

# The Secret Government Rulebook For Labeling You a Terrorist

By [Jeremy Scahill](#) and [Ryan Devereaux](#) 23 Jul 2014, 2:45 PM EDT [625](#)

The Obama administration has quietly approved a substantial expansion of the terrorist watchlist system, authorizing a secret process that requires neither “concrete facts” nor “irrefutable evidence” to designate an American or foreigner as a terrorist, according to a key government document obtained by *The Intercept*.

The “March 2013 Watchlisting Guidance,” a [166-page document](#) issued last year by the National Counterterrorism Center, spells out the government’s secret rules for putting individuals on its main terrorist database, as well as the no fly list and the selectee list, which triggers enhanced screening at airports and border crossings. The new guidelines allow individuals to be designated as representatives of terror organizations without any evidence they are actually connected to such organizations, and it gives a single White House official the unilateral authority to place entire “categories” of people the government is tracking onto the no fly and selectee lists. It broadens the authority of government officials to “nominate” people to the watchlists based on what is vaguely described as “fragmentary information.” It also allows for dead people to be watchlisted.

Over the years, the Obama and Bush Administrations have fiercely resisted disclosing the criteria for placing names on the databases—though the guidelines are officially labeled as unclassified. In May, Attorney General Eric Holder even invoked the state secrets privilege to prevent watchlisting guidelines from being disclosed in litigation launched by an American who was on the no fly list. In [an affidavit](#), Holder called them a “clear roadmap” to the government’s terrorist-tracking apparatus, adding: “The Watchlisting Guidance, although unclassified, contains national security information that, if disclosed ... could cause significant harm to national security.”

The rulebook, which *The Intercept* is publishing in full, was developed behind closed doors by representatives of the nation’s intelligence, military, and law-enforcement establishment, including the Pentagon, CIA, NSA, and FBI. Emblazoned with the crests of 19 agencies, it offers the most complete and revealing look into the secret history of the government’s terror list policies to date. It reveals a confounding and convoluted system filled with exceptions to its own rules, and it relies on the elastic concept of “reasonable suspicion” as a standard for determining whether someone is a possible threat. Because the government tracks “suspected terrorists” as well as “known terrorists,” individuals can be watchlisted if they are suspected of being a suspected terrorist, or if they are suspected of associating with people who are suspected of terrorism activity.

“Instead of a watchlist limited to actual, known terrorists, the government has built a vast system based on the unproven and flawed premise that it can predict if a person will commit a terrorist act in the future,” says Hina Shamsi, the head of the ACLU’s National Security Project. “On that dangerous theory, the government is secretly blacklisting people as suspected terrorists and

giving them the impossible task of proving themselves innocent of a threat they haven't carried out." Shamsi, who reviewed the document, added, "These criteria should never have been kept secret."

The document's definition of "terrorist" activity [includes](#) actions that fall far short of bombing or hijacking. In addition to expected crimes, such as assassination or hostage-taking, the guidelines also define destruction of government property and damaging computers used by financial institutions as activities meriting placement on a list. They also define as terrorism any act that is "[dangerous](#)" to property and intended to influence government policy through intimidation.

This combination—a broad definition of what constitutes terrorism and a low threshold for designating someone a terrorist—opens the way to ensnaring innocent people in secret government dragnets. It can also be counterproductive. When resources are devoted to tracking people who are not genuine risks to national security, the actual threats get fewer resources—and might go unnoticed.

"If reasonable suspicion is the only standard you need to label somebody, then it's a slippery slope we're sliding down here, because then you can label anybody anything," says David Gomez, a former senior FBI special agent with experience running high-profile terrorism investigations. "Because you appear on a telephone list of somebody doesn't make you a terrorist. That's the kind of information that gets put in there."

The fallout is personal too. There are severe consequences for people unfairly labeled a terrorist by the U.S. government, which shares its watchlist data with local law enforcement, foreign governments, and "private entities." Once the U.S. government secretly labels you a terrorist or terrorist suspect, other institutions tend to treat you as one. It can become difficult to get a job (or simply to stay out of jail). It can become burdensome—or impossible—to travel. And routine encounters with law enforcement can turn into ordeals.

In 2012 Tim Healy, the former director of the FBI's Terrorist Screening Center, [described](#) to CBS News how watchlists are used by police officers. "So if you are speeding, you get pulled over, they'll query that name," he said. "And if they are encountering a known or suspected terrorist, it will pop up and say call the Terrorist Screening Center.... So now the officer on the street knows he may be dealing with a known or suspected terrorist." Of course, the problem is that the "known or suspected terrorist" might just be an ordinary citizen who should not be treated as a menace to public safety.

Until 2001, the government did not prioritize building a watchlist system. On 9/11, the government's list of people barred from flying included just 16 names. Today, the no fly list has swelled to tens of thousands of "known or suspected terrorists" (the guidelines refer to them as KSTs). The selectee list subjects people to extra scrutiny and questioning at airports and border crossings. The government has created several other databases, too. The largest is the Terrorist Identities Datamart Environment (TIDE), which gathers terrorism information from sensitive military and intelligence sources around the world. Because it contains classified information that cannot be widely distributed, there is yet another list, the Terrorist Screening Database, or TSDB, which has been stripped of TIDE's classified data so that it can be shared. When

government officials refer to “the watchlist,” they are typically referring to the TSDB. (TIDE is the responsibility of the National Counterterrorism Center; the TSDB is managed by the Terrorist Screening Center at the FBI.)

In a statement, a spokesman for the National Counterterrorism Center told *The Intercept* that “the watchlisting system is an important part of our layered defense to protect the United States against future terrorist attacks” and that “watchlisting continues to mature to meet an evolving, diffuse threat.” He added that U.S. citizens are afforded extra protections to guard against improper listing, and that no one can be placed on a list solely for activities protected by the First Amendment. A representative of the Terrorist Screening Center did not respond to a request for comment.

The system has been criticized for years. In 2004, Sen. Ted Kennedy [complained](#) that he was barred from boarding flights on five separate occasions because his name resembled the alias of a suspected terrorist. Two years later, CBS News [obtained](#) a copy of the no fly list and reported that it included Bolivian president Evo Morales and Lebanese parliament head Nabih Berri. One of the watchlists snared Mikey Hicks, [a Cub Scout](#) who got his first of many airport pat-downs at age two. In 2007, the Justice Department’s inspector general issued a scathing report identifying “[significant weaknesses](#)” in the system. And in 2009, after a Nigerian terrorist was able to board a passenger flight to Detroit and nearly detonated a bomb sewn into his underwear despite his name having been placed on the TIDE list, President Obama admitted that there had been a “[systemic failure](#).”

Obama hoped that his response to the “underwear bomber” would be a turning point. In 2010, he gave increased powers and responsibilities to the agencies that nominate individuals to the lists, placing pressure on them to add names. His administration also issued a set of new guidelines for the watchlists. Problems persisted, however. In 2012, the U.S. Government Accountability Office [published](#) a report that bluntly noted there was no agency responsible for figuring out “whether watchlist-related screening or vetting is achieving intended results.” The guidelines were revised and expanded in 2013—and a source within the intelligence community subsequently provided a copy to *The Intercept*.

**1.59 Expedited Nomination Procedures for Temporary, Threat-Based Categories.** This provision is intended to enable categories of individuals to be temporarily upgraded in watchlist status based on current and credible intelligence information or a particular threat stream that indicates a certain category of individuals may be used to conduct an act of domestic or international TERRORISM. This temporary, threat-based expedited upgrade (TBU) is made at the direction of the Assistant to the President for Homeland Security and Counterterrorism or his/her designee (Appropriate Official) and should be narrowly tailored to address the threat.

## “Concrete facts are not necessary”

The five chapters and 11 appendices of the “Watchlisting Guidance” are filled with acronyms, legal citations, and numbered paragraphs; it reads like an arcane textbook with a vocabulary all its own. Different types of data on suspected terrorists are referred to as “derogatory

information,” “substantive derogatory information,” “extreme derogatory information” and “particularized derogatory information.” The names of suspected terrorists are passed along a bureaucratic ecosystem of “originators,” “nominators,” “aggregators,” “screeners,” and “encountering agencies.” And “upgrade,” usually a happy word for travellers, is repurposed to mean that an individual has been placed on a more restrictive list.

The heart of the document revolves around the rules for placing individuals on a watchlist. “All executive departments and agencies,” the document says, are responsible for collecting and sharing information on terrorist suspects with the National Counterterrorism Center. It sets a low standard—“[reasonable suspicion](#)”—for placing names on the watchlists, and offers a multitude of vague, confusing, or contradictory instructions for gauging it. In the chapter on “Minimum Substantive Derogatory Criteria”—even the title is hard to digest—the key sentence on reasonable suspicion offers little clarity:

“To meet the REASONABLE SUSPICION standard, the NOMINATOR, based on the totality of the circumstances, must rely upon articulable intelligence or information which, taken together with rational inferences from those facts, reasonably warrants a determination that an individual is known or suspected to be or has been knowingly engaged in conduct constituting, in preparation for, in aid of, or related to TERRORISM and/or TERRORIST ACTIVITIES.”

The rulebook makes no effort to define an essential phrase in the passage—“articulable intelligence or information.” After stressing that hunches are not reasonable suspicion and that “there must be an objective factual basis” for labeling someone a terrorist, it goes on to state that no actual facts are required:

“In determining whether a REASONABLE SUSPICION exists, due weight should be given to the specific reasonable inferences that a NOMINATOR is entitled to draw from the facts in light of his/her experience and not on unfounded suspicions or hunches. Although irrefutable evidence or concrete facts are not necessary, to be reasonable, suspicion should be as clear and as fully developed as circumstances permit.”

While the guidelines nominally prohibit nominations based on unreliable information, they explicitly regard “uncorroborated” Facebook or Twitter posts as sufficient grounds for putting an individual on one of the watchlists. “Single source information,” the [guidelines state](#), “including but not limited to ‘walk-in,’ ‘write-in,’ or postings on social media sites, however, should not automatically be discounted ... the NOMINATING AGENCY should evaluate the credibility of the source, as well as the nature and specificity of the information, and nominate even if that source is uncorroborated.”

There are a number of [loopholes](#) for putting people onto the watchlists even if reasonable suspicion cannot be met.

One is clearly defined: The immediate family of suspected terrorists—their spouses, children, parents, or siblings—may be watchlisted without any suspicion that they themselves are engaged in terrorist activity. But another loophole is quite broad—“associates” who have a defined relationship with a suspected terrorist, but whose involvement in terrorist activity is not known.

A third loophole is broader still—individuals with “a possible nexus” to terrorism, but for whom there is not enough “derogatory information” to meet the reasonable suspicion standard.

Americans and foreigners can be nominated for the watchlists if they are associated with a terrorist group, even if that group has not been designated as a terrorist organization by the U.S. government. They can also be treated as “representatives” of a terrorist group even if they have “neither membership in nor association with the organization.” The guidelines do helpfully note that certain associations, such as providing janitorial services or delivering packages, are not grounds for being watchlisted.

The nomination system appears to lack meaningful checks and balances. Although government officials have repeatedly said there is a rigorous process for making sure no one is unfairly placed in the databases, the guidelines acknowledge that all nominations of “known terrorists” are considered justified unless the National Counterterrorism Center has evidence to the contrary. In a recent [court filing](#), the government [disclosed](#) that there were 468,749 KST nominations in 2013, of which only 4,915 were rejected—a rate of about one percent. The rulebook appears to invert the legal principle of due process, defining nominations as [“presumptively valid.”](#)

## Profiling categories of people

While the nomination process appears methodical on paper, in practice there is a shortcut around the entire system. Known as a [“threat-based expedited upgrade,”](#) it gives a single White House official the unilateral authority to elevate entire “categories of people” whose names appear in the larger databases onto the no fly or selectee lists. This can occur, the guidelines state, when there is a “particular threat stream” indicating that a certain type of individual may commit a terrorist act.

This extraordinary power for “categorical watchlisting”—otherwise known as profiling—is vested in the assistant to the president for homeland security and counterterrorism, a position formerly held by CIA Director John Brennan that does not require Senate confirmation.

The rulebook does not indicate what “categories of people” have been subjected to threat-based upgrades. It is not clear, for example, whether a category might be as broad as military-age males from Yemen. The guidelines do make clear that American citizens and green card holders are subject to such upgrades, though government officials are required to review their status in an “expedited” procedure. Upgrades can remain in effect for 72 hours before being reviewed by a small committee of senior officials. If approved, they can remain in place for 30 days before a renewal is required, and can continue “until the threat no longer exists.”

“In a set of watchlisting criteria riddled with exceptions that swallow rules, this exception is perhaps the most expansive and certainly one of the most troubling,” Shamsi, the ACLU attorney, says. “It’s reminiscent of the Bush administration’s heavily criticized color-coded threat alerts, except that here, bureaucrats can exercise virtually standard-less authority in secret with specific negative consequences for entire categories of people.”

The National Counterterrorism Center declined to provide any details on the upgrade authority, including how often it has been exercised and for what categories of people.

## Pocket litter and scuba gear

The guidelines provide the clearest explanation yet of what is happening when Americans and foreigners are pulled aside at airports and border crossings by government agents. The fifth chapter, titled “[Encounter Management and Analysis](#),” details the type of information that is targeted for collection during “encounters” with people on the watchlists, as well as the different organizations that should collect the data. The Department of Homeland Security is described as having the largest number of encounters, but other authorities, ranging from the State Department and Coast Guard to foreign governments and “certain private entities,” are also involved in assembling “encounter packages” when watchlisted individuals cross their paths. The encounters can be face-to-face meetings or electronic interactions—for instance, when a watchlisted individual applies for a visa.

In addition to data like fingerprints, travel itineraries, identification documents and gun licenses, the rules encourage screeners to acquire health insurance information, drug prescriptions, “any cards with an electronic strip on it (hotel cards, grocery cards, gift cards, frequent flyer cards),” cellphones, email addresses, binoculars, peroxide, bank account numbers, pay stubs, academic transcripts, parking and speeding tickets, and want ads. The digital information singled out for collection includes social media accounts, cell phone lists, speed dial numbers, laptop images, thumb drives, iPods, Kindles, and cameras. All of the information is then uploaded to the TIDE database.

Screeners are also instructed to collect data on any “pocket litter,” scuba gear, EZ Passes, library cards, and the titles of any books, along with information about their condition—“e.g., new, dog-eared, annotated, unopened.” Business cards and conference materials are also targeted, as well as “anything with an account number” and information about any gold or jewelry worn by the watchlisted individual. Even “animal information”—details about pets from veterinarians or tracking chips—is requested. The rulebook also encourages the collection of biometric or biographical data about the travel partners of watchlisted individuals.

The list of government entities that collect this data includes the U.S. Agency for International Development, which is neither an intelligence nor law-enforcement agency. As the rulebook notes, USAID funds foreign aid programs that promote environmentalism, health care, and education. USAID, which presents itself as committed to fighting global poverty, nonetheless appears to serve as a conduit for sensitive intelligence about foreigners. [According to the guidelines](#), “When USAID receives an application seeking financial assistance, prior to granting, these applications are subject to vetting by USAID intelligence analysts at the TSC.” The guidelines do not disclose the volume of names provided by USAID, the type of information it provides, or the number and duties of the “USAID intelligence analysts.”

A USAID spokesman told *The Intercept* that “in certain high risk countries, such as Afghanistan, USAID has determined that vetting potential partner organizations with the terrorist watchlist is warranted to protect U.S. taxpayer dollars and to minimize the risk of inadvertent funding of

terrorism.” He stated that since 2007, the agency has checked “the names and other personal identifying information of key individuals of contractors and grantees, and sub-recipients.”

## Death and the watchlist

The government has been widely criticized for making it impossible for people to know why they have been placed on a watchlist, and for making it nearly impossible to get off. The guidelines [bluntly state](#) that “the general policy of the U.S. Government is to neither confirm nor deny an individual’s watchlist status.” But the courts have taken exception to the official silence and footdragging: In June, a federal judge described the government’s secretive removal process as unconstitutional and “[wholly ineffective](#).”

The difficulty of getting off the list is highlighted by a passage in the guidelines stating that an individual can be kept on the watchlist, or even placed *onto* the watchlist, despite being acquitted of a terrorism-related crime. The rulebook justifies this by noting that conviction in U.S. courts requires evidence beyond a reasonable doubt, whereas watchlisting requires only a reasonable suspicion. Once suspicion is raised, even a jury’s verdict cannot erase it.

Not even death provides a guarantee of getting off the list. The guidelines say the names of dead people will stay on the list if there is reason to believe the deceased’s identity may be used by a suspected terrorist—which the National Counterterrorism Center calls a “demonstrated terrorist tactic.” In fact, for the same reason, the rules permit the deceased spouses of suspected terrorists to be placed onto the list *after* they have died.

For the living, the process of getting off the watchlist is simple yet opaque. A complaint can be filed through the Department of Homeland Security Traveler Redress Inquiry Program, which launches an internal review that is not subject to oversight by any court or entity outside the counterterrorism community. The review can result in removal from a watchlist or an adjustment of watchlist status, but the individual will not be told if he or she prevails. The guidelines highlight one of the reasons why it has been difficult to get off the list—if multiple agencies have contributed information on a watchlisted individual, all of them must agree to removing him or her.

If a U.S. citizen is placed on the no fly list while abroad and is turned away from a flight bound for the U.S., the guidelines say they should be referred to the nearest U.S. embassy or consulate, which is prohibited from informing them why they were blocked from flying. According to the rules, these individuals can be granted a “One-Time Waiver” to fly, though they will not be told that they are traveling on a waiver. Back in the United States, they will be unable to board another flight.

The document states that nominating agencies are “under a continuing obligation” to provide exculpatory information when it emerges. It adds that the agencies are expected to conduct annual reviews of watchlisted American citizens and green card holders. It is unclear whether foreigners—o

<https://firstlook.org/theintercept/article/2014/07/23/blacklisted/>