Center for National Policy

Charting a Secure, Prosperous, and Resilient Future

"Beyond Law Enforcement and Screeners: Elevating the Role of Public Engagement and Resilience in Rail and Transit Security"

Written Testimony to support

a hearing of the

Committee on Homeland Security and Government Affairs
United States Senate

on

"See Something, Say Something, Do Something:
Next Steps for Securing Rail and Transit"

by

Stephen E. Flynn, Ph.D.
President
Center for National Policy
sflynn@cnponline.org

Dirksen Senate Office Building – Room SD-342
Washington, D.C.

10:00 a.m..
June 22, 2011

"Beyond Law Enforcement and Screeners:
The Role of Training and Public Education in Rail and Transit Security"

Dr. Stephen E. Flynn
President, Center for National Policy

Chairman Lieberman, Ranking Member Collins, and distinguished members of the Committee on Homeland Security and Government Affairs. I am honored to have this opportunity to testify on the critically important issue of rail and transit security nearly ten years after the attacks of September 11, 2011 on New York and Washington.

At the outset, it is important to acknowledge, that rail and transit security simply have not been a priority for the Bush and Obama Administrations, both in terms of policy focus and dollars and cents. By one estimate, typically $9 is spent on security for every passenger who flies. Meanwhile we are spending roughly one penny per rail and transit passenger.[1] When it comes to this critical sector, as a nation we have barely crossed the starting line. But, there is a potential silver lining to the embryonic state of rail and transit security. We can avoid trying to replicate the kind of costly enforcement-centric approach that generally assumes operators and users pose a potential threat to the system unless they are subject to screening by security officials. In its place, we can invest in a more effective, sustainable, and affordable system of reaching out to commuters and workers who operate in and around rail and transit systems, and inform, empower, and support them as part of solution before, during, and immediate after a security incident. We can also assign a higher priority to effectively responding and recovering from intentional attacks and accidental incidents in order to reduce the disruptive appeal of targeting the rail sector.

Assessing the Threat:

The renewed attention to rail security has been animated by intelligence gathered by U.S. Special Forces during their raid on the compound of Osama bin Laden that pointed to possible plots to derail trains in the United States. The vulnerability is a real one as demonstrated just last week when Amtrak announced that it would be stepping up security along its rail lines while the FBI investigated the discovery on Jun 11, 2011 of an incident of intentional tampering of a switch box along an Amtrak route in Iowa. Overseas incidents in Madrid, London, and Mumbai all make clear that trains and train stations are in the crosshairs of contemporary terrorist organizations.

Since 2008, I have been honored to serve as a member of the National Security Preparedness Group (NSPG), led by former 9/11 Commission chairs, Governor Tom Kean and Congressman Lee Hamilton. In September 2010, the NSPG released a report *Assessing the Terrorist Threat*, that found that the United States is facing a growing risk of small-scale attacks executed by homegrown terrorists. A number of recent studies and reports seem to confirm these assessments. In February 2011, the New America Foundation and Syracuse University published a report that found that "nearly half" of

[1] Testimony from James C. Little, International President of the Transport Workers of America, AFL-CIO, before the House Committee on Homeland Security. February 13, 2007. http://chsdemocrats.house.gov/SiteDocuments/20070213174618-07221.pdf

the 175 cases of Al Qaeda related homegrown terrorism since September 11, 2001, occurred in 2009 and 2010.[2] Among the most serious incidents, and the one most relevant for the topic of the hearing today, is the September 2009 plan by Najibullah Zazi to blow up the New York City subway.

The likelihood that there will be more efforts to target rail and transit systems is a logical outcome of this evolution of terrorist threat. With the dismantling of much of al Qaeda's senior leadership infrastructure including the May 1, 2011 death of Osama bin Laden, the capacity for al Qaeda to plan and execute sophisticated large-scale attacks in North America has significant declined. Large-scale attacks organized by aligned groups or other terrorist organization are still possible, but they are increasingly difficult to carry out without attracting attention. This is because catastrophic-scale attacks require a group of operatives with a capable leader, communications with those overseeing the planning, and time to conduct surveillance and rehearse the attack. Money, identity documents, safehouses for operatives, and other logistical needs have to be supported. All this effort ends up creating multiple opportunities for detection and interception by intelligence and law enforcement officials.

But attacks on freight trains and mass transit can be carried out by homegrown operatives, acting as lone wolves or with one or two accomplices. These attacks are far more difficult for the intelligence community to detect and for federal law enforcement to intercept. They also satisfy another contributing variable that is fueling smaller-scale attacks: the recognition by al Qaeda that terrorist attacks on the United States do not have to be spectacular or catastrophic to be effective. As the attempted bombing of Northwest Airlines Flight Number 563 on Christmas Day 2009 dramatically illustrated, even near-miss attacks can generate considerable political fallout and a rush to impose expensive and economically disruptive new protective measures. Since relatively small and unsophisticated attacks have the potential to generate such a big-bang for a relatively small investment, the bar can be lowered for recruiting terrorist operatives, including those who belong to the targeted societies.

The October 2010 air cargo incident involving explosives hidden ink cartridges shipped from Yemen is consistent with this trend towards smaller attacks, but with the added element of aspiring to create significant economic disruption. The would-be bombers had no way of knowing that the cartridges would end up on a commercial airliner with hundreds of passengers or a dedicated air cargo carrier with a small crew. That was not important since they understood that destroying any plane in midair would trigger U.S. officials and others to undertake an extremely costly and profoundly disruptive response that would undermine the movement of global air cargo.

To summarize, in the absence of a new security focus, mass transit systems and rail freight are likely to become increasingly attractive targets for terrorist organization. These systems are relatively easy to access since they provide multiple entry points, very

[2] "Post-9/11 Jihadist Terrorism Cases Involving U.S. Citizens and Residents," *A Study by the New America Foundation and Syracuse University's Maxwell School of Public Policy*, March 2011, available at http://homegrown.newamerica.net/.

often over a vast geographic area, with little to no physical security barriers to entry. Homegrown terrorists are likely to familiar with these systems. Attacks on mass transit, especially stations, particularly when undertaken during peak-commuting hours, can potentially be even more deadly than an attack on a single aircraft. At the same time, should such an attack lead to the shutting down of a transit system, the resultant denial of service can be crippling to the operation of a major urban economy.

How Not to Advance Rail and Transit Sucurity:

In crafting a way forward in rail and transit security, we should first avoid four-missteps that have marked the post-9/11 approach to homeland security.

The first rule is *to avoid alienating the very public that security officials are obligated to protect*. This is a lesson that was learned the hard way by the U.S. military in Iraq and it is now imbedded in the Army Field Manual that guides counterinsurgency operations. Getting the public to submit to new security measures as a condition of their gaining access to transportation systems is relatively straight forward. But coercing compliance has the downside of creating passivity and often generating resentment. Alternatively, when the general public understands and views an effort to advance security as appropriate, they will actively collaborate in achieving its goal. When it comes to rail and transit security, federal officials should pursue efforts that engender the support and active involvement of the riding public and the operators they serve.

Rule 2 is *do not promise more than can be delivered*. No security regime will be fool proof. This is why it is a bad idea for public officials to be tightlipped about the known limits of any specific technology or protocol. The new scanning technology now in use at U.S. airports can be evaded by common drug smuggling techniques. At U.S. seaports, radiation portals have been deployed with considerable fanfare to support the inspection of inbound containers. But these portals are unlikely to detect shielded nuclear material which means that a nuclear weapon or even a dirty bomb encased in lead could pass through the portals without triggering an alarm. Allowing unrealistic expectations to go unchecked guarantees disappointment and mistrust over the long run.

A corollary of this rule is to be wary of measures that are weighted more towards providing the "optics of security" rather than real security. For example, the presence of cement barriers outside a train station may reassure daily commuters. But if those barriers are not anchored to the ground, an explosive-laden truck could ram them aside and make it to the station's entrance. The ensuing tragedy would leave commuters feeling rightfully deceived and the families of victims outraged. Security protocols must survive a "morning-after test"; that is, they should be able to withstand a postmortem by the public about their adequacy, even if they failed to thwart an attack. If the post-incident assessment deems the security measures to be lacking credibility, there will be hell to pay.

Rule 3 is to *resist the secrecy reflex*. Too much homeland security-related work is being done behind closed doors. On its face the oft-stated rationales for this secrecy are compelling. For

instance, it seems sensible to avoid identifying vulnerabilities that potential adversaries might then decide to target. Also, if the details of security measures are publicly know, a determined adversary might devise a successful work around. And too much candor about threats and vulnerabilities might generate excessive public fear.

But the proclivity for the national security, intelligence, and federal law enforcement communities to operate in a world of classified documents and windowless rooms is counterproductive. Too often, the people who design, operate, or manage critical systems are left out of the security loop. This is especially the case with critical infrastructure, the vast majority of which is in the hands of the private sector. Even if a company's chief security officer is cleared to receive security briefings, it does little good if she cannot pass the details along to her colleagues and bosses. As a result, most of the expertise for devising creative, sensible, and sustainable solutions is not being tapped. To determine the best way to protect something like rail freight and mass transit systems, federal officials should err on the side of openness when it comes to sharing information with operators and managers of those systems and should actively solicit their input.

While releasing detailed blueprints of protective measures to the general public would be foolish, there is a potential counterterrorism benefit to being more open about what is being done to protect critical systems like rail transportation. This is because the secrecy reflex often ends up working against the goal of keeping public anxiety in check. People are most frightened when they sense they are vulnerable to a threat but feel powerless to deal with it. For nearly a decade Americans have been hearing that terrorism is a clear and present danger. But more often than not, they have been told to go about their daily routines because their government is hard at work protecting them. This is much like a doctor telling a patient that she is suffering from a potential life-threatening illness and then providing only vague information about what can be done about it. No one wants to get disturbing news from their physician, but it becomes much less stressful once they get the details of a prognosis, receive a clear outlay of the available treatments, and are given the opportunity to make decisions or take actions that provide an element of personal control over the outcome. In the same way, the American public will be less fearful and more prepared if they are given the information they will need to better withstand, rapidly recover from and adapt to the next major terrorism attack. It follows that elevating the *risk-literacy* of Americans should be a top homeland security priority.

The fourth and perhaps most important rile is *do not overreact*. What is fueling the appeal of terrorism as a tactic against the United States is the confidence that terrorists have that Americans will react by embracing draconian measures with little consideration for cost or unintended consequences. Regrettably, since 9/11, this is precisely the kind of response that Washington has been publicly embracing in both word and deed.

The Way Forward – An Emphasis on Resilience

A strategic approach to rail and transit security should have three key elements. It should begin with the recognition that commuters and workers in and around the rail and mass transit system should be seen as the frontlines of prevention. Intelligence and law

enforcement officials can play an important support role, but it is unrealistic to assign them the dominant role. Transit and rail systems are difficult to protect because they tend to be open to so many users across a wide geographic area and their operations are very time-sensitive. A typical New York City subway station has at least four entrances for passengers and major stations can have more than a dozen. When trains are delay, platforms can quickly become heavily congested. The MetroNorth, Long Island Railroad, the New Jersey Transit and PATH are regional systems that carry daily commuters across city and even state boundaries. Given the small number of tracks available to support their ridership, these trains must abide by a strict schedule to avoid creating cascading delays throughout the system

While on its face, mass transit looks hopelessly difficult to secure, it has a tremendous asset when it comes to detecting a potential security threat—its riders and operators know and are deeply vested in the safety and efficiency of the system. Unlike aviation where passengers typically have only episodic contact with planes and air terminals, the overwhelming majority of commuters do so each day, often at the same time, and frequently sit in the same area on trains. They are both attune to the normal rhythm of the transit experience, and typically perceptive about any changes. Train conductors often know many of their commuters by face if not by name. Engineers, maintenance, and support personnel are intimately familiar with their operational environment. Ticket agents, taxi drivers, vendors, and shoeshine boys have the means to detect aberrant activity in even the most hectic train station. Everyone is inherently vested in making the transit experience a safe and timely one. All should be asked to share in that responsibility and provided with training and education to play that role.

While the New York City "See Something, Say Something" campaign is a helpful stepping-off point, the public needs to know what they should be looking out for, who they are saying something to, and what they can expect as an outcome. There are lots of opportunities to communicate with the transit public while they are at stations, on platforms, and aboard trains. Every effort should be made to use contact with riders as "teaching moments." Warnings should have meaningful content and there should be guidance that outline simple task for dealing with emergencies. Outreach should be done to major employers who have a large number of commuters to solicit them in supporting more extensive training efforts. Wherever possible, commuters and their employers should also be encouraged to "do something" such as receive Red Cross training and participate in programs modeled on the Metro Citizen Corps established by the Metro Police in Washington, DC.

Training of the professionals who operate within and around the transit system needs to be substantially stepped-up. The just-released June 14, 2011, GAO report on "Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing" documents the inconsistency and inadequacy of railroad security training programs around the country.[3] Maddeningly, the failure of TSA to issue

[3] GAO-11-688T Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing, June 14, 2011, http://www.gao.gov/new.items/d11688t.pdf

regulations for these programs as required by the *Implementing Recommendations of the 9/11 Commission Act of 2007* has effectively put rail security in a deep freeze for over three years. This is because most local jurisdictions have been hesitant to pursue their own effort until direction arrives from Washington. But the answer is not simply for TSA to rush out new regulations developed by its headquarters staff. These regulations need to be developed with input from transit unions and other transportation professionals who understand the rail operations.

One model training program that should be rolled out within major rail stations is *Logan Watch*. Logan Watch takes a whole community approach to terminal security at Boston's Logan Airport. Every employee at Logan Airport receives training on identifying and acting on suspicious activity. This should be an annual requirement at all airports and major transportation terminals around the United States.

The second strategic imperative is to insure that security efforts are appropriately balanced across jurisdictions and not simply concentrated, piecemeal fashion, within the jurisdiction of a few major cities. Rail security also should not be treated in isolation since it frequently connects with other modes of transportation including bus service, ferry service for passengers, and trucks, ships, and barges for freight. One model worthy of emulation for dealing with cross-jurisdictional and intermodal issues is Connecticut's Transit Security Committee that includes security officials from the transit agencies operating within the state, as well as representatives from the maritime, aviation, trucking, highway, and pipeline sectors. These Committees should also include transit representatives from adjacent states when that is appropriate as well as senior managers and transit union representatives. As with Area Maritime Security Committees, formally established regional transit security committees could be provided an opportunity to vet and prioritize federal grant proposals.

A third strategic imperative is to emphasize the *resilience* of transit systems. Specifically, more should be done to make these systems better able to withstand, and to more effectively response and recover to the probability that they may be targeted some day. Focusing on resilience is not an act of resignation and pessimism. Certainly, pragmatism requires an acknowledgement that there is no such thing as fail-safe prevention measures. We should be prepared for when things go wrong. But improving resilience can actually support the prevention goal by creating a deterrent. Since the primary appeal of engaging in acts of terrorism is the harm it will inflict and the disruption that it will generate, resilient systems make less attractive targets. If a terrorist attack results in a fizzle instead of a big bang, there is little incentive for an adversary to undertake them.

It is important to recall that the July 7, 2005 attacks on the London Underground were met with a swift and effective emergency response. London emergency responders routinely conduct major drills and exercises. Several of the London firefighters had actually received training at "Disaster City" at Texas A&M University and publicly attributed their successful response to that training. Had the emergency response been badly managed, it is likely that London commuters would have been more hesitant to re-

board trains the morning after the attacks. In short, investing in effective emergency response is key to quickly restoring a targeted transit system, and a demonstrated capacity to rapidly restoring service is key to deterring/preventing an attack on the transit system in the first place. To this end more funding should be provided (1) to support transit workers and emergency responders from across the United States to attend the Texas Engineering Extension Service (TEEX) program, and (2) to conduct major training exercises annually.

To conclude, a renewed focus on transit security provides an opportunity to recalibrate our approach to homeland security so that it draws on America's greatest national security asset—our people. Law enforcement and some security technology can be helpful. However, neither will ever be an effectively substitute for a better informed and empowered transit public, a well-trained workforce, and capable emergency responders.

Chairman Lieberman and Senator Collins, I thank you for this opportunity to testify today and look forward to responding to any questions that you might have.

Stephen Flynn is the president of the Center for National Policy and author of "Recalibrating Homeland Security" that appears in the May/Jun 2011 issue of Foreign Affairs.