Testimony of Stewart A. Baker

Before the Committee on Homeland Security and Governmental Affairs
United States Senate

"The Department of Homeland Security At 10 Years: Examining Challenges and Achievements and Addressing Emerging Threats"

September 11, 2013

Thank you, Chairman Carper, Ranking Member Coburn, and distinguished members of the Committee, for this opportunity to testify on the state of the Department of Homeland Security ("DHS").

This is a timely hearing. DHS has now been in existence for 10 years. We should not expect big shifts in the structure or mission of the Department unless those shifts are driven by the Department's successes or failures. So it is fair to ask what DHS has done well, where it has stumbled, and, especially, how it can do better in the future.

DHS's Failing

I begin with DHS's biggest failing. Despite considerable effort, and even some progress, DHS has not developed the tools and institutions it needs to unify the work of its many components. By saying that, I do not mean to suggest, as some would have it, that DHS is a sprawling and inherently uncontrollable amalgam of agencies. That is wrong. The Department has had many management successes, some of them critical to stopping terrorist attacks. But in many cases, the key to success has been the personal, daily involvement of the Secretary or Deputy Secretary. We have been lucky to have only three secretaries in the last ten years, all of whom have understood how to lead large agencies. They have achieved a lot through force of personality. But personality is not enough. What we need is the equivalent of the Office of the Secretary of Defense – a strong, institutionalized set of offices devoted to carrying out the Secretary's policies and decisions on issues when the Secretary cannot spend time every day on the problem. This should be done by the offices that focus on policy, planning, international affairs, procurement, and personnel, but these have limited authority and staff. They have been hampered by resistance from component agencies, and in many cases from legacy authorizing committees who see any strengthening of the Department's center as undermining their authority and prerogatives.

This issue is especially pressing now, given the leadership changes underway and the difficult budget outlook ahead. After seven fat years in budget terms, DHS is now deep into a cycle of lean years that may stretch far into the future. As we try to do more with less, it's even more important to set policy and budget priorities across component lines. Budget decisions simply must be based on how each component's expenditures fit the Department's highest priorities. For the first time, DHS has to identify redundancies and may have to eliminate or scale back programs that have 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.

Apart from centralizing oversight, there are other steps that can be taken to ensure that the center holds. The assistant secretary for policy should be elevated to undersecretary status, as was intended when it was created. When I held that office, the Secretary and Deputy Secretary treated me as an undersecretary and *de facto* third in command for the Department. But the failure to institutionalize the office's status has made it difficult to sustain that role. That, in turn, has left the Department with a thinner bench and fewer officials who are fully prepared to step in and lead when – as now – the Secretary and Deputy Secretary are gone. Restoring the intended and historic status of the office of policy would help to avoid future leadership crises.

Another way of addressing the looming budget crisis is to make lemonade from it. The same forces cutting DHS's budget are affecting the Department of Defense and the intelligence community. These agencies and their contractors badly need to find new buyers for equipment and technology originally developed for conflicts in Afghanistan and Iraq. DOD and the Intelligence Community have invested billions of dollars in the development and deployment of new capabilities, from sophisticated sensor and surveillance networks to data integration and analysis capabilities, to cybersecurity tools. Many of these technologies are directly relevant to supporting homeland security missions. Customs and Border Protection ("CBP") and the Science and Technology Directorate ("S&T") in particular have taken positive steps in this direction, working with DOD to identify potential solutions. More fully leveraging that which we've already paid for would bolster homeland security capabilities while reducing the need to spend additional taxpayer dollars on new research and development. To facilitate this kind of concerted effort, multiple organizations and actors – from DOD, the intelligence community, and DHS to the private sector and others – will need to work together to identify what equipment and technologies are most relevant and create efficient processes for their transfer and ongoing operation.

DHS's Success: Intelligence-Driven Security Screening

Let me now turn to one of the Department's unquestionable successes – 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 many other priorities.

It's not easy to find a handful of terrorists and criminals in a flood of millions of travelers, especially if you have less than 30 seconds to make the call. DHS quickly realized that taking more time to inspect everyone would not solve the problem. Indeed, DHS could quadruple the wait (and the hassle), and it'd still be trying to find bad guys based on two minutes of scrutiny. As a result, border officials began gathering more background data earlier on all travelers, and they used that data to decide which travelers needed more than 30 seconds of attention.

And DHS's use of advance information at the border – particularly Passenger Name Record ("PNR") data – has produced a number of tangible successes. Faisal Shahzad, the would-be Times Square bomber was pulled off a plane at JFK as it was preparing to leave the country because of PNR data. Similarly, the PNR data of Najibullah Zazi – the guy who rented a truck and drove cross country to set off explosives in the New York City subway – was used to identify the scope of the conspiracy. These are just the public successes. In fact, PNR data has aided nearly every recent high profile terrorist investigation. And, it's not just national security cases that benefit from the use of PNR. PNR also enables more traditional law enforcement operations, identifying, for example, previously unknown individuals involved in narcotics and currency smuggling operations.

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, DHS has information-sharing agreements with dozens of countries. The Department has also implemented ESTA, a "reservation" system that allows the Department to screen risky VWP travelers before they begin their trips. DHS should continue to expand the VWP to partners who are willing to take steps and share information that improve both countries' security.

DHS has further expanded available information by launching Global Entry, which speeds clearance at the border for travelers who have been vetted in advance. There are now nearly 900,000 participants in the program, and just last month the Department announced that vetted citizens from the United Kingdom, Germany, the Republic of Korea, and Qatar are eligible for Global Entry benefits. DHS should be applauded for its efforts to continue to expand Global Entry to include citizens from Brazil, India, and elsewhere. Adding these travelers to Global Entry will not reduce our ability to screen them for terrorism purposes, but it will give us more information to use in the screening process while also speeding most travelers through the checkpoints much faster. Finally, having overcome some State Department resistance, DHS's international operations are increasingly robust. The Department has begun gathering more data in foreign airports, posting U.S.

government officers there to interview and in some cases pre-clear travelers, a convenience that is avidly sought by local governments. It is also working with a growing number of partners – especially in our hemisphere – to enhance coordination and build capacity.

These programs have improved the efficiency and effectiveness of border screening immensely while also speeding most travelers across the border more quickly. But they did not happen without immense effort. Privacy campaigners did their best to kill them. The European Union, which is far more enthusiastic about regulating American security programs than its own security agencies, spent a decade negotiating and then breaking agreements with DHS in the hope of killing travel data programs.

Despite this resistance, 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.

But that does not mean that it is perfect, as the recent controversy over the proposed pre-clearance in Abu Dhabi illustrates. In my view, our international engagement strategy needs a more coherent plan, with priorities, to make sure we get the most important information about the riskiest travelers at least cost to the United States. The criteria also need to be more transparent to our potential foreign partners, many of which are actively seeking engagement. 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 as well. Transportation Security Administration ("TSA") personnel face the same problem securing passenger flights against terrorists, such as Richard Reid, the shoe bomber and Umar Faroukh Abdulmutallab, the underwear bomber. Screening technology, such as a standard metal detector, was unable to detect the explosives used in these plots. Unlike border officials, though, TSA ended up taking more time to inspect everyone, treating all travelers as potential terrorists, and subjecting many to whole-body imaging and enhanced pat-downs. We can't blame TSA for this wrong turn, though. Privacy lobbies persuaded Congress that TSA couldn't be trusted with data about the travelers it was screening. With no information about travelers, TSA had no choice but to treat them all alike, sending us down a long blind alley that has inconvenienced billions.

At long last, however, TSA has begun successfully to implement risk-based screening that takes data and passenger risk into account. Under the Secure Flight program, TSA now receives each traveler's name, gender, and date of birth from the airlines for pre-screening. This data is hardly sensitive, but it has begun to transform passenger screening. Even more encouraging is TSA's TSA Pre✓™ program, which is currently at 40 airports and will be operational at 100 airports nationwide by the end of this year. Participation in TSA Pre✓™ enables the "known" traveler to use a "fast" lane where the most aggravating and time-consuming security procedures have been largely eliminated. Because TSA Pre✓™ is voluntary and has been rolled out cautiously, privacy campaigners have been quiet. To date, more than 15 million passengers have experienced TSA Pre✓™.

DHS should seize this moment to further integrate air and border security approaches so that TSA and CBP both know that a traveler is coming their way in time to plan for screening. While the Department has made great strides towards integration of its various databases, this process is not yet complete. All elements of the Department should have as much information as possible regarding those they are screening, whether that information was originally collected by CBP, TSA, Immigration and Customs Enforcement ("ICE"), or any of DHS's other component agencies.

Such a strategy would not be free of controversy or complication. Because of past privacy limitations, it is likely that DHS will need Congressional assistance to achieve this goal. But the gains in reduced delays, in increased security, and in personal dignity would be significant. No one wants to be against privacy, but we've tried the privacy campaigners' preferred solution, denying even the smallest scrap of data to the government, and they saddled us with ten years of stupid screening at our airports, where a lack of data forced TSA to treat everyone like a suspected terrorist. No one liked that solution, with good reason. It's time to recognize that failure and encourage experiments in smarter, faster, more informed screening based on data-sharing.

During its second decade DHS will face threats and risks beyond terrorism. One area where the risks are certainly growing, and which will require investment of new resources, as well as the assistance of Congress, is cybersecurity and operations. As former Secretary Napolitano rightly noted just before her departure: "More must be done, and quickly."

Work in Progress: Cybersecurity

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

DHS seems to have successfully fended off the many agencies and committees that wanted to seize parts of its cybersecurity mission. Recent presidential orders have given DHS a large role in civilian cybersecurity. This is consistent with the Homeland Security Act, which clearly gave DHS authority over those issues, but that Act does not provide specific or explicit authorization for many of the cybersecurity activities that the Department is now carrying out, especially with respect to protecting critical infrastructure. It is reasonable, then, to codify authority for DHS's existing activities, thereby cementing the Department's role for the future. This basic step may seem obvious, but this is Washington, and doing the obvious is not easy.

That's particularly true when the technology is changing as fast as our attackers change tactics. When I left the Department, it was just getting started on Einstein – an effort to detect malware and other intrusion signatures aimed at the federal civilian agencies. Deployment of Einstein is now widespread, covering perhaps 60% of the federal workforce. Of course, detecting intrusions is not the same as stopping them. Einstein 3A is meant to automate intrusion prevention, and it is just rolling out now. What's more, as security researchers have realized how hard it is to stop attacks at the edge of the network, watching inside networks has become a higher priority, and DHS has taken responsibility for deploying Continuous Diagnostics and Mitigation ("CDM") technology to scan civilian networks for flaws and signs of compromise. These are all necessary and very large programs that pose implementation and turf challenges. Not surprisingly, some agencies have questioned whether DHS has the authority to do what is necessary, and providing a statutory basis for DHS's programs would be a valuable contribution that this committee could make to cybersecurity.

One problem that should be of particular interest to the committee is the risk of conflict between the Federal Information Security Management Act ("FISMA") and CDM. In essence, CDM performs many of the functions that FISMA requires. However, FISMA envisions a paper-centered audit process that is far too slow for the current threat, while CDM performs its audits electronically, on a 72-hour cycle. Everyone recognizes that CDM is better than a paper process, and FISMA should be modified to reflect changes in both the threat and the solution, as well as to make clear that DHS has responsibility for implementing the operationally demanding solution.

These are all complex systems that DHS is essentially running for most of the civilian government. That would be a challenge for an established agency with a veteran workforce, but DHS does not have nearly the number of trained personnel it needs. 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. There are bright spots. Doug Maughan, in the S&T Directorate, has the respect of his counterparts at NSA and Goldman Sachs. Phyllis Schneck, recently named as the Department's deputy undersecretary for cybersecurity, has great technical and private sector credibility in the field. DHS is on the right track, but the way is steep. It must keep expanding its technically competent cybersecurity staff, because that is the foundation of all the other things it must do. That likely means that it must have authority to hire workers in ways that do not fit the standard federal process.

The other challenges for DHS in cybersecurity are many. They include:

Building a clear relationship with NSA.

I am one of the few officials who has worked at a policy level for both the National Security Agency ("NSA") and DHS. There are certainly days and even weeks when I feel like the child of a troubled marriage. But the fact remains that the outlines of a working relationship between DHS and NSA are obvious. As a concerted campaign of leaks has left NSA reeling and mistrusted by the public, it must be clear that on cybersecurity matters affecting the civilian sector, DHS is calling the policy shots. At the same time, DHS must rely heavily on NSA's technical and operational expertise to succeed. 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 authority to cajole and convene 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. 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. But the same could have been said about the financial derivatives trade in 2007. We cannot allow the private sector to cut costs by vastly increasing risk, whether in cybersecurity or in financial markets.

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. Even on their own terms, the businesses lobbying against a substantive cybersecurity bill are likely to fail. Most of the soft quasi-regulatory provisions business groups rejected last year in talks with the Senate were incorporated into an executive order that they had little ability to influence. Those provisions will in turn become the basis for future, harder regulations, particularly if Congress delays action until we have a cybersecurity meltdown.

For now, however, it will be up to DHS to use the soft authorities and the mandate conferred by an executive order with energy and wisdom. And, to be candid, that is a big enough job for the near future.

Action beyond the legislative and executive order.

The legislative stalemate does not mean that DHS can only improve cybersecurity by pushing the private sector to do things it doesn't want to do. There are many other steps that DHS could take to improve cybersecurity without touching the regulatory third rail. Here are some:

Information-sharing. Everyone understands why the targets of cyberattacks need to share information. We can greatly reduce the effectiveness of 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. In a world of zero-day attacks and polymorphic malware, it must be automated and must occur at the speed of light, not at the speed of lawyers or bureaucrats.

I supported the Cyber Intelligence Sharing and Protection Act ("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 blocked by privacy groups, as seems likely, we need to ask whether the automated system we need can be built without falling foul of those aging privacy laws. A more creative and determined approach to the law is needed.

To take one example, many of the privacy rules that restrict sharing can be waived if a service's customers consent to the sharing. Since the purpose of the sharing is to protect the cybersecurity of those same customers, they are highly likely to consent in large numbers. Working with government, service providers could find ways to obtain consent to a data-sharing regime designed to protect both privacy and cybersecurity – all without amending existing law.

This committee can move information-sharing forward by calling on DHS to lead an interagency effort that would work within existing law to improve information sharing by considering the adoption of statutory interpretations, standard customer terms, and other techniques that serve everyone's interest in better cybersecurity.

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 more and thicker defenses to protect ourselves. We started on this Maginot Line exercise because attribution of cyberattacks seemed too difficult; attackers could hop from country to country and server to server to protect their identities.

But that view is out of date. Intelligence agencies have stopped trying to trace each hop the hackers take. Instead, they've found other ways to compromise the attackers, penetrating their networks directly, observing their behavior on compromised systems and finding behavioral patterns that disclose much. In short, we *can* know who are our attackers are. We can know where they live and what their girlfriends look like. That's because it's harder and harder for hackers to function in cyberspace without dropping bits of identifying data here and there. The massive amount of data available online makes the job of attackers easier, but it can also help the defenders if we use it to find and punish our attackers.

Sometimes the best defense really is a good offense; we need to put more emphasis on breaking into hacker networks and gathering 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.

Again, this committee can put DHS at the center of a new emphasis on attribution. Its Computer Emergency Readiness Team and intelligence analysis arms should be issuing more detailed information about the tactics and tools being used by individual attack units and fewer bland generalities for local law enforcement agencies.

Move from attribution to deterrence. The committee could also perform a service by calling on DHS to take the lead in identifying ways to use attribution more effectively to deter cyberattacks. There are many ways to improve deterrence. While the administration has become more open about identifying Chinese cyberattacks as a particular problem, the Snowden affair has made "naming and shaming" less effective in this context. Instead, we should be looking for other ways to identify individual attackers and their enablers and then bring U.S. legal pressure to bear on them. This is a target-rich environment:

- The Magnitsky Act, passed in 2012, imposes trade sanctions on Russian officials for human rights violations they committed in Russia. Yet government-sponsored hackers have been violating the human rights of Americans in the United States, spying on and sabotaging Tibetan rights groups, for example. How can it be that we are doing more to punish human rights violations in Russia than right here at home? Sanctions of this sort can be imposed on the basis of intelligence that remains classified, and it does not require legislation. It requires only that the Administration consider cyberattacks to constitute an economic emergency.

- Some of the hackers identified publicly by private security researchers do business in the West. Others may have jobs with Chinese multinationals. Some got their start as hackers at Chinese universities.

> This creates an opportunity. Foreign multinationals and universities need visas to come to the United States. Before we issue visas to entities that have hired or enabled the hacking of American companies, we should require them to cooperate in our efforts to identify and penalize hackers.

Use DHS law enforcement authorities more effectively. The law enforcement agency most associated in the public mind with cybercrimes is the Federal Bureau of Investigation ("FBI"). This is a little odd because two DHS law enforcement agencies, the Secret Service and ICE, both have strong cybercrime units and may between them handle as many cases as the FBI.

My concern is not who gets the credit for these investigations. But we cannot let law enforcement determine our cybersecurity posture. Agencies like the FBI and Secret Service only occasionally solve hacking cases, and even more rarely are they able to actually arrest the hackers. If they are allowed to hoard evidence of cyberintrusions, we may lose valuable intelligence about the intruders' tactics and targets. This committee should consider legislation calling for a coordinated approach to all computer intrusions to ensure that detailed information sharing occurs across agency lines. At the same time, it is often law enforcement that tells businesses they have been compromised. 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. But that happens less than it should, judging by the experience of my clients. A deeper, Congressionally mandated coordination would make these encounters far more useful to the private sector.

Finally, I fear that letting law enforcement take the lead on a case-by-case basis means that investigations are not being prioritized in ways that would maximize their intelligence value. (Since these investigations rarely lead to prosecutions, using criminal authorities to gather information about attackers should be a particularly high priority – even when there is no prospect of criminally prosecuting the attackers.) While interagency coordination with the FBI can be a challenge, coordination between DHS's cybersecurity offices and the ICE and Secret Service investigators also seems to be equally *ad hoc* at best. This committee should consider requiring DHS's law enforcement agencies to work computer crime cases under the coordinating and deconflicting authority of the National Protection and Programs Directorate ("NPPD") to ensure strategic use of law enforcement authorities and proper sharing of information.

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 $50,000 or $100,000 a week. The money they are spending is almost entirely defensive. 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 is a treadmill. Like me, these companies see only one way off the treadmill: to track the attackers, to figure out who they are and where they're selling the information, and then sanction both the attackers and their customers. But under federal law, there are grave doubts about how far a company can go in tracking their attackers. I think some of those doubts are exaggerated, but only a very brave company would ignore them.

Now, there's no doubt that U.S. 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 higher priority attacks.

In my view, that's a mistake. The United States should do some full-bore criminal and intelligence investigations of private sector intrusions, especially those that appear to be state-sponsored.

But if we want a solution that will scale, we have to let the victims participate in, and pay for, the investigation. Too many government officials have viewed 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 is 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. Every one allows the victim to supplement law enforcement while preserving social control and oversight.

DHS very likely has sufficient authority to try that solution tomorrow, as does the FBI. DHS's law enforcement agencies often have probable cause for a search warrant or even a wiretap order aimed at cyberintruders. But they rarely have the resources to use that authority fully and strategically against the intruders. I know of no legal barrier to relying on private resources to conduct a deeper investigation under government supervision. (The Antideficiency Act, which prohibits acceptance of 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 done this?

I understand the concern expressed by some that we cannot turn cyberspace into a free-fire zone, with vigilantes wreaking vengeance at will. No one wants that. Government should set limits and provide oversight for a true public-private partnership, in which the private sector provides many of the resources and the public sector provides guidance and authorities. The best way to determine how much oversight is appropriate is to move cautiously but quickly to find alternatives to the current failed cybersecurity strategy. Again, this committee can move the ball forward by authorizing DHS and its law enforcement agencies to develop a pilot project – working with hacking victims and their security firms to use government authorities in a cooperative fashion.

Use existing funds to improve state and local cybersecurity preparedness. There may still be low-hanging fruit in the Department's budget to improve cybersecurity. For example, we can make it easier for state and local governments to use existing grant funding to beef up their cybersecurity. Over the last decade DHS has provided billions of dollars to state and local governments to fund the purchase of a wide range of security capabilities. Cybersecurity tools – from installing basic firewalls to deploying advanced defenses that rely on virtual "detonation chambers" – are allowable purchases, along with hazmat suits and interoperable communications tools. However, DHS can do more to encourage state and local governments to spend grant funds on cybersecurity, and Congress should support those efforts.

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