Dear Admiral Neffenger:
a challenge to TSA's new administrator

ALSO:
SECURITY & ROUTE SELECTION
INFRARED IMAGING TECHNOLOGY
CIVIL AVIATION IN THE DIGITAL NOW
SHENZHEN AIRLINES ARSON
DEAR TSA ADMINISTRATOR
ADMIRAL NEFFENGER:
FROM ONE FORMER COAST GUARD TO ANOTHER

The Transportation Security Administration has a new man at the helm – Admiral Neffenger. The agency has many critics and there is little doubt that there will be no let-up in the creativity of those who seek to bypass the measures it takes to safeguard American skies, but every challenge has a solution and Jeffrey C. Price has drawn up an initiative which he feels might help Admiral Neffenger along the way and, in doing so, create a more effective, respected agency.

Dear Admiral Neffenger,

From one former 'coastie' to another, Semper Paratus and congratulations on your appointment to one of the most enviable positions in the federal government. At times, it may feel like you've taken command of the Titanic, after it's already hit the iceberg. You have a ship you did not design, a crew you did not train and you're supposed to not only save everyone on board, but also get the ship underway again. I do not envy your task. But there is still a way to succeed. You have an opportunity to choose your own legacy, to improve the culture of TSA and to massively improve aviation security.

Sir, I suggest you do three things: first, understand something every 'coastie' knows in their heart, and that is, no matter how hard you try you can't save them all. Second, make security fit aviation, not aviation fit security. And third, build a system of security professionals who are educated and trained to protect the system. Your Transportation Security Officers, and the passengers will thank you for it.

You will be told that you have to be right all the time, while the terrorists only have to be right once. Nice catch-phrase, but unrealistic as an aviation security strategy. Just as in the Coast Guard, you must define your own success because you can't save everyone. How many terrorists has TSA caught? None. But that's okay, it's not in TSA's mission to catch terrorists. That's the FBI's job. TSA is about deterring crime and terrorism and we can't accurately measure how many people have not attacked aviation because of a deterrent measure, no more than we can determine how many people have not robbed a house because a porch light was left on. We all know that another successful attack is possible - we can no more prevent that than we can prevent how many families decide to go sailing in dangerous weather. There are too many variables to ever have a 100% secure system. So our standard must be: did we do everything in our power, to protect the system while still allowing air transportation to take place? It's about deterrence. I would never suggest we take our foot off the gas, but we must focus on what we can control, which is to provide a layered security system that convinces the bad guy that their attack will either: (a) not be successful, (b) not have a significant impact, and (c) if it is successful and has a significant impact, that we are going to fix what's broke or failed, and carry on - resiliency is a huge deterrence.

Aviation is as essential to the United States just as our power, water, food and other transportation systems. It's not a nicety, nor a luxury. The 9/11 attacks resulted in the near economic collapse of the U.S. When air travel stops, flights are missed, business deals that people are relying on for their livelihood fall through, people lose jobs, the essential medical device doesn't get to the dying patient in time, the once in a lifetime family vacation that is only possible by air, fails to happen, the final trip to see an aging relative or sick child is missed.

The trickledown effect erodes our economy, cuts into our values and eats away at our way of life. For aviation to work, it must move, efficiently, effectively, and as safely and as securely as possible.
as possible. The new IMAX movie, ‘Living in the Age of Airplanes,’ does a great job of explaining how dependent we are on aviation. Trying to protect everything results in protecting nothing and when we change one part of the system it affects the others. Example: backing up screening lines creates other vulnerabilities, and long lines stress out screeners who then miss threats. I know, I was one back in the 80s. [Note: I do understand that TSA is about all modes of transportation security, but you’ll find you spend the majority of your time in aviation, as it’s aviation that the terrorists keep coming back to.]

A top priority to is to ‘seek first to understand, then to be understood.’ Covey’s fifth habit. TSA’s reputation problems with the industry is that no one takes the time to understand how aviation works, and why it must work - prescriptions are written before ever seeing the patient. I am glad to see that you’re already meeting with our key industry and association leaders and are touring airports - just be sure to hit a variety of airports, big and small, because, as they say in our industry, when you’ve seen one airport, you’ve seen one airport.

Aviation security is more than just TSA, screening and air marshals. Another mistake of the past is TSA focus as screening being the only layer of security, even the security layer graphic posted on the TSA website forgets three of the most critical elements in aviation security – airport access control, credentialing and perimeter security - effectively the back door. However, there are hundreds of aviation security experts throughout the US, already working at airports as Airport Security Coordinators - and their expertise is going untapped. They stand by, willing to help - but they need you to understand their world, and they need real engagement.

Engagement with the airport community takes more than just having a block on the organisational chart that says ‘Industry Engagement’. True engagement means building trust to work together to implement effective policies. It means putting forth your commanders’ intent and letting the experts come up with the implementation. It means building a culture of security professionals who are working together, rather than against each other, or worse, ignorant of each other.

I understand that many TSA employees came into the job believing they were the last line of defence against terrorism, but they need to stay in their lane and focus on that very important job. Beware of mission creep - not everyone gets to be the quarterback, but everyone on the team has an essential role.

...H ow M any T errorists H as T SA C AUGHT? N one. B ut T hat’s O Ka y. I T ’s N ot in T SA’ s M ission T o C atch T errorists. T hat’s T he F BI’s J ob...

Beware of false assumptions. I recently heard a statistic from a research study that stated there’s a 1 in 25 million chance of another hijacking. But, the assumptions were that (a) air marshals are only there for transition when the pilot has to use the lavatory, (b) secondary flight barriers were more effective (which they may be - that’s worth revisiting), (c) that the next hijacking would look like the 9/11 hijacking and finally (d) that cockpit doors are some impenetrable force field. Interesting research, but these are dangerous assumptions if one is going to evaluate real threats. Hijackers have been gaining access to locked cockpit doors for decades, and who is to say the next group of hijackers won’t have automatic weapons that have been smuggled on board by airline or airport insiders, and the hijacker won’t have knowledge of the cockpit door mechanisms and how to exploit or override them, or won’t persuade the pilots to open the door? I’m not giving away secret knowledge I’m talking about the TWA 847 hijacking - in 1985. There’s a value to knowing our history.
On 9th September 2009, a single, unarmed man hijacked an Aeromexico flight into Mexico City, with only a fabricated story and a cardboard box. There sadly was no ‘let’s roll,’ no one stepped up to stop him. In fact, some of the passengers didn’t even know the plane had been hijacked.

“...WHEN LONDON WAS HIT WITH BOMBS ON THEIR SUBWAYS AND BUSES IN 2005, THEY DIDN’T HIRE 85,000 PEOPLE AND START SCREENING EVERYONE BEFORE BOARDING...”

Too often we don’t train our personnel in their roles and how the system works. Just the other day, I spoke to three TSOs who did not know the name of the area they were protecting. Consider adding an aviation security textbook into the training curriculums for TSOs, TSIs and your SES levels. I was recently amazed to see an educational programme for TSOs that didn’t include ANY aviation security text, but did include a transportation security text (without an aviation security chapter). If you want aviation security experts, you need to be trained in aviation security - Habit 5 again - aviation is different.

Risk-based security must continue - our biggest enemy is not bombs and guns, but political overreaction. When London was hit with bombs on their subways and buses in 2005, they didn’t hire 85,000 people and start screening everyone before boarding. They utilised other methods to increase security that didn’t eliminate public transportation nor adopt unsustainable strategies that bankrupted the country. Terrorism is like the flu, every season there will be a different strain, so it’s up to us to adjust our tactics as necessary, without killing the ‘patient’ with the vaccine.

Don’t get target-fixed on one threat and ignore the others. Get that your top priority will be screening. So do what’s necessary to fix it. If the existing technology doesn’t work, buy stuff that does. If the people aren’t working, re-train them and if they can’t be trained, then move them out. But, it’s not just about finding prohibited items - it’s about training people to make good decisions and to make them at the lowest level, by educating them on the mission and what they are trying to truly protect. The Coast Guard is exceptional at this, so please show TSA how to do it.

Customer service training, along with a REAL understanding of what aviation security is, and what the TSO role is in it, will go a long way to rebuilding respect. When people feel that there are competent individuals at the checkpoints, making good decisions and following sensible processes, respect, trust and eventually a perspective that ‘these people know what they are doing,’ will slowly start to be rebuilt. This adds tremendous value to deterrence.

We need to get the word out to the police and airport security community on the real threats, so we can focus our limited time, resources and money on the actual threats. I recently heard a Sheriff talk about how astonished he was that he was able to get on a small Cessna 172 airplane and there wasn’t any of the security that he sees at a commercial service airport. He thought this was a gaping security hole that had just gone ignored, and didn’t realise it’s a completely different system. Failing to understand the big threats results in spending money and staff time on lower-level threats.

I’m a believer in the air marshal layer of security - just the thought that they could be on board is a deterrent factor, but it looks like that agency needs some attention. Fix what’s broken there, and add a force multiplier to the air marshal programme by moving forward on initiatives to allow qualified state and local law enforcement officers to carry concealed on commercial flights.

TSA needs to push for real, beneficial change in our industry, not just motion without progress. Biometrics - I’m not talking about at the screening checkpoint, because frankly it’s less of a threat when a bad guy slips through the document check as long as he’s screened and doesn’t do anything. Biometrics needs to roll out first in the airport access control areas, where we don’t have as many layers of physical screening, and where there’s a significant insider threat.

“...TERRORISM IS LIKE THE FLU, EVERY SEASON THERE WILL BE A DIFFERENT STRAIN...”

And speaking of employee screening and inspection, while Atlanta, Orlando and Miami have embraced TSA-style screening for their employees, these airports have huge revenue streams and can afford to do this. Many smaller airports cannot, and there may be more cost-effective ways to conduct employee inspections and get the same result.

I know I’ve outlined a tall order, but there’s a way to accomplish it all. Let’s humour our imagination, and embrace Security Management Systems (SeMS). SeMS is already gaining momentum throughout the world as a practical, strategic approach to reducing risk in air travel, yet TSA and many in our industry still pursues old thinking against threats that have evolved past that level of thought. SeMS
is a way to create a culture shift in TSA, and also enables us to make security fit aviation, instead of aviation fit security. Risk-based security is a move in the right direction and has elements of SeMS within it, so now it’s time to expand this throughout the TSA and the aviation system.

You are already familiar with Safety Management Systems, but unfortunately, I’ve never heard the SeMS term in any of TSA’s vocabulary. Why wait on a programme that moves us away from everyone chasing a soccer ball and moves us toward everyone moving in the same direction, proactive measures, risk assessments so we’re not wasting money on threats that aren’t really threats, determining what works through audits and internal reporting and instilling a real security culture.

"...I CHALLENGE YOU TO RAISE THE REPUTATION, AND THUS THE CREDIBILITY AND DETERRENCE LEVEL OF TSA..."

SeMS may also help get the Transportation Security inspector workforce working more closely with the ASC and air carrier security personnel - true engagement in both word and deed, rather than trying to play ‘gotcha’ games on regulatory enforcement actions and worry about how many access points are closed. That metric needs to be reversed - the effectiveness of a TSI should not be on the most amount of enforcement actions on their airport operator but the least. The philosophy of the beatings will continue until morale improves has never worked. With SeMS there are audit systems that can help ensure that everyone is moving the ball in the same direction, not just engaging in a shell game to avoid regulatory action. I’ve literally met hundreds of your TSIs, who are again, smart people, and who have a lot to bring to the table, once they are given the flexibility in implementing the directives and initiatives, and once trust has been rebuilt at the local levels.

SeMS is more about whether the mission is being accomplished, rather than whether one particular layer is always working. Most airports will not embrace SeMS until its required, as many of the local governments that run local airports, will not support something unless it’s a regulation. It’s up to the TSA to take the initiative, but this will not be without resistance - the problem is, the industry does not yet trust the TSA. The shortcomings of TSA’s active shooter training or the Large Aircraft Security Program experiment have tainted TSA’s reputation and many airport operators no longer believe that TSA has the solution it goes back to seeking first to understand and realising that TSA personnel came into an industry where there were already thousands of aviation security professionals. I’m familiar with the excellent efforts TSA is now making on developing insider threat training, and also familiar with the resistance they are already getting from the airport industry. It’s a case of valuable training that may be eventually watered down because of the lack of trust between the TSA and the industry. Again, it’s about rebuilding trust and that happens when we seek first to understand, when we make our focus on making security fit aviation, not the other way around, and when raise the standards of professionalism.

SeMS can raise the training and performance standards across the board. I remember my military training - there were standards and we were trained to the standards. The military is known for how much training it puts its personnel through whereas after nearly three decades in the civilian side of the house, training is seen as a necessary evil in order to be ‘compliant’, rather than truly prepared. TSA, through industry-wide implementation of SeMS can raise the standards, to a level that the traveling public deserves and expects.

Like it or not, in the industry, Kip Hawley’s legacy was the liquid rule and upgrades to our X-ray systems and body imaging capabilities. John Pistole’s legacy was risk-based security and not worrying about what Congress was running off to chase every other day. I challenge you to raise the reputation, and thus the credibility and deterrence level of TSA, through real industry engagement and a focus on what you can control. Like I learned in USCG OCS, the term ‘Not on my Watch’ recognised that I couldn’t save everyone, but I can save many people, just by focusing on what I can control.

Imagine for a moment, the consummate Coast Guard professional - now, what actions made them a professional? They were trained to high standards, they were highly competent and you could trust them to do the right thing. When a Coast Guard helicopter or ship arrives on scene to rescue a family off a sinking boat, that family knows that everything going to be okay, because they are in the hands of the professionals. They know their commander’s intent, they are experts in their job but stay in their lane unless they need to improvise; they are highly educated and understand the entire system, and their role in it, and they have the freedom to make their own decisions about how to get the job done.

That’s the culture TSA needs and you can succeed by instilling it.

Use SeMS to change the culture of TSA, truly educate the workforce and listen to those in the field about what works and what doesn’t. You can’t prevent every breach, prohibited item or even every attack, but you can build a resilient system of aviation security professionals, that are respected by passengers and are feared by terrorists and criminals. When the bad guys believe that professionals are running the show, they run somewhere else. How’s that for a legacy?

Good luck Sir!

JEFF PRICE
Professor, Metropolitan State University of Denver
Lead Author, ‘Practical Aviation Security: Predicting and Preventing Future Threats’
U.S. Coast Guard 1989-1992