

**Department of Homeland Security:  
An Assessment of the Department and a Roadmap for its Future**

**Statement of Stewart A. Baker  
Partner, Steptoe & Johnson LLP  
Visiting Fellow, Hoover Institution, Stanford University**

**Before the Committee on Homeland Security  
House of Representatives**

**September 20, 2012**

Thank you, Chairman King, Ranking Member Thompson, and distinguished members of the Committee, for this opportunity to testify on the state of the Department of Homeland Security.

This is a timely hearing. We are approaching the tenth anniversary of the Homeland Security Act that created the Department. It's time to ask what the Department has done well, where it has failed, and how it can do better in the future.

**Where DHS Still Falls Short**

I will cut to the chase. The Department's biggest unmet challenge is making sure that its components are working together to the same goal. This was a central objective of the Homeland Security Act. It combined many agencies into a single Department so that all of them would use their authorities cooperatively in the fight against terrorists.

That may seem obvious, but this is Washington, and doing the obvious is not easy. The coordination efforts of a ten-year-old department do not always impress component agencies that can trace their origins to the founding of the Republic.

The good news of the last ten years is that the Department has had three Secretaries who had no doubt about who was running the Department and who insisted on the cooperation of all parts of the Department to implement their highest priorities. The bad news is that, in my view, these accomplishments owe more to the Secretaries' personalities than to the institutions they have built. In general, the offices that support the Secretary, from the various management offices to the office of policy, have not created a framework that can coordinate the big, proud components of DHS on issues that are outside the spotlight of Secretarial attention.

The need to strengthen those institutions is especially pressing now. We face a possible change of leadership at DHS no matter who wins the next election. And the Department faces a difficult budget outlook. Even in a time of record deficits, DHS's budget has hit a ceiling. There is almost no prospect of overall budget increases in the future, and cuts are likely. Budget decisions simply must be based on how each component's expenditures fit

the Department's highest priorities. The Department will have to identify redundancies and may have to eliminate programs with powerful constituencies. If that is not done on the basis of a careful, institutionalized review of the Department's overall strategy, we will not use the scarce dollars that remain in a way that best protects the country. That would be a tragedy.

### **Three Case Studies**

That, of course, is a very general evaluation. Let me be more specific about several important DHS initiatives.

#### **1. Data-based security screening**

One of the Department's unquestionable successes is the way it has unified the government's screening and enforcement on the border, something that was once a side business for three or four departments with other priorities. DHS realized early that it couldn't spend even five minutes with every traveler who was crossing the border. Instead, it had to concentrate on the riskiest travelers, and to do that it needed more information about travelers, as far in advance as possible. As with so much at the Department, this has been a bipartisan priority; Secretary Napolitano has preserved and improved many data programs launched under earlier Secretaries. And DHS's data programs have contributed to the identification and apprehension of several travelers seeking to commit acts of terror on US soil in recent years.

This initiative has been a great success – one that could not have been achieved without the Department. The use of travel reservation (“PNR”) data to screen travelers has come under constant attack on bogus privacy grounds from the European Union, which has torn up its earlier agreement to honor the program every time a new Secretary has been sworn in. And every time, the new Secretary has insisted on maintaining the program.

The Department has also gone on the offensive to get other important data about travelers. Before the Department was created, remarkably, our border inspectors had no way to know whether travelers from other countries had been convicted even of the most serious crimes. Now, thanks to the leverage of the Visa Waiver Program, every participating country other than Japan has a “PCSC” agreement with the US, that will provide access to travelers' criminal records. The Department has also implemented ESTA, a “reservation” system that allows the Department to screen VWP travelers for potential risk before they begin their trips.

The Department has further expanded available information by launching Global Entry, which speeds clearance at the border for travelers who have been vetted in advance. Going forward, it will have background information on frequent travelers from a number of foreign partners, including the Netherlands, South Korea, Germany, Australia, and Brazil. As a result, DHS can focus more resources on riskier travelers.

Finally, DHS has begun gathering more data in foreign airports, successfully posting US government officers there to interview and in some cases to pre-clear travelers, a security-enhancement that benefits both the individual traveler and the host government.

These data programs have improved the efficiency of border screening while also speeding most travelers across the border more quickly. Despite the hostility of privacy campaigners, the programs have proved themselves. There have been no known abuses of the data. This is a success that could only have been achieved by a unified Department. It is a success that DHS can be proud of.

That does not mean that it is perfect. In my view, our international negotiation strategy needs a coherent plan, with priorities, to make sure we get the most important information about the riskiest travelers at least cost to the United States. I also fear that our last PNR agreement accepted too many of Europe's limitations on PNR while surrendering too many protections for the program. And I'm disappointed that we have not persuaded Japan to supply information about the yakuza, or professional criminals, who may be traveling to the United States. But these are tactical criticisms of a program that is a great strategic victory.

Indeed, it is a victory that is paying dividends in airports around the country. Everyone likes to criticize TSA, and one of the most valid criticisms is that it treats all of us like suspected terrorists. What's less known is that this treatment was more or less mandated by privacy campaigners, who persuaded Congress that TSA could not be trusted with the same travel reservation data that our border officials use every day. Lacking any information about travelers, TSA had no choice but to treat them all alike.

Now that the use of data for screening at the border has proven itself, the dam is beginning to break for TSA as well. TSA now has access to each traveler's name, gender, and date of birth. Increasingly, it also knows about the traveler's travel history, based on the voluntary provision of frequent flier data. It has shown how this data allows risk-based variations in screening, using date of birth to reduce screening hassles for children under twelve and seniors over seventy-five. And overseas, in response to the Christmas Day bomb attempt, CBP and TSA are combining forces to do data-based screening of passengers on US-bound foreign flights. Finally, TSA is using Global Entry and other data to create a known traveler screening process for domestic flights.

This is all great progress, though more is needed. In the next five years, TSA should expand its use of data-based screening further, expediting travel for the great majority while demonstrating that it can be trusted with personal data. Because of past privacy limitations, it is likely that TSA will need Congressional assistance to achieve this goal.

## **2. Cybersecurity**

Sometimes it's easier to persuade the team to give you the ball than to actually run with it. That is DHS's problem in cybersecurity right now.

DHS seems to have successfully fended off the many agencies and committees that wanted to seize parts of its cybersecurity mission. Whether DHS can carry out the mission, though, remains uncertain.

Although the Homeland Security Act clearly gave DHS authority over civilian cybersecurity issues, it did not give DHS the kind of trained personnel it needed. Finding talented cyberwarriors is a challenge even for private sector firms. Attracting them to the Department has been doubly difficult, especially with a hiring process that in my experience was largely dysfunctional. The Department's biggest challenge is hiring and maintaining a cybersecurity staff that can earn the respect of private cybersecurity experts. With the exception of a handful of officials, DHS has not yet built a cadre of employees who can match their counterparts at NSA or Goldman Sachs. This is critical. If DHS fails in personnel, it will likely fail in the rest of its cybersecurity-related activities.

There are other challenges for DHS in cybersecurity. They include:

- **Building a better relationship with NSA.** The outlines of a working relationship with NSA are obvious. DHS should provide policy guidance based in law and prudence for any cybersecurity mission affecting the civilian sector, but it must rely heavily on NSA's technical and operational expertise. This fundamental truth has been obscured by personalities, mistrust, and impatience on both sides. It's got to end, especially in the face of adversaries who must find the squabbling email messages especially amusing because they are reading them in real time.
- **Gaining authority to insist on serious private sector security measures.** DHS has plenty of legislative authority to cajole and convene the private sector in the name of cybersecurity. It's been doing that for ten years. The private sector has paid only limited attention. In part that's because DHS had only modest technical expertise to offer, but it's largely because few industries felt a need to demonstrate to DHS that they were taking its concerns seriously. That is one reason that DHS needs at least some authority to demand that industry respond to the cybersecurity threat, especially where it poses risks to civilian life that are not adequately recognized by the market. I fully recognize that cybersecurity measures do not lend themselves to traditional command-and-control regulation, and that information technology is a major driver for economic growth. That's a reason to be cautious about how government approaches the private sector. But it's not a reason for government to ignore the risk of a cybersecurity meltdown. It's worth remembering that, for a couple of decades, we were told that the financial derivatives trade was too complex for traditional government regulation and a major driver of economic growth, and that the private sector could do a better job of internalizing risk than any government regulator. We should not wait for the cybersecurity equivalent of the financial meltdown to give DHS a larger role in cybersecurity standards.

Sometimes the businessmen arguing against regulation are wrong – so wrong that they end up hurting their own industries. I believe that this is true of those who oppose even the lightest form of cybersecurity standards. Most of the soft quasiregulatory provisions that business groups rejected in talks with the Senate will likely be incorporated into an executive order that they will have little ability to influence. Even worse from their point of view, the pressure for legislation is likely to continue -- and will become irresistible if we suffer a serious infrastructure failure as a result of hacking. In that event, the cybersecurity legislation that Congress adopts will have to go beyond the executive order and into the territory of much tougher regulation. By failing to adopt more limited legislation now, Congress is sowing the seeds for more aggressive regulation in the future.

- **Moving beyond the fight over “regulation”.** That said, DHS cannot wait for a national consensus on its regulatory role. There are many other steps that DHS could take to improve cybersecurity without touching the regulatory third rail. Let me outline a few of them here:

- Information-sharing.

It should be obvious why the targets of cyberattacks need to share information. We can greatly reduce the effectiveness of those attacks if we use the experience of others to bolster our own defenses. As soon as one victim discovers a new command-and-control server, or a new piece of malware, or a new email address sending poisoned files, that information can be used by other companies and agencies to block similar attacks on their networks. This is not information-sharing of the “let's sit around a table and talk” variety. It must be automated and must occur at the speed of light, not at the speed of lawyers or bureaucrats.

I supported CISPA, which would have set aside two poorly-conceived and aging privacy laws that made it hard to implement such sharing. I still do. But if CISPA is going to be blocked for a time by privacy objections, as seems likely, we need to ask a different question: Can the automated information-sharing system that we need be built without rewriting those aging privacy laws? I believe that it can; we simply need a more creative and determined approach to the law. Administration lawyers, who have taken an unnecessarily rigid view of existing law, should be sent back to find ways to build automated information sharing under existing law.

- Emphasize attribution.

We will never defend our way out of the cybersecurity crisis. I know of no other crime where the risk of apprehension is so low, and where we simply try to build thicker and thicker defenses to protect ourselves.

The obvious alternative is to identify the attackers and to find ways to punish them. But many information security experts have grown skeptical of this alternative. As they point out, retribution depends on attribution, and attribution is difficult; attackers can hop from country to country and from server to server to protect their identities.

That skepticism is outmoded, however. Investigators no longer need to trace each hop the hackers take. Instead, they can find other ways to compromise and then identify the attackers, either by penetrating hacker networks directly or by observing their behavior on compromised systems and finding behavioral patterns that uniquely identify the attackers. It is harder and harder for anyone to function in cyberspace without dropping bits of identifying data here and there. If our security is inherently flawed, so too is the security of our attackers. This means that it is realistic to put attribution at the center of our response to cyberattacks.

We should take the offense, surrounding and breaking into hacker networks to gather information about what they're stealing and who they're giving it to. That kind of information will help us prosecute criminals and embarrass state-sponsored attackers. It will also allow us to tell the victim of an intrusion with some precision who is in his network, what they want, and how to stop them. DHS's intelligence analysis arm should be issuing more such reports and fewer bland generalities about terrorism risks for local law enforcement agencies.

- Use DHS law enforcement authorities more effectively.

Law enforcement agencies have a vital role to play in cybersecurity – even when the prospect of actually arresting the attacker is remote. Law enforcement agencies have investigative authorities, including search warrants and wiretaps, that can help identify attackers. Those authorities should be used strategically to aid in the overall attribution effort.

The best way to achieve that goal is for DHS's cybersecurity office to be fully coordinated with law enforcement agencies that have criminal investigative authorities. By pooling information, authorities and resources, these agencies should pursue a common strategy—one that identifies the bad guys, first to disable their attacks and eventually to bring them to justice. Coordination between DHS and the FBI may have its challenges, but today it seems that there is only modest coordination even between DHS's cybersecurity office and its own cybercrime investigators. Certainly I have seen no sign that ICE and Secret Service investigations are prioritized strategically based on guidance from the DHS cybersecurity office. The result is wasted opportunities and wasted resources. Instead, ICE and Secret Service cybercrime investigators should be detached to a

task force run by the cybersecurity office as a way of dramatizing the need for an all-of-DHS approach to the problem.

Law enforcement authorities create a second opportunity that we are not fully exploiting. Increasingly, it is law enforcement that tells businesses they have been compromised. But usually the first question from businesses is one best directed towards the cyberdefenders rather than the cybercops: “What can we do to get the attacker out?” This is a “teachable moment,” when all of DHS's cyberdefense and industry-outreach capabilities should be engaged, talking to the compromised company about the nature of the intruder, his likely goals and tactics, and how to defeat them. Currently, however, DHS's cybersecurity office and its cybercrime investigators do not present themselves as a unified team when visiting the victims of attacks. Better coordination within the Department would pay dividends and provide a model for coordination across department lines.

- Recruit private sector resources to the fight.

In my private practice, I advise a fair number of companies who are fighting ongoing intrusions at a cost of \$50 or \$100 thousand a week. The money they are spending is going almost entirely to defensive measures. At the end of the process, they may succeed in getting the intruder out of their system. But the next week, the same intruder may get another employee to click on a poisoned link and the whole process will begin again. It's a treadmill. Like me, these companies see only one way off the treadmill: to track the attackers, figure out who the attackers are and where they're selling the information, and then sanction the attackers and their customers.

When private companies' cybersecurity executives were surveyed recently, “more than half thought their companies would be well served by the ability to ‘strike back’ against their attackers.” W. Fallon, *Winning Cyber Battles Without Fighting*, Time (Aug. 27, 2012). And the FBI's top cybersecurity lawyer just this week called our current strategy a “failed approach” and urged that the government enable hacking victims “to detect who's penetrating their systems and to take more aggressive action to defend themselves.” Washington Post (Sep. 17, 2012).

He's right. But under federal law, there are grave doubts about how far a company can go in hacking the hackers. I happen to think that some of those doubts are not well-founded, but only a very brave company would ignore them.

Now, there's no doubt that US intelligence and law enforcement agencies have the authority to conduct such an operation, but by and large they don't. Complaining to them about even a state-sponsored intrusion is like

complaining to the DC police that someone stole your bicycle. You might get a visit from the police; you might get their sympathy; you might even get advice on how to protect your next bicycle. What you won't get is a serious investigation. There are just too many crimes that have a higher priority.

In my view, that's a mistake. The Department, drawing on the resources of the entire government, should do some full-bore criminal and intelligence investigations of private sector intrusions, especially those that appear to be state-sponsored. We can identify the attackers, and we can make them pay.

But if we want do that at scale, we have to let the victims participate in, and pay for, investigations that the government will never have the resources to pursue. Too many government officials have viewed such private countermeasures as a kind of vigilante lynch mob justice. That just shows a lack of imagination. In the real world, if someone stops making payments on a car loan but keeps the car, the lender doesn't call the police; he hires a repo man. In the real world, if your child is kidnapped, and the police aren't making it a priority, you hire a private investigator. And, if I remember correctly the westerns I watched growing up, if a gang robs the town bank and the sheriff finds himself outnumbered, he deputizes a posse of citizens to help him track the robbers down. Not one of those solutions is the equivalent of a lynch mob or of vigilante justice. Every one allows the victim to supplement law enforcement while preserving social control and oversight.

DHS could probably experiment with that solution tomorrow if it chose, as could the FBI. Its law enforcement agencies often have probable cause for a search warrant or even a wiretap order aimed at cyberintruders. I know of no legal barrier to obtaining such an order, then relying on a private contractor paid by the victims to actually carry out the search or the tap, as long as that happens under government supervision. (The Antideficiency Act, which arguably prohibits the government from accepting free services, has more holes than my last pair of hiking socks, including exceptions for protection of property in emergencies and for gifts that also benefit the donor.)

If systematic looting of America's commercial secrets truly is a crisis, and I believe that it is, why have we not already unleashed the creativity and resources of the private sector that attackers are victimizing?

Mr. Chairman, that concludes my prepared testimony. I will be pleased to answer any questions the committee may have.