AMERICAN ENTERPRISE INSTITUTE

Statement before the Senate Committee
on Homeland Security and Governmental Affairs
On the Weaponization of the Quiet Skies Program

Counterterrorism Security Conundrums and the Demerits of Watch-Listing

JIM HARPER
Senior Nonresident Fellow

September 30, 2025

Executive Summary

The story of Quiet Skies is a useful indictment of an entire genre of counterterrorism program, the "watchlist." Watch-listing is a constitutional and security half-measure that departs from traditional law enforcement and security principles, such as separation of powers and the presumption of innocence.

By focusing on people first rather than prevention of crime and attack, watch-lists invite inquiry into motivation and ideology, ethnic and national background, so they will tend to threaten violations of First Amendment speech and association rights as well as wrongful discrimination. Comparing various dimensions of conventional law enforcement and counterterrorism helps to show why programs like watch-listing are fraught.

The strategic logic of terrorism is to seek overreaction on the part of victim states, with results including waste of blood and treasure and delegitimization. Quiet Skies has been a waste of taxpayer dollars and, misused for political purposes, a delegitimizing influence on domestic U.S. constituencies. There is a literature on terrorism risk management and "layered" security that could improve counterterrorism and homeland security programs.

Potential steps to foreclose the "next" Quiet Skies include reducing Congress's delegation of authority to the Department of Homeland Security, greater congressional oversight, improving public oversight by reducing secrecy, increasing judicial oversight by affirming a right to travel, and privatization of at least some security responsibilities.

Chairman Paul, Ranking Member Peters, and members of the committee,

Thank you for the opportunity to testify before you today. I am Jim Harper, a nonresident senior fellow with the American Enterprise Institute and a senior research fellow at the University of Florida's College of Journalism and Communications, First Amendment Project. For twenty-five years, I have been a policy analyst specializing in the intersections among law, technology, and society. My legal education focused on constitutional law, and my major area of professional focus has been privacy. I was drawn into counterterrorism because of the privacy consequences of many counterterrorism programs.

Your committee and my co-panelists have revealed and articulated the misuses of the Quiet Skies program and other watchlists. I will focus on the question of how to prevent the misuses of such programs in the future. The answers, I believe, lie in understanding the security conundrums created by terrorism and the institutional dynamics of all actors around the homeland security enterprise. These dynamics created a program, Quiet Skies, the existence of which delivered marginal or zero security gains. That program could be warped to political purposes without security costs.

Recognizing those dynamics may help you devise risk-management systems and institutional relationships that direct homeland security programs toward cost-efficient success while immunizing against misuse such as the political shenanigans that have been credibly alleged here. As we approach a quarter century dealing with security against terrorism, there is still much work to do on producing balanced, threat-appropriate responses consistent with American values and our fundamental law. We are still paying the price of terrorism in the form of overreaction, and that is terrorism's ongoing success.

Introduction

We enter into political society to secure our pre-existing, God-given rights against each other and outsiders. In doing so, we embrace the risk that the government we have formed for our mutual protection may invert its role and threaten those rights. This, in dressed up language, is what happened in the case of Quiet Skies. Rather than protect Americans' rights, the program invaded them.

Quiet Skies is in a category of homeland security programs with a native disability: it is oriented toward counterterrorism. That orientation is a recipe for failure—not because of successful terrorist attacks, but because securing against terrorism is a *sui generis* problem. It's actually a series of *sui generis* problems dressed up as a coherent security

problem by the similarity of their potential effects on our population, the creation of fear or "terror."[1]

We don't know what any future terror attack will look like. We don't know who will execute it or try to. Those problems had greater salience in the past. The blessing of having so few terrorist attacks is the curse of counterterrorism programs because our security agencies have no model of what to look for or pursue. So the imperative in counterterrorism is to look everywhere for anything. The natural result of such a diffuse charge is that programs such as Quiet Skies do essentially nothing, creating room for using the program to dole out penalties and favors: for monitoring of political enemies and release from monitoring for political friends.

Investigating People Rather than Wrongdoing

The story of Quiet Skies is a useful indictment of an entire genre of counterterrorism program, the "watchlist." The watchlist concept has existed long enough now that it may seem to be a valid security practice, but it is an investigatory and constitutional half-measure that wastes resources as it threatens our liberties.

Consider the Kafkaesque absurdity of the watchlist as such. It is a list of people who are bad enough to be put on a list, their freedoms to be shaved down in various clandestine ways, but not bad enough to be fully investigated, arrested, and charged. By doling out minor punishments and derogations on freedom unilaterally, watch-listing defies our constitutional separation of powers, in which law enforcement is supposed to bring charges to be adjudicated in the judicial branch. Watch-listing derogates from the presumption of innocence, an ancient legal principle adopted into English and then American common law.[2]

My surmise is that watch-listing is an upshot of the strange psychology of counterterrorism.

[1] "Terrorism" resists a workable definition. Here I am using the "terror" and "terrorism" concepts in their limited sense indicating activities by people with ideological or political agendas that create broad-based fears, not as the all-purpose epithet lobbed at political or ideological opponents who commit crime.

[2] *See* A.H. Godbey, "The Place of the Code of Hammurabi, 15 The Monist 199, 210 (Apr. 1905) ("It is a fundamental principle of the code of Hammurabi that the presumption is always in favor of the innocence of the accused: the burden of proof is thrown upon the accuser."); John Sassoon, Ancient Laws & Modern Problems: The Balance Between Justice and a Legal System 41-44 (2004) (recounting an ancient legal dispute in which "Ninkuzu is the accuser and the heirs of Atu are the accused; and the burden of proof rested in the third millennium BC where it would rest today – with the accuser.").

Acts of terror are an infinitesimally small risk to Americans' lives and limbs. In 2009, John Mueller of the Ohio State University cited the chance of anyone living outside a war zone being killed by an international terrorist at about 1 in 75,000 over an 80-year period. The chance of dying in an automobile accident over the same interval was about 1 in 80—three orders of magnitude greater.

It is worthwhile to encourage loved ones to drive safely. Terrorism shouldn't—and generally doesn't—even cross people's minds when they go out in the world.

In the absence of September 11-scale attacks every several years—which has been the case in the years since Mueller produced these numbers—the chance of death by terror attack falls to about 1 in 130,000. Mueller characterized that as similar to the risk of being struck by an asteroid.[3]

The statistically tiny threat of terrorism doesn't seem to matter. It certainly didn't matter in the years immediately after 2001.

Terrorism put us in a thrall, and it affected how we all think about security. There was something about the dramatic video imagery we saw over and over again, something about the idea that exotic looking men in faraway places hate us and our way of life (so we told ourselves; there is research on their actual motivations). These dynamics put us in a movie where we would do battle as a nation with supervillains. We began a figurative "War on Terror," which was understandable but unwise and counterproductive, as a strategy cannot be defeated.

It is no surprise that all this affected our approach to security. Where dispassionate security analysis would have focused on prevention—making sure nobody could do bad things—we were drawn to interdiction—focusing on bad people.

On the security merits, watch-listing is poor practice. The ideal in watch-listing is that you are able to discern who among, perhaps, *everyone in the world* wants to do you harm. To do watch-listing well, you need to know who among those are idle blowhards and who actually have the motivation and acuity to do something. You have to recognize a change in these states: when an inept hater gathers enough knowledge and will to act, when a capable opponent loses will or skill. Watch-listing naturally drives toward investigating such things as motivation and ideology, or ethnic and national background, so it invites violations of

[3] Cato Institute, "Shaping the Obama Administration's Counterterrorism Strategy Policy Forum," Cato Policy Report 11-12 (Mar./Apr. 2009) https://www.cato.org/sites/cato.org/files/serials/files/policy-report/2012/8/cpr31n2-5.pdf.

First Amendment speech and association rights as well as wrongful discrimination. To do watch-listing, you also need strong enough identity systems and information to make sure that you recognize those people when they arrive at gateways, such as the U.S. border, airports, or any other place they might act. The overwhelming difficulty of securing ourselves in this manner, by orienting toward bad people, drives the conclusion that it is a fraught exercise.[4]

We do focus on people in security and law enforcement, of course. But that focus is generally reserved for when the security systems that work against *anyone* have failed.

Think freshly about how security works. We live and many work inside buildings, which naturally protect. We lock their doors and windows at night. We have dogs, alarm systems, and neighbors, or all of the above. We hide valuables. We have police forces that circulate in towns and cities. These are a few of the many infrastructures and practices that provide the bulk of our security without reference to who may do wrong. Most security is prevention.

Criminal law enforcement generally kicks in after those background systems are defeated. It is then that we start to ask about people—who did it, where they have gone, what they have done with the proceeds of criminal activity, who they worked with, and so on. (Systematic efforts to defeat preventive security systems—conspiracies, racketeering, and so on—also invite criminal law investigations, of course.)

Watch-listing can't ask any of the questions that criminal law enforcement does, because nothing has happened. What watch-listing has produced instead seems to be a CYA system for security bureaucrats.[5] For any given security bureaucrat that comes across a potential bad person, the incentive set is clear. If you do nothing and they act, you will be blamed for failing to intervene. Nominating that person for a watchlist "does something," absolving you of responsibility in the event of a bad outcome. It is buck-passing exercise, because the placement of a person on a watchlist does not actually start or contribute to a

[4] *See* American Civil Liberties Union, "What's Wrong With the Government's Rules for Watchlisting" https://www.aclu.org/sites/default/files/field_document/watchlisting_guidance_takeaways.pdf.

[5] I intend to throw shade with the phrase "security bureaucrats." Countless men and women work in programs that are effective. They are not security bureaucrats. Some working in programs that are ineffective have valorously come forward to make that known. *See* Empower Oversight, "Air Marshal Whistleblowers Allege Gross Waste and Abuse of Authority in Protected Disclosures to Congress," Press Release (Aug. 14, 2024) https://empowr.us/air-marshal-whistleblowers-allege-gross-waste-and-abuse-of-authority-in-protected-disclosures-to-congress/. Those who knowingly work in ineffective programs, counting the days until retirement, are my security bureaucrats.

serious investigation that seeks to bring charges or otherwise punish or prevent whatever wrongdoing might be afoot.

The result has been watchlist bloat. In 2014, the "accomplishment" of adding the one millionth person to the Terrorist Identities Datamart Environment (TIDE) was revealed in leaked documents, producing a well-placed outpouring of derision.[6] I do not have a present sense of where we are in watch-listing today, but I cannot discern in theory what could possibly make watch-listing an effective security method consistent with the Constitution and our values the way conventional law enforcement is.

Conventional Law Enforcement and Counterterrorism Compared

A side-by-side comparison of conventional law enforcement and watchlist-based counterterrorism may help illustrate the challenge that the latter faces.

Harm Type

Conventional law enforcement addresses itself to traditional, relatively common, and thus highly recognizable harms and wrongs: theft, violence, fraud, and the planning for same. Counterterrorism has as a focus attacks and events that might terrorize, which is not a fixed or recognizable set of activities, as "terror" is contingent on media and public response.[7] Without any way of knowing what activity may terrorize, the fixation is on the last known thing to terrorize, an attack on air transportation.[8]

Incidence

There are many instances of the wrongs addressed by criminal law. This allows law enforcement personnel to recognize patterns of activity that are indicative of crime. There

[6] *See, e.g.*, Scott Sheckford, "Contain Your Shock: Huge Numbers of People on Watch Lists Have No Connection to Terrorist Groups," Reason (Aug. 5, 2014) https://reason.com/2014/08/05/contain-your-shock-huge-numbers-of-peopl/.

[7] In the past, I have written and spoken doubtful of "cyberterrorism" because of the inability of "cyber" attacks to actually terrorize. "The Underwhelming Threat of Cyberterrorism," Cato Institute Policy Report (Jan./Feb. 2011) https://www.cato.org/policy-report/january/february-2011/underwhelming-threat-cyberterrorism#.

[8] The aspect of the September 11, 2001 attack that did the most work, the commandeering attack, was actually foreclosed by late that morning. The passengers on Flight 93, realizing that their plane may be used as a giant bomb, fought back, leading to the plane's crash in Shanksville, Pennsylvania. It did not reach any strategic target or produce significant imagery for the public to consume. The hardening of cockpit doors and protocols to secure cockpits against invasion have driven the likelihood of another commandeering attack on air travel to a very low level.

is no similar high incidence of terrorist acts, so there are no patterns to look for digitally or intuitively in developing terrorism suspicion.[9]

Public, Reviewable, Constitutional Suspicion Protocols

Conventional law enforcement has protocols for assessing suspicion and what can be done when given levels of suspicion have been reached. One is the "reasonable suspicion based on articulable facts" doctrine articulated by the Supreme Court in *Terry v. Ohio*, which allows minor intrusions upon privacy (search) and liberty (seizure) interests when the threshold is reached.[10] The second is the "reasonable expectation of privacy" test, which governs full-fledged searches and seizures, allowing them when the Fourth Amendment's probable cause standard has been met.[11]

Quiet Skies apparently had protocols. The TSA blog,[12] the Department of Homeland Security's (DHS) Privacy Impact Assessment,[13] and a DHS Office of Inspector General (OIG) report[14] all referred to "risk-based, intelligence-driven rules." But we do not know what they were. The publicly available version of the OIG report redacts the number of such rules and examples of them. Unredacted language suggests some relationship between the rules and other federal government watchlists.[15]

---

[9] See Jeff Jonas and Jim Harper, "Effective Counterterrorism and the Limited Role of Predictive Data Mining," Cato Policy Analysis No. 584 (Dec. 11, 2006) https://www.cato.org/policy-analysis/effective-counterterrorism-limited-role-predictive-data-mining#; U.S. Senate Committee on the Judiciary, "Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs," Full Committee Hearing (Jan. 10, 2007) https://www.judiciary.senate.gov/committee-activity/hearings/balancing-privacy-and-security-the-privacy-implications-of-government-data-mining-programs.

[10] Terry v. Ohio, 392 U.S. 1, 21 (1968) ("…in justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion."). I would prefer the doctrine rely on facts that are actually articulated rather than "articulable."

[11] Katz v. United States, 389 U. S. 347, 361 (1967) (Harlan, J., concurring).

[12] Transportation Security Administration, "Facts About the 'Quiet Skies'" blog post (Aug. 22, 2018) https://web.archive.org/web/20201020122942/https://www.tsa.gov/blog/2018/08/22/facts-about-quiet-skies.

[13] Department of Homeland Security, "Privacy Impact Assessment Update for Secure Flight, Silent Partner and Quiet Skies," DHS/TSA/PIA-018(i) (Apr, 19, 2019) https://www.dhs.gov/sites/default/files/publications/pia-tsa-spqs018i-april2019_1.pdf.

[14] Department of Homeland Security, Office of Inspector General, "TSA Needs to Improve Management of the Quiet Skies Program (REDACTED)," OIG-21-11, (Nov. 25, 2020) https://www.oig.dhs.gov/sites/default/files/assets/2020-11/OIG-21-11-Nov20-Redacted.pdf.

[15] *Id*. at 1. The report was itself unavailable to the public as "sensitive security information" until declassified.

I have substantial criticisms of the suspicion protocols in conventional law enforcement,[16] but I can level such criticisms because of crucially important merits: They are rooted in the Constitution, they are publicly available, and they are regularly reviewed, challenged, and applied in public courts of law. These features, particularly the latter one, channel the suspicion protocols in traditional criminal law consistent with our constitutional values and norms. The secret suspicion protocol(s) in the Quiet Skies program did not.

Resolution in Courts

In conventional law enforcement, there is some resolution of cases through arrest and prosecution of suspects. It is possible for cases to drag on without resolution, but given the cadence in criminal law enforcement—of new, real crimes to pursue—incentives cut against keeping cases open and investigating suspects beyond the time when such activity seems likely to bear fruit.

The Quiet Skies program never saw a case reach fruition. It does not appear to have been an expectation of Quiet Skies that it would. Instead, it was a program for interdicting people whose activities did not raise sufficient suspicions to merit interdiction. As a program, it walked away from constitutional standards and law enforcement or security goals. This is why, I suspect, the program could mutate into use for political penalties and favors. Everyone involved probably knew intuitively that using it that way did not affect real security.

Counterterrorism programs like these may not just struggle to secure. They can actually make us worse off.

More On Terrorism

In 2010, with our nation nearing a decade of experience with counterterrorism, Christopher Preble, Ben Friedman, and I co-edited a book on counterterrorism called, "Terrorizing Ourselves."[17] Whether insightful or obvious, the overarching thesis was that terrorism does

[16] *See, e.g.*, Jim Harper, "Administering the Fourth Amendment in the Digital Age," National Constitution Center, A Twenty-First Century Framework for Digital Privacy – White Paper Series (May 10, 2017) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4692954; Jim Harper, "Escaping Fourth Amendment Doctrine After Jones: Physics, Law, and Privacy Protection," Cato Supreme Court Review (2012) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4692926; Jim Harper, "Reforming Fourth Amendment Privacy Doctrine," 57 Am. U. L. Rev. 1381 (2008). *See also*, Jim Harper, "Personal Information is Property," 73 Kan. L. Rev. 113 (2024) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4691923.

[17] BENJAMIN H. FRIEDMAN, JIM HARPER, AND CHRISTOPHER PREBLE, EDS., TERRORIZING OURSELVES (2010).

most of its work through overreaction on the part of the victim state. We classed these overreactions into three types:

- *Waste of Blood and Treasure*: When states needlessly go to war and waste the blood of soldiers or when terrorism countermeasures cost more than they provide in security, wasting the wealth of the people.

- *Recruitment and Sympathy Gains*: Violence or other countermeasures that engender sympathy for terrorists' causes, aiding in recruitment and support.

- *Delegitimization*: "Terrorists can cause victim states to come loose from their ideological moorings, reducing their credibility and authority with various audiences. A state with a liberal, tolerant credo, for example, may appear hypocritical to allies and domestic constituencies alike when response to terrorism appears illiberal and intolerant."[18]

Quiet Skies has elements of the first and third characteristics. It has been a clear waste of taxpayer money. An expenditure of Americans' taxpayer dollars is an expenditure of their time, portions of their lives, that should never go to ineffective programs.

As importantly, Quiet Skies was a departure from our ideological moorings, a security program made up of constitutional half-measures that resulted in the credible accusation of a Deep State cabal. Whether that accusation lands for you or not, the confidence of our own people in the legitimacy of their government is threatened by a program that does not follow traditional, constitutional rules for the conduct of security and law enforcement programs in the United States.

Terrorists are not evil geniuses. They are losers who have found solace in gang-membership[19] and stumbled across a powerful strategy. It embarrasses me to say that nearly a quarter century along, the September 11, 2001, attacks are still inducing us to waste taxpayer money and wander away from our Constitution. Through Quiet Skies and similarly defective programs, poorly calibrated responses to terrorism are *still* weakening us as a nation.

---

[18] *Id*. at 3.

[19] Max Abrahms, "What Terrorists Really Want: Terrorist Motives and Counterterrorism Strategy," 32 International Security 78 (Spring, 2008) https://www.jstor.org/stable/30129792.

Things have improved as the threat of terrorism has lost salience, but we must continue to press forward with restoring our freedom and security through effective risk management.

Terrorism Risk Management

The term "risk" seems more often abused in government security circles than properly used. The Financial Action Task Force's (FATF) global financial surveillance mandates are littered with risk language, for example.[20] My study of FATF programs has convinced me that the risks being managed in such programs are the risks of government authorities prosecuting financial institutions, not the risks of crime and threats to national security relating to financial flows.

So it seems to be with many counterterrorism programs claiming to do risk management, including Quiet Skies. Watch-listing people and then watching them seems to be security-related activity. But it does little to cost-effectively manage true threats. It manages the threat that blame will be accorded to agencies if there is some kind of successful attack.

In 2006, the DHS Data Privacy and Integrity Advisory Committee (DHS Privacy Committee), on which I served at the time, published a "Framework for Privacy Analysis of Programs, Technologies, and Applications" that I believe does a creditable job on terrorism risk management.[21] It is not a narrow, privacy-oriented document. Because privacy generally gives way in the face of reasonable suspicion, the framework provides a system for determining the reasonableness of programs on their security merits.

The heart of the document is the third "step" of the analysis it recommends, which is to examine risk management and efficacy.[22] The steps included in this fairly readable document are:

- Target Assessment ("What are you trying to protect?")

- Threat Assessment ("What are you trying to protect it from?")

[20] *See, e.g.*, Financial Action Task Force, "Risk-Based Approach for the Banking Sector" (Oct. 2014) https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Risk-based-approach-banking-sector.html.
[21] Department of Homeland Security Data Privacy and Integrity Advisory Committee, "Framework for Privacy Analysis of Programs, Technologies, and Applications," Report No. 2006-01 (Mar. 7, 2006) https://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_03-2006_framework.pdf.
[22] *Id*. at 3-4

- Risk Assessment ("What is the likelihood of each threat occurring and the consequence if it does?")

- Response Characterization ("What kind of action does the program take in response to the threat?") The possible response types are:

    - Acceptance—the rational alternative when a threat has low probability, low consequence, or both.

    - Prevention—alteration of the target or its circumstances to diminish the risk of the bad thing happening.

    - Interdiction—confrontation with, or influence exerted on, an attacker to eliminate or limit its movement toward causing harm.

    - Mitigation—preparation so that, in the event of the bad thing happening, its consequences are reduced.

- Risk Transfer Assessment ("Does the response create new risks to the asset or others?")

The document goes on to assess privacy-related costs of such programs so they can be weighed against security benefits. A full analysis would, of course, consider dollar costs as well. There must be balancing between public expenditures—again, small pieces of the lives of tax-paying Americans—and the expected lives and dollars saved by a given response or program. Responses without an articulated, expected favorable outcome should not be pursued.

Security "Layers"

With the idea in mind that risk management is how we protect things, consider the "layers" metaphor for security programs. The things we want to protect are ringed by metaphorical circles of protection. This is most simply illustrated by something simple, like a bank.

Among the layers that protect a bank and thus deposits against robbery are ("closest" to "furthest," with response type):

- Insurance (mitigation)
- A vault that is physically difficult to open or break into (prevention)
- Protocols that limit access to cash (prevention, mitigation)
- Background checks on employees (interdiction)
- Security cameras (interdiction)
- Armed guards (interdiction)
- Silent alarm systems (interdiction)
- Dye packs (interdiction)
- General police patrols (interdiction)
- Criminal law enforcement (interdiction)
- Incarceration (interdiction)
- Education systems (interdiction)

There are many more layers, but hopefully it is easy to see how these form metaphorical circles spreading from immediately around the protected thing, the bank and its deposits.

Yes, education systems are an outer-layer security measure (interdiction-type) because a good education creates job prospects and entrepreneurial opportunities that lower the enticement of bank robbery. It interferes with would-be bank robbers very early, putting them on paths to productive lives.

The layers around air security are many. They include:

- Airplane design resistant to explosion (mitigation)
- Hardened cockpit doors and cockpit-denial protocols (interdiction)
- Passenger inspection (interdiction)
- Passenger “trust” programs (interdiction)
- General law enforcement (interdiction)
- Surveillance and intelligence (interdiction)
- Peaceable foreign policy (interdiction)

These measures vary widely in effectiveness. By listing them, I do not endorse them all or equally. The security measures that work against anyone seem quite a bit stronger. So passenger inspection I have always believed to do the vast bulk of any lifting needed late in the game, because denying people the tools they might use to attack air travel is a simple, pure bar on attacks. “Trusting” travelers—trying to predict good behavior based on biography—seems quite fallible, and it is also subject to identity fraud.

Yes, a peaceable foreign policy is an outer-layer security measure (interdiction-type) because it dissuades would-be terrorists from seeing that activity as worthwhile.

Risk management exists, and it can be applied to counterterrorism. (Downplaying terrorism is part of good counterterrorism.) The question is what institutional adjustments can produce better risk management.

Steps to Foreclose the Next Quiet Skies

As a nation and society, we need to assess risk and balance the benefits of security programs with their costs to other values that are dear, including privacy, constitutional rights, and fiscal rectitude.

The Department of Homeland Security is not, and will never be, a true risk-balancing organization. We probably should not want it to be. There are internal checks that do some work, such as the DHS Privacy Committee before it was neutered by "tasking orders" that sought to make it speak only when spoken to. The Privacy Impact Assessment process probably takes some burrs off of programs without really altering the course of the misbegotten ones.

Our constitutional system relies on tensions among branches of government. We can use those and tensions among agencies, rather than trying to have a single government body arrive at all the answers. There are a number of ways to build tensions into our systems that I think will lead to better outcomes. One of the most important balancing systems is probably Congress.

De-Delegate Authority

Congress is comprised of people who face re-election regularly, so it is a better balancer of values than federal agencies. It is the organ of government to which the Constitution assigned the role of policymaking. Withdrawing policymaking authority from the executive branch and bringing it back to the legislative branch should improve future outcomes.

The Aviation and Transportation Security Act (ATSA)[23] was a huge delegation of authority to the executive branch. It created a new Transportation Security Administration in 2001 with only the vaguest of directives about what to do and how to do it.[24] A new Under Secretary of

[23] Public Law No. 107-71 (1st Sess.)
[24] *Id*. at § 101.

Transportation for Security (later transferred to a new Department of Homeland Security) would be "responsible for security in all modes of transportation."[25] There would be screening operations,[26] it was clear, but their scope and parameters, measures of effectiveness, and the rights and liabilities of travelers went unaddressed. There would be an expanded Federal Air Marshals system.[27] There was little contemplation of what to do if there were not sufficient threats to justify having them.

There is telling language in a subsection of ATSA saying that the Under Secretary would "develop policies, strategies, and plans for dealing with threats to transportation security."[28] Under my idealistic view of the roles of the two branches, you in the legislative branch would determine the policies. You would probably determine strategies. And you might even devise plans for the executive branch to carry out. There would at least be clear indicia of when executive branch agencies have succeeded or failed at carrying out your intentions.

That is the ideal, and we can certainly understand the reason for the haste with which Congress passed this statute. But that does not undercut the point that the hugely broad delegation authorized whatever the Transportation Security Administration ultimately came up with.

You, the Congress, should take back authority from the executive branch. Revisions of transportation security authorities would cabin the activities of the DHS and TSA so that they carry out programs of your devising. It may be productive to go through existing programs and authorize explicitly the ones you find to work cost-effectively, de-authorizing the ones you find do not.

Congressional Oversight

This hearing is an example of processes that create balance. Direct congressional oversight sends signals to executive branch agencies about how to use the authorities they have. Oversight through hearings and letters is a far cry from actually controlling the executive branch through authorizing language, of course, and the executive branch is so large today that it is very hard to oversee. But more oversight is always welcome.

[25] *Id*. (new 49 U.S.C. § 114(d)).
[26] *Id*. (new 49 U.S.C. § 114(e)).
[27] *Id*. at § 105.
[28] *Id*. (new 49 U.S.C. § 114(f)(3)).

Public Oversight/Transparency/Anti-Secrecy

Opining about the psychology of counterterrorism above, I said that we have put ourselves in a movie fighting against supervillains. If real, those dynamics might justify the level of secrecy we have in the counterterrorism enterprise. But it is not real, and that secrecy comes at a terrible cost to our democratic republican form of government: It denies the public and the courts opportunities to play their roles in oversight of the government.

Senator Daniel Patrick Moynihan's book, SECRECY: THE AMERICAN EXPERIENCE, is an under-sung contribution to an important area of policy that is more important than ever. Drawing on his experiences as a member of the Senate Select Committee on Intelligence and chairman of the Commission on Protecting and Reducing Government Secrecy, he asserts in the book that secrecy leaves policymakers less informed, denies government accountability, and sharply limits public debate about policy and government conduct. The corrosiveness of secrecy is on display in Quiet Skies, where secrecy extended the life of a program that did nothing productive, while it hid from victims that they were being surveilled, their freedom to travel degraded.

Secrecy has been used to deny people access to the courts because they often cannot prove the existence or effects of secret programs on their rights without legal discovery, and, in a tour de force of circularity, discovery is prevented by claims to secrecy.

Judicial Oversight

Enhanced judicial oversight is another way to drive balance into counterterrorism programs. One idea is for Congress to declare that there is a right to travel on par with other rights specifically enumerated in the Bill of Rights. That would enhance judicial oversight of programs affecting transportation.

The federal courts give a right to travel at least uneven treatment,[29] the result being that when people object to government incursions on their travel, their cases almost always fail before the true security merits of a policy can be considered. Were people to have a clearly recognized right to travel, which Congress can encourage, the merits and demerits of

[29] Compare Shapiro v. Thompson, 394 U.S. 618, 629 (1969) (noting the right of all citizens to be "free to travel throughout the length and breadth of our land uninhibited by statutes, rules, or regulations which unreasonably burden or restrict this movement") to Gilmore v. Gonzales, 435 F. 3d 1125, 1137 (9th Cir. 2006) (Would-be cross-country traveler "does not possess a fundamental right to travel by airplane even though it is the most convenient mode of travel for him.").

transportation security policies could be hammered out more thoroughly in courts. Agencies would have to fully justify their policies because they must overcome presumptions in favor of Americans' exercise of their rights. Cost-effective security measures surely would pass muster even against a claim of right to travel. Ineffective and overly invasive programs would not.

Privatization

The psychology of terrorism and counterterrorism has done more than just skew specific government security practices. It also drives the premise that security is a governmental responsibility as opposed to a private one.

In most fields, we expect individuals and companies to secure their own stuff first. Criminal law enforcement is provided to all on equal terms, but if a person in the plastics business came to you and said, "Yeah, I need you to provide my company's security now," you would probably kick them out of the room. At least you should.

Terrorism has us thinking that attacks on private infrastructure and business are a public policy problem. In some respects they are. There are dimensions to security against certain dimensions of terrorism that are public goods, such as intelligence. Political leaders can do a great deal to ward off overreaction to terrorism, which does have society-wide and thus political connotations. But global corporations have substantial capacities to gather information that relates to their businesses and security. At least some responsibility for security can be pressed back into the private sector so that the challenges of risk management—finding that balance—are with the people who have the most skin in the game.

In 2005, I engaged in a debate with Robert Poole of the Reason Foundation in which I argued for elimination of the TSA.[30] I may be a little less strident now, but the arguments I made then hold up reasonably well. On the question of government versus private risk management, I wrote:

> TSA security measures have been inconsistent and mindlessly reactive. This is because bureaucracies are poor at assessing and balancing risk. They are much better at surfing public opinion and following political cues. Witness the TSA's obsession with small, sharp things early in its tenure and the shoe fetish it adopted

[30] Robert Poole and Jim Harper, "Transportation Security Aggravation," Reason magazine (Mar. 2005) https://reason.com/2005/03/01/transportation-security-aggrav-2/.

after Richard Reid demonstrated the potential hazards of footwear. This is not a foresighted, research-based, risk-assessing organization.

Highly effective, nonregulatory systems exist to analyze and respond to risk. They operate well, though not perfectly, when they are allowed to. They start with the tort system, which places responsibility for avoiding foreseeable harms with the parties in the best position to avoid them. Through insurance contracts, businesses in every sector of the economy spread risk and often purchase expert advice on loss avoidance.

***

Airlines should be given clear responsibility for their own security and clear liability should they fail. Under these conditions, airlines would provide security, along with the best mix of privacy, savings, and convenience, in the best possible way.

If not elimination of the TSA and full privatization of security in this area, it may still be worth considering whether some dimensions of security can be restored to the private sector, so that liability rules, the insurance system, and other mechanisms can do some of this work. Privatization of security responsibility would reduce subsidies to the corporate sector now given through the direct provision of security services and insulation from liability.

Conclusion

We are in a time of welcome openness to change at the Department of Homeland Security. The DHS under Secretary Noem has eliminated Quiet Skies, for the good. DHS and Secretary Noem have rescinded the "shoes-off" policy at airport checkpoints.[31] That policy was a reaction to one failed attack, and it remained in place far too long, inconveniencing travelers and driving them away from air travel.

Secretary Noem has signaled that the "liquids rule" may go by the wayside, too.[32] It was a reaction to the revelation of a nascent plan to smuggle constituents of a liquid explosive called TATP onto an airplane. The probability of such an attack coming to fruition was very

[31] Department of Homeland Security, "DHS to End 'Shoes-Off' Travel Policy," press release (July 8, 2025) https://www.dhs.gov/news/2025/07/08/dhs-end-shoes-travel-policy.
[32] CBS News moneywatch, "Homeland Secretary Kristi Noem says TSA may change rules about liquids on flights," (July 17, 2025) https://www.cbsnews.com/news/tsa-liquid-carry-on-restrictions-relax-kristi-noem-comments/.

low, and it was defeated by a security layer quite far from the airport (surveillance). The added inconvenience and expense of the liquids rule probably dissuades people from air travel in significant numbers, doing more damage than it provides in security. It has stayed around too long.

My hope is that DHS leadership has recognized REAL ID enforcement also to be a fool's errand. The practice of checking IDs at the airport is premised on the same conceptual errors that undergird watch-listing. Though the agency has stayed mum, it has made it very easy to travel without a REAL ID.[33] The difficulty of complying with ID requirements, the time spent fumbling for and showing ID, and various other slight inconveniences repeated from thousands of times per day to millions of times per month also probably suppress access to air travel more than it provides security.

Why should it be important for people to access air travel? The issue of infant air travel illustrates.

Infant travel is a rare exception to the risk phobia usually seen in air travel. It appears well settled that infants should be allowed to be unbelted on airplanes, because the alternative is not infants strapped into their own seats but infants in cars. And the risk of death by car accident for people of all ages is much greater than the risk of being on a plane.

"If the extra cost of buying airline tickets for the young children led only 5 to 10 percent of families to drive rather than fly," a University of California San Francisco and University of Washington study of separate seating for infants found in 2003, "the projected increase in highway deaths would exceed the number of airplane crash deaths prevented."[34]

Moving people from airplanes to cars is deadly.[35] The additional cost in time and aggravation of niggling security procedures that do not have robust benefits has undoubtedly moved American travelers into cars. Over two decades, millions of would-be flights have been switched to drives, and likely tens or hundreds have needlessly died.

---

[33] *See* Jim Harper, "Airline Security's Best-Kept Secret," AEIdeas, American Enterprise Institute (July 24, 2025) https://ctse.aei.org/airline-securitys-best-kept-secret/.

[34] University of California San Francisco, "Airline Infant Safety Seat Rule Could Cause More Deaths Than It Prevents, Pediatricians Say," press release (Oct. 2003) https://www.ucsf.edu/news/2003/10/97119/airline-infant-safety-seat-rule-could-cause-more-deaths-it-prevents.

[35] *See* Insurance Institute for Highway Safety, "Fatality Facts 2023: State by State," https://www.iihs.org/research-areas/fatality-statistics/detail/state-by-state.

Getting people into planes is good for Americans' spirits, good for the economy, and good for saving lives.

There is a wonderful coincidence that everything done by terrorists is illegal, so ordinary law enforcement is counterterrorism without the misleading psychological baggage. Pursuing criminal activity is counterterrorism—and it is strategically wise counterterrorism because it does not award terrorists the status they seek, of being an outsized threat to our nation. While pursuing criminal activity of all kinds aggressively, staying calm, cool, and collected as a nation is good counterterrorism.

There is a wonderful coincidence that *effective* programs tend to be constitutional programs. When search and seizure activities work effectively to uncover criminal wrongdoing, whether terroristic or not, it is reasonable and can be found so under the Fourth Amendment by a neutral magistrate, as the Constitution requires.

Investigations that are secret until a criminal charge is brought do not deny constitutional due process. Disclosure is not due until investigations are concluded and charges brought.

Secret investigations that are not aimed at bringing criminal charges and thus never reveal themselves DO deny due process, because they subject innocent Americans to monitoring and investigation with no opportunity to question or counter such activity. Innocent Americans suffer unilateral mistreatment with no effective redress. That is the story of Quiet Skies, a product of failure to grapple with the security conundrums created decades ago by a single act of terrorism.