Minneapolis for a visa violation. FBI agents at the field office suspected him of terrorism and sought, increasingly desperately, to search his laptop computer. They were frustrated in a debate with

---

<sup>2</sup> The saga of what the two agencies told each other and when was played out in leaks and counter leaks. See Walter Pincus and Don Eggen, “CIA Gave FBI Warning on Hijacker,” *Washington Post*, June 4, 2002, p. A1.

<sup>3</sup> Bob Drogin, Eric Lichtblau, and Greg Krikorian, “CIA, FBI Disagree on Urgency of Warning,” *Los Angeles Times*, October 18, 2001.

<sup>4</sup> Joe Klein, “Closework: Why We Couldn’t See What Was Right in Front of Us,” *The New Yorker*, October 1, 2001, pp. 44-49.

<sup>5</sup> <http://specials.ft.com/attackonterrorism/index.html>

headquarters about one of those walls between intelligence and law enforcement that had been raised during the 1970s, the FISC.

Before the FISC, presidents had claimed the prerogative of warrantless searches for national security purposes. In a compromise between presidential discretion and civil liberties, the FISC created a special secret court in Washington to review requests for covert national security wiretaps and searches by the FBI and the NSA. By the FISC standard, however, the “primary purpose” of any search had to be a suspected connection to a foreign power, and the FBI offices disagreed on whether Moussaoui met that standard. The debate continued through September 11.<sup>6</sup>

The impact of the other three oppositions more particular to intelligence also can be seen in the run-up to September 11. The first is that between open sources and secrets. Cold War intelligence, focused on a secretive Soviet Union, gave pride of place to secrets and secret sources. Intelligence still does. Yet the world is much more open, with torrents of information. Yet that information, unlike the secrets from spies or spy satellites, is neither “owned” by intelligence nor can it be regarded as reliable; it is a stew of fact, fiction, and disinformation. To be sure, terrorists do not advertise their plans, nor do they have informative websites, and so traditional intelligence methods are very much relevant. But so are open sources. The *Los Angeles Times*, for instance, reported that a simple check of public records and addresses through the California Department of Motor Vehicles would have disclosed the correct location for the two hijackers who were the subject of the August 23 cable. A check with credit card companies would have shown air ticket purchases and provided valid addresses.<sup>7</sup>

A fifth distinction, between analyst and collector, has direct bearing on the future of intelligence sharing, across the federal government and between it and states and localities. During the Cold War, given the reliance on technical and secret sources, the distinction made sense. Collectors could pass their take to analysts, who would assemble the various sources. Sharing concentrated on collection, of espionage, signals, or imagery. Now, though, in the world of too much, too unreliable information, the best “collector” is an expert on substance—an “analyst.” He or she knows what might be a signal in a storm of noise. Future sharing thus will need to involve analysts, not just or primarily collectors.

The final Cold War distinction separated intelligence from policy. More than other countries, the United States drew a bright white line between the two. The justification, which made considerable sense during the Cold War, was that if intelligence got too close to the stakes and biases of policy officials, its objectivity would be compromised. Intelligence would become “politicized.” The concern remains a fair one, but if the tragic saga of September 11 shows anything, it demonstrates that intelligence needs to be close to, indeed intertwined with, those responsible for policy and operations.

## THE INTELLIGENCE OF HOMELAND SECURITY

The Bush administration’s proposal to turn the Office of Homeland Security into a full-fledged department, with its own intelligence analysis capacity, displayed both the strength of these oppositions and the need to rethink them. Because terrorism at home is new terrain for the nation, it will take us time to work through the implications of the changed threat. In terms of organization, if the United States now were starting from scratch, it would never recreate the existing intelligence or law enforcement structures. Establishing a Department of Homeland Security (DHS) is a good first step, but there surely is no magic organizational solution.

In the original administration proposal, the intelligence analysis unit was to be separated from collection, neither receiving raw intelligence nor tasking collectors. However, those restrictions would make the new office hostage to the conclusions that other agencies chose to share with it. Rather, if the intelligence capacity is to be a serious one, it will need authority both to receive raw intelligence and to

---

<sup>6</sup> Philip Shenon, “Traces of Terror: The Terror Suspect,” *New York Times*, July 7, 2002, p. A24.

<sup>7</sup> Drogin, et al., “CIA, FBI Disagree.”

task the intelligence collectors. It will need access to foreign intelligence and to the domestic material that emerges from law enforcement. It would not be simply a departmental intelligence operation like the State Department's Bureau of Intelligence and Research (INR); rather, it also would serve the broader set of officials, especially in the White House office, whose mandate is homeland security. And if it were to be effective in warning, it would need to be tightly connected to a range of policymakers, not just the federal officials who issued the warning but also the state and local (and private) people who interpreted it.

It will need to be focused on terrorism and oriented domestically. Of current institutions, the CIA and intelligence's Counterterrorism Center, which is located at the CIA, are, for legal reasons, aimed mostly abroad. Operators, not analysts, have dominated the center. At present, remarkably, no agency systematically reviews domestic information for intelligence and warning purposes as opposed to law enforcement; the FBI has expressed only the intention to begin doing so. While FBI Director Robert Mueller's initiative seeks to change this, the FBI really has not done intelligence. As he put it, the bureau collects a lot of information but seldom puts it together.

The DHS intelligence capacity would link intelligence tightly to warning. Getting warning too close to operations was a concern after the bombing of Pearl Harbor in 1941, but seems the right approach now. In the run-up to Pearl Harbor, Army and Navy intelligence had, apparently, been reluctant to sound the tocsin based on what was inevitably "iffy" evidence of an impending Japanese attack. They were close to their operational colleagues and thus knew that it was a costly nuisance for those operators to act on warning—for instance, putting the fleet to sea—if the warning turned out to be a false alarm.<sup>8</sup> The concern is fair, but now the warners (at the CIA, for instance) are so disconnected from those who must act that they are tempted to overwarn—a temptation in evidence this past summer. Moreover, the new assessment capacity will have lots of competition around town, hence lots of checks should its assessments appear to be tailored to suit the convenience of DHS operators.

Governor Tom Ridge, as director of the Office of Homeland Security, instituted a color-coded chart of national warning, ranging from green through blue, yellow, and orange, to red. The idea is based on twenty years of experience in Britain. It is a good one, but the United States lacks Britain's experience, so no one—not state and local officials, much less private citizens—knows yet what the colors mean. Ideally, information should flow in both directions, not just from the intelligence community to the homeland security department and thence to the country, but in the other direction as well. There are lots of eyes and ears out there in this country. The new assessment capacity will have neither mandate nor staff to routinely get information from state and local authorities—that will remain, apparently, mostly an FBI function—but it will provide incentive in the form of an eager consumer. This, plus the tight link to warning will give it some chance to make the warning system mean something to local officials, even in time to ordinary citizens.

The new unit also could provide additional incentive for the CIA and the FBI to communicate, in the form of another set of eyes looking at, and to, both, and trying to integrate information from both. It hardly would be decisive in producing easier communication between the two main agencies—there is too much history, not to mention constitutional concern. But the new intelligence unit would be a customer with a direct stake in the intersection of the information and analysis produced by the two. And even if the new assessment unit were slow to carve out a standing, it still would be, as Governor Ridge put it, another set of eyes. After all, analysts are inexpensive by comparison to sophisticated collection.

The assessment bureau will face formidable immediate challenges. It will start out being weak, with no leadership, reputation, or regular seat at any table. It will be very dependent on the success of the

---

<sup>8</sup> The classic study of the failure of warning at Pearl Harbor is Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford: Stanford University Press, 1962).

larger department. If the DHS remains weak, its intelligence arm cannot be much more than another set of eyes, ones mostly looking in the wilderness. It might be observed, however, that the CIA, too, started out with little and quickly became an important player. But the CIA had not only wartime veterans and reputation, it also inherited an operations mission.

If it is to be more than a departmental intelligence arm, like INR, the new unit would need to be a kind of “domestic CIA” —or, more appropriately, a “domestic DI,” the CIA’s Directorate of Intelligence. Not only will it need budget to match that scale, it would need staff, which will not be easy to come by. Apparently, the intention is to build the new unit out of the Department of Energy intelligence organization. That has been a relatively serious one among the smaller intelligence units in town, and it has benefited from connections to the DOE laboratories. But it does not have much standing beyond issues of DOE concern, and so its overlap with the mission of the new assessment staff is quite partial—mostly in the area of weapons of mass destruction.

Ideally, the new unit will cast a wide net, looking not just for card-carrying intelligence analysts but for people with experience in terrorism and law enforcement, as well as those, like analysts at the Southern Poverty Law Center, who have experience at following hate groups, militias, and religious extremists. The wider the net is cast, unfortunately, the more difficult and slower it will be to bring in analysts and, especially, get them the requisite security clearances. In time, the new unit might become a leader in establishing new ways of sharing information across the distinction between open and secret. In the short run, though, it will have to earn its spurs with fellow intelligence agencies and so be the cleanest of the clean when it comes to handling classified documents.

What information sources will it have? On the “foreign” side of the distinction, it will need both “finished” and “raw” intelligence, just as do CIA analysts (like them, of course, it does not need to know the identities of secret sources). The big technical collectors—the National Security Agency (NSA) for signals and the National Imagery and Mapping Agency (NIMA) for imagery—should not be a problem because they are in the service business, generally on the prowl for consumers. How much of value the two, and especially the NSA, can provide with respect to the new unit’s domestic orientation will depend on decisions about what those agencies can and cannot collect. For the CIA and Counterterrorism Center, the new colleague will look to some extent like a rival, especially as its mission and customers expand. The rivalry, though, might be muted by the new unit’s focus on here, rather than abroad, which is terrain that is both unfamiliar and risky for the “foreign” intelligence agencies. It should benefit from the sponsorship not just of the White House homeland security director but also from that of the National Security Council (NSC); indeed, the NSC counterterrorism and infrastructure protection operations will be tempted to regard it as *their* staff.

The new unit is intended to play an important role in assessing vulnerability, especially that of America’s information and other infrastructures. In this respect, too, it will be breaking new terrain, for it will be a major contributor to “net assessments” of vulnerability. This means that it will need to work closely with both the government’s infrastructure protection operations—in the White House, Commerce Department, and FBI—and with the private-sector managers of the infrastructures. It also will be handling what are the nation’s most important secrets; knowing what is vulnerable would be a roadmap for would-be terrorists. And while it will work with other agencies and with corporations, it will need technical capacity of its own, in order to make sense of intelligence about terrorist capabilities that would be relevant to a net assessment of vulnerability.

In many respects, its key connection will be with the FBI and information from law enforcement activities. The FBI is likely to view the new unit, not to mention the new department, as an intruder, all the more so given Mueller’s intention to reshape the bureau away from law enforcement and toward intelligence and prevention. In this area, both its legal mandate and its relations with collectors could be problematic. Its challenge will be to fuse information across the “foreign” and “domestic” distinction. For it, the two domains should be a seamless web. So it will need access to federal grand

jury proceedings, other FBI case materials, and the like, as well as any NSA take collected under law enforcement mandates or through FISC warrants. That will run straight into the Cold War distinctions—foreign versus domestic, and intelligence versus law enforcement.

It thus remains to be seen how much information from law enforcement the new unit can receive and how useful that information will be, but it should be considerable. Over time, moreover, the DHS and its intelligence unit will develop their own connections to domestic law enforcement and kindred groups. Surfing the Internet for open source information also will be fruitful, as existing groups monitoring hate and other extremist groups have demonstrated.

If the unit succeeds at all, it will want to become a serious player, with “publications” of its own. These will add to the flood of information in Washington, and that fact will be decried by Congress as duplication. But one person’s duplication is another’s tailoring for specific purposes. The new operation will have a focus and set of consumers. And September 11 drove home how many more signals there are out there than the current system has the capacity to sort out. So, within broad limits, more analysis is preferable to less.<sup>9</sup>

### SHARING INTELLIGENCE WITH OURSELVES

The challenge of intelligence cooperation among ourselves in the war on terrorism is indeed formidable. Not only are there, by one count, 18,000 governmental entities involved, but there are many more if private players are added, not just corporations but nongovernmental organizations (NGOs) as well. And, egads, almost none of them have security clearances! Thus far, intelligence sharing has been pretty haphazard. After September 11, it turned out that there was information about possible nuclear threats to New York, information that no part of the federal government troubled to share with New York officials. At the other extreme, California’s governor interpreted very skimpy information about threats to the state’s bridges as a reason for public announcement and stepped-up protection.<sup>10</sup>

Intelligence and law enforcement do have experience in sharing intelligence, both at home and abroad, and the mechanisms that have been developed are suggestive for new innovations. They seek, like the warning color chart, to diminish the burden of classified information, to sanitize that information so as not to reveal the source, to bring outsiders into the circle of cleared recipients, at least for some period, or to do all three in various combinations:

- *NSA Critic system.* This system was developed decades ago to enable time-sensitive national security information (for instance, the outbreak of war) to reach presidents and other national security decisionmakers within ten minutes. It was developed with NSA mostly because the agency had the sophisticated technology to make it possible.
- *NATO tear lines.* The U.S. military is quite creative in sanitizing intelligence to be shared with coalition partners. Sensitive traffic comes in a message with a “tear line”: the information is shared with coalition partners, while the source identification is ripped off. In mid-2002, Congress considered legislation to make it easier for intelligence agencies to strip classified material from information that might then be shared with state and local officials—emulating

---

<sup>9</sup> This is a point The Century Foundation (formerly the Twentieth Century Fund) has made before. See *In From the Cold: The Report of the Twentieth Century Fund Task Force on the Future of U.S. Intelligence* (New York: Twentieth Century Fund Press, 1996).

<sup>10</sup> *Time* broke the New York story; see Massimo Calabresi and Romesh Ratnesar, “Can We Stop the Next Attack?” *Time*, March 11, 2002, p. 24. For an account of the California bridges episodes, see “Davis Reveals Warning of Attacks on Bridges: Blasted for ‘Overreacting’—Security Boost on 4 State Spans,” *San Francisco Chronicle*, November 2, 2001, p. A1.

the practice with allies in contingency operations or with the international police agency, Interpol.<sup>11</sup>

- *Civil applications committee*. This mechanism was developed to share satellite and other technical intelligence data with civil environmental agencies. It relies on bringing in outsiders, people with relevant experience and with enough standing in communities outside intelligence, to vouch for the value of what is being transferred.
- *Sharing signals intelligence (SIGINT)*. The sharing of this data and analysis is much richer and more symmetrical than is the case for imagery. Sharing imagery is affected by the “it was invented here” syndrome, while in signals the cooperation runs back not just to Anglo-American code-breaking at Bletchley Park but also to Australians breaking Japanese codes in support of U.S. forces.
- *FBI task forces*. The FBI routinely organizes task forces with state and local law enforcement officials to pursue joint operations, for instance against organized crime, drug traffickers, or gangs. The local officers work as full partners of the FBI. The rub is that to do so, they need to be cleared to the same level as FBI agents, which is Top Secret (though the clearance process is often expedited).

The implications of the changed threat run well beyond organization, to what is collected, by whom, and under what restrictions—very sensitive issues of domestic intelligence gathering. The September 11 terrorists not only trained in Afghanistan, they also used European cities such as Hamburg, Germany, and Brixton, England, as staging areas where they could live, train, and recruit in a protective environment. Similarly, they mixed easily in some areas of the United States, south Florida, and southern California. The nation’s need is not just to follow individuals, it is also to know what is being said on the streets and in the mosques of Brixton or Boston—it is doing at home what has heretofore been considered “foreign” intelligence.

The terrorist threat takes us back to just the thicket that investigations of intelligence worried about a generation ago. Then, the investigations led to higher walls between intelligence and law enforcement—the FISC, for instance. Reportedly, the FISC has turned down just one Justice Department request for authority, out of 12,000.<sup>12</sup> To critics, that is taken as a lack of oversight. To supporters, it suggests that the requirement of the court has made federal officials very careful in screening and preparing their requests, perhaps even too careful. The interplay in the summer of 2001 between FBI headquarters and the bureau’s field office in Minneapolis can be taken as one of excessive caution by headquarters in refusing the field office’s request for more investigation of Moussaoui.

After September 11, intelligence and law enforcement have been pushed toward each other, yet how far remains controversial. The USA PATRIOT Act of November 2001, for instance, began to facilitate the sharing with ourselves by making it easier to move information across the organizational distinctions, especially that dividing intelligence from law enforcement. Before the law was enacted, any information that was before a federal grand jury could be shared with CIA analysts *only* with a court order. Thus, analysts might be denied access to information that was a critical puzzle piece in their effort to understand terrorist networks. Now, that information can be shared more easily. The act also loosened the FISC standard to permit covert searches if investigating the suspicion of a foreign connection was a “secondary purpose.” The new law updated wiretapping authority to cope with a world of multiple, mobile cell phones, not just static, analog phones. In the summer of 2002, Mueller relaxed rules that had restricted FBI agents from activities that are permitted to ordinary citizens, such as surfing the Internet or visiting churches and similar public places of interest.

---

<sup>11</sup> Juliet Eilperin and Bill Miller, “House Approves Intelligence-Sharing Bill,” *Washington Post*, June 27, 2002.

<sup>12</sup> See <http://fly.hiwaay.net/~pspoole/fiscshort.html>.

Going further to shift the culture of the FBI from law enforcement to prevention, as Mueller has called for, is a dramatic change—so dramatic that it may not be wise. In any case, it is the work of a generation, not a couple of years. Ultimately, if we require not just good law enforcement but good domestic intelligence, can the FBI do both? Former national security adviser Brent Scowcroft has suggested creating a separate career track in the bureau for intelligence—a call that fell on stony ground. By tradition, law enforcement has been the bureau’s dominant mission, and its internal pecking order has been dominated by special-agents-in-charge. Should the FBI be split into two agencies, one for law enforcement and the other for domestic intelligence?

If domestic intelligence is now an urgent need, should we create not just a Department of Homeland Security, but a home office—our version of MI-5, the British domestic intelligence service—as several members of Congress have suggested? Creating a new service would not solve the turf disputes born of overlapping missions—MI-5 and Britain’s preeminent law enforcement agency, Scotland Yard, disputed for years over which one would take the lead in dealing with the IRA terrorist threat to England. But, somewhat paradoxically, a separate U.S. domestic service might make for clearer lines of accountability than would leaving domestic intelligence as the stepchild in a reshaped FBI.

And if domestic intelligence means not just tracking suspected terrorists but also monitoring the chatter in the mosques of Chicago or the strip malls of south Florida, how much are we prepared to run the risk that rights of Americans, let alone non-Americans (who have far fewer rights), will be compromised? Finally, in the other direction, how does the public provide warning? Do people call local authorities, visit websites, or offer anonymous tips? Should there be penalties for false calls or for tips that turn out to be score settling? How should feedback be handled? Local authorities now complain routinely that they never hear what happens with information they provide to the FBI. In coming to grips with these questions, the creation of a department of homeland security, with an intelligence capacity to match, provides a beginning, but just a bare beginning.

August 21, 2002

---

Gregory F. Treverton, now at RAND, was vice chair of the National Intelligence Council during the first Clinton administration. His *Reshaping Intelligence for an Age of Information*, which was sponsored by The Century Foundation, was published last year by Cambridge University Press.

All of the publications for this project, along with additional Homeland Security information are available at <http://www.homelandsec.org>.

For more information please contact Tina Doody at 212-452-7750 or [doody@tcf.org](mailto:doody@tcf.org).