



Homeland Security

[Subscribe](#) | [Contact Us](#) | [Site Map](#)[Home](#)[Topics](#)[How Do I?](#)[Get Involved](#)[News](#)[About DHS](#)[Home](#) » [News](#) » **Secretary of Homeland Security Janet Napolitano's Third Annual Address on the State of Homeland Security**

News

[Blog](#)[Comunicados de Prensa](#)[Data](#)[Events](#)[Fact Sheets](#)[Multimedia](#)[Press Releases](#)[Publications](#)[Speeches](#)[Testimony](#)[Media Contacts](#)[Social Media](#)

Secretary of Homeland Security Janet Napolitano's Third Annual Address on the State of Homeland Security: "The Evolution and Future of Homeland Security"

Release Date: February 26, 2013

Washington, D.C.

The Brookings Institution
(Remarks as Prepared)

Thank you for that introduction, Elaine, and thank you all for the warm welcome. It's a pleasure to be here this morning. As most of you know, in a few days, we will mark the 10th anniversary of the Department of Homeland Security.

And while ten years may not sound like a long time in the lifespan of a Federal department, it's a significant milestone, as well as an opportunity to consider just how much has changed in that time.

The attacks of 9/11 served as the impetus for the creation of DHS, and also brought to light the changes to our world that had been building for many years ... changes that required immediate action ... and a fundamental shift in how to keep the nation safe.

Our security posture in these difficult times was, in many ways, a necessary function of protecting our nation from threats that we were just beginning to understand. In that way, the immediate post-9/11 period and the early years of the Department were a kind of DHS version 1.0 ... the foundation for much of what has developed since.

Over the past four years, we've seen a second phase of the Department's development and advancement – DHS 2.0 – with stronger partnerships with all involved with homeland security, including government, law enforcement, first responders, the private sector, and the public, at every level.

We now reach our next era – DHS 3.0 if you will. And as you'll see, the software metaphor isn't really accidental at all. So for this, my third annual State of Homeland Security address, I want to talk a bit about the significant change we've seen over the past ten-plus years, and some of the considerable progress that we've made in that time.

To be clear, this isn't the traditional report about the state of the Department. It's about the state of our nation's homeland security. It's the state of a concept that, before 9/11, only existed on paper within a few think tanks, like here at Brookings.

Today, a decade after the creation of a Cabinet-level agency bearing that name, homeland security has come to mean much more ... it means the coordinated work of hundreds of thousands of dedicated and skilled professionals, and more than ever, of the American public, of our businesses and families, communities and faith-based groups.

It's the collective effort of all of these on which I report today.

Pre 9/11

Our nation emerged from the tragedy of 9/11, and with the benefit of hindsight, we now know how multiple failures contributed to those attacks. Intelligence failures prevented us from uncovering the details of al-Qaeda's plot ahead of time, and institutional barriers prevented what limited information we did have about the hijackers from being shared among authorities, and, therefore, connecting the dots.

Weaknesses in our visa and border entry procedures enabled some of the terrorists to lawfully enter and stay in the United States using fraudulent documents, or by providing false information. Gaps in our aviation security system allowed them to board aircraft and carry out

the plot; once we learned of the hijackings, a lack of coordination slowed our response.

And despite the heroism of first responders on the ground, larger, systemic problems, like a lack of emergency communications, hindered rescue operations. In other words, pre 9/11, our state of security was reactive and disjointed, with ad hoc intelligence-sharing, overwhelmed and ineffective border and immigration processes, lack of partnerships among law enforcement, and too much focus on investigation after the fact instead of prevention and protection.

I saw this firsthand. On 9/11, I was Attorney General of Arizona, and I can attest to the many questions we had in those first hours, and the gaps that existed, between the Federal government and the states. Addressing these fundamental gaps was the driving force behind the creation of the Department of Homeland Security ten years ago.

DHS 1.0

I think any discussion of the history of DHS must first begin with an acknowledgment of the critical work of my predecessors – Governor Tom Ridge and Secretary Michael Chertoff. They and their leadership teams had a monumental undertaking on their hands ... bringing together the original 22 agencies that formed the department and integrating their functions, against a backdrop of continued terrorist threats from at home and abroad.

The early years of the Department led to many important innovations and enhancements – from major improvements to our aviation security system, including federalizing our screener workforce, to the creation and use of a single US Government known or suspected terrorist watchlist to screen travelers, establishing a biometric entry system at ports of entry, and other major advancements in port, cargo, and border security. This was tough work, and a lot of credit should go to all of the men and women who helped build DHS over its first several years.

DHS 2.0

When I became secretary in 2009, we looked hard at how we could build on this progress and accelerate it further ... in essence, create DHS 2.0. Fundamental to this was the recognition that even though we had made significant progress since the 9/11 attacks, the threat landscape was constantly shifting and we needed to stay ahead of it.

We still faced threats from al-Qaeda, and other foreign-based terrorist groups inspired by their ideology. Indeed, we better understood how terrorist threats on the other side of the world could affect our homeland, with far-reaching consequences to our global systems of trade and travel, communications and finance.

We were also confronting the reality of homegrown threats, including from individuals who may have no particular connection to terrorism, but nevertheless can threaten our cities and communities, our schools, and our places of worship. And so what we've spent the past four years putting in place is something completely different – an approach that is more efficient, risk-based, and designed to detect, prevent, and respond to a range of threats – from terrorist attacks to natural disasters.

This approach is built upon the notion that in a world of evolving threats, we can no longer simply be reactive or isolated. We have to leverage information to identify threats sooner, target our security measures to areas where they will have the greatest impact in decreasing risk, allocate our resources according to risk-based priorities, and engage a full range of partners in our work.

Terrorism

A good example is how we've brought this thinking to our founding mission – protecting against a terrorist attack. We know it is essential not only that information is shared among relevant agencies, but also that law enforcement and frontline personnel at all levels: internationally, in our states, cities, and communities, as well as those who screen passengers and cargo and protect our borders, have a comprehensive understanding of threats. And ... *and* ... that we get them that information in real-time.

This is the driving force behind the integration of our intelligence sharing and analysis capabilities, to fix gaps such as those exploited by Umar Farouk Abdulmutallab in trying to down a U.S.-bound airliner on Christmas Day in 2009. This is also the driving force behind our support for the national network of fusion centers that serve as centers of information-sharing and analysis among state and local law enforcement.

And we see the results of this collaboration every day. For example, after the attempted bombing in Times Square in 2010, information from state and local databases was shared between fusion centers, which aided the investigation and helped law enforcement identify possible associates.

Border Security

We have applied this data-driven, risk-based model to how we secure our borders – land, air, and sea – and how we enforce our immigration laws as well. Today, a single, unified agency secures our ports of entry and ensures the flow of travel and trade. Our officers are better trained, and we have invested in technology and infrastructure improvements to help expedite lawful travelers and cargo.

We have also deployed historic levels of staffing and technology along our land borders, and as a result, we have a far better ability to detect, deter, and apprehend those trying to illegally enter our country, including through aerial surveillance of the entire Southwest border. As a result, illegal immigration attempts are now at 40 year lows.

Immigration Enforcement

Likewise, we now enforce our immigration laws according to common sense priorities focused on the greatest threats to our communities. Previously, that was not the case, meaning a college student who came here with her parents when she was a child was considered the same priority as a drug smuggler.

This has changed. Last year alone, we removed more than 250,000 criminals from the United States, a record amount. At the same time we have ensured that our immigration officers can use discretion when deciding what cases we prioritize for removal.

For example, we established a process to allow young people brought to the United States illegally as children to request consideration of deferred action for a period of two years, subject to renewal, and, as a result, apply for work authorization. And we have engaged in historic efforts against human traffickers, counterfeiters, and those that violate and steal our intellectual property.

Cybersecurity

There's perhaps no better example of how DHS has evolved to address new and evolving threats than the issue of cybersecurity. The cyber realm wasn't even a major focus of the early Department. Now, it is one of our five core mission areas.

Cybersecurity has come to affect almost every aspect of modern life. All of us depend on cyber-controlled systems for energy, communications, transportation, and defense. Over the past four years, we have built and deployed systems to detect intrusions and defend federal cyber networks. We have expanded our 24/7 watch center, the NCCIC. We have comprehensive plans in place to manage cyber incidents.

And to stay ahead of rapidly-evolving threats and technology, we are moving aggressively to recruit, educate and train our cyber workforce for the future, with the skills and talents we need to tackle this problem in the years ahead.

Disaster Preparedness and Response

Just as we have adapted to meet evolving threats to aviation and border security, and cyber networks, we have also transformed our disaster response system to better meet the needs of disaster survivors. Over the past four years, we have led the Federal government's response and recovery efforts to support state, local and tribal communities in 285 major disasters.

In addition to devastating floods, wildfires, and tornadoes, we have seen other major natural disasters like Hurricane Sandy. And we have dealt with unprecedented, complex events like the BP Deepwater Horizon oil spill.

We have helped to rebuild FEMA into a strong, agile, and capable agency. Likewise, we've helped communities build a culture of preparedness ... a culture that recognizes that the American people are not a liability to be protected, but a tremendous asset to be leveraged. I am proud of how today's FEMA, and all of DHS, have dealt with these disasters, like Sandy, and I believe the reforms we've made over the past four years have made DHS and FEMA the best disaster response agency in the world.

DHS 3.0

So the obvious question is where do we go from here? How do we move from our "DHS 2.0" accomplishments of countering terrorism and improving border security, from smarter immigration enforcement to stronger cybersecurity and capable disaster response and recovery ... to Homeland Security 3.0. What does that look like?

The work we've done, I think, provides a stronger foundation than ever to address the inevitable challenges we will face, and an ever-changing threat landscape. And we know that these challenges will evolve, requiring a nimble and flexible response by the Federal government, and by the many partners we engage across the country, and, increasingly, around the world.

They will require that we continue strengthening our nation's capabilities to prepare for, respond to and recover from threats and events of all sizes, whether from Mother Nature or those seeking to do us harm. And, I think we must do even more to inform and engage the public in this shared responsibility for our safety and security.

Agility and resilience. Engagement and integration. These are some of the key principles that will define Homeland Security 3.0.

We must continue to embed our risk-based approach within everything we do. One key way is by smartly using information and intelligence analysis to allow us to focus our time and energy on people and cargo that pose the greatest risk, and in a manner where we can have the

greatest ability to protect these systems. Our goal in supporting a risk-based approach to security is not only to keep our country more secure, but also to facilitate the lawful travel and trade that drives our economic growth.

In other words, if we're looking for a needle in the haystack, an approach that is risk-based allows us to start looking through a much, much smaller stack while doing away with a cumbersome one-size-fits-all method. The continued development of cutting edge security technologies will certainly aid in this regard.

And we must be able to remain flexible and agile, with the ability to deal with multiple, simultaneous threats or events by leveraging the national capability we have built at all levels – federal, state, local, tribal, and territorial – and with our many international partners, as well as those in the private sector as well. Let me walk you through just a few examples of how we are doing this today, and where our priorities will be.

Trusted Travel and Trade

One area in particular must continue to receive our sustained attention, and that is aviation, where we've seen a range of attempted attacks since 9/11. Following the 2009 Christmas Day plot, DHS launched a global initiative to address existing vulnerabilities in international aviation, because as that attack demonstrated, a vulnerability in any part of the international system can put the entire global network at risk.

With international organizations like the International Civil Aviation Organization (ICAO), we worked to improve information sharing, encourage deployment of advanced screening technology, and the development of international security standards. These kinds of steps will not only help us close gaps in aviation, but they will allow us to find new ways to build on the foundation we have laid.

For example, expanding the screening travelers using Advance Passenger Information/Passenger Name Records, what we call API/PNR with more countries, and sharing the results will allow us to identify potential threats earlier and increase our ability to take action before they board an aircraft to come to US.

And by greatly expanding trusted traveler initiatives like Global Entry and TSA Pre-check with an eye toward expediting screening for even more passengers, as we've done for children **12** and **under** and seniors **75** and older, we can focus our efforts on those who we don't know as much about, and those who pose the greatest risk.

In the coming months, TSA will work to develop additional programs that expand risk-based security initiatives to additional populations. In fact, by the end of 2013 TSA expects that one in four passengers will qualify for expedited screening, up from 1 in 12 last year

Immigration Reform

Another area of great importance for us, and, of course, for the future of our nation is achieving commonsense immigration reform. Our immigration system has been broken for too long, and the time to fix it is now. As the Chair of our Senate Authorizing Committee, Senator Carper, just told me on our recent trip to the Arizona border, it's time for Congress to stop giving us more buckets and instead, fix the ship.

Our communities, workers, and employers are all frustrated by a system that treats a drug smuggler the same as a high-achieving student, undercuts honest employers, and leaves millions in fear of deportation and vulnerable to fraud and other crimes.

This system makes it harder for law enforcement to focus on the greatest threats in their communities, instead spending time and resources on low-priority cases. Last month, President Obama put forward a set of principles that he believes will address the long-standing problems with our immigration system.

The President's principles support stronger, sustained border security and immigration enforcement. In fact, the most effective way to achieve greater border security is through common sense immigration reform that strengthens employers' accountability and that updates our legal immigration system.

The priorities laid out by the President also gives us better tools to focus on employers who hire illegal labor, and by doing so, create the market demand for illegal immigration. They would provide a rigorous pathway to earned citizenship for those already here. And we would significantly improve the legal immigration system.

Common sense reform will help eliminate the main driver of illegal immigration – the desire to find work. As we make it easier for businesses to get the workers they need legally, and more difficult for undocumented workers to find jobs, it will relieve pressure on the border and reduce illegal flows.

And that will enable law enforcement to keep their focus on those who pose national security or public safety threats, including narco-traffickers, human smugglers, and transnational criminal organizations. The time to modernize our immigration laws is long overdue, and we stand ready to work with Congress to achieve this important goal for our country, the American people, and all those seeking to contribute their talents and energy to our great nation.

Cybersecurity

One of the most important areas where we are investing greatly is the future of cybersecurity. We have made it a top priority to help build a 21st century cyber workforce – the next generation of skilled individuals who want to come to DHS, make an impact, and serve their country in this important field.

Beyond that, however, we also need the public and private sector to work more effectively to tackle two key challenges: improving real-time information sharing while protecting individual privacy and civil liberties, and promoting adoption of cybersecurity best practices for our nation's core critical infrastructure.

We need greater information sharing so that the government can learn from the private sector, where people fight this threat every day. And we need to ensure that the government can use information at various levels of classification to help the private sector protect itself.

The Executive Order President Obama issued earlier this month takes some important steps towards greater cybersecurity. For decades, industry and government have worked together to protect the physical security of critical assets that reside in private hands, from airports and seaports to national broadcast systems and nuclear power plants.

There is no reason we can't work together in the same way to protect the cyber systems of our critical infrastructure upon which so much of our economic well-being, national security, and daily lives depend.

Engaging the Public

In all areas – whether protecting our aviation sector, cyberspace, or our communities, we recognize that the public has an important role to play in our shared security. It is why we created a national "If You See Something, Say Something," campaign to encourage citizens to report suspicious activity to local law enforcement.

It's why we launched Stop.Think.Connect. to raise awareness of cyber security so that good cyber practices become as routine as putting on a seat belt. And it's why we need to keep updating old systems with modern means of communication.

For example, FEMA's smartphone apps, and social media tools make it easier than ever to access critical information about what to do before, during, and after a disaster. DHS 3.0 requires us to do more than ever to reach the public we serve by the multiple means of communications they use.

I'll close by saying that this is a story, I think, of evolution and progress, and of lessons learned. The state of our homeland security is stronger because of these efforts.

In ten years' time, our operations have become more cohesive, and our workforce better trained. And today, we benefit from the experience of the more than 50,000 veterans who work for the department. Crises and disasters have tested our capabilities, but also provided valuable experience, and, in many ways, proved the mettle of this young Department.

At the same time, we're inserting the administrative nuts and bolts of a large, new agency. And here too I believe we've achieved notable milestones... from creating an acquisition review board and conducting technology portfolio reviews, to a new Honors program, to internal leadership development, and scholarship programs that span our many missions and components.

In 2009, I launched an Efficiency Review to look across the department's agencies and functions to identify ways that we could reduce expenditures while maximizing our effectiveness.

Driven by employee ideas and executed by cross-component employee teams, ER has led to more than \$4 billion in savings and cost avoidances that has been reinvested into our critical missions. All large organizations must continually strive to improve, and we are constantly looking for ways to become more efficient and effective at the same time.

Nonetheless, we will strive to succeed – our nation deserves no less. So on behalf of the hundreds of thousands of men and women ... the Coast Guardsman who rescues a sailor; the TSO who keeps a loaded gun off a plane; the cyber expert who prevents harm to our banking system; the FEMA worker who comforts a destitute family; the Border Patrol agent who spends days and weeks in 100 degree plus temperatures patrolling our border; the scientist who figures out a better way to protect a plane; and other example upon example.

We commemorate our beginnings; our maturation; and our future. This is not a day just to look back and pat ourselves on the back. It's a day to re-commit and to move forward. It's time for Homeland Security 3.0.

###

Review Date: February 26, 2013



U.S. DEPARTMENT OF
HOMELAND SECURITY

TOPICS

- [Border Security](#)
- [Citizenship and Immigration Services](#)
- [Civil Rights and Civil Liberties](#)
- [Cybersecurity](#)
- [Disasters](#)
- [Economic Security](#)
- [Homeland Security Enterprise](#)
- [Homeland Security Jobs](#)
- [Human Trafficking](#)
- [Immigration and Enforcement](#)
- [International Engagement](#)
- [Law Enforcement Partnerships](#)
- [Preventing Terrorism](#)
- [Transportation Security](#)

GET INVOLVED

- [Blue Campaign](#)
- [Citizen Corps](#)
- [If You See Something Say Something](#)
- [Ready.gov](#)
- [Stop.Think.Connect.](#)
- [U.S. Coast Guard Auxiliary](#)

HOW DO I?

- [For the Public](#)
- [For Businesses](#)
- [For Travelers](#)
- [At DHS](#)
- [A-Z Index](#)

NEWS

- [Blog](#)
- [Comunicado de Prensa](#)
- [Data](#)
- [Events](#)
- [Fact Sheets](#)
- [Media Contacts](#)
- [Multimedia](#)
- [Press Releases](#)
- [Publications](#)
- [Social Media](#)
- [Speeches](#)
- [Testimony](#)

ABOUT DHS

- [The Secretary](#)
- [Budget & Performance](#)
- [Careers](#)
- [Contact Us](#)
- [Doing Business with DHS](#)
- [History](#)
- [Laws & Regulations](#)
- [Mission](#)
- [Organization](#)

SITE LINKS

- [Contact Us](#)
- [DHS Component Websites](#)
- [En Espanol](#)
- [Privacy Policy](#)
- [Notices](#)
- [Plug-in](#)
- [FOIA](#)
- [Inspector General](#)
- [Site Map](#)
- [GobiernoUSA.gov](#)
- [USA.gov](#)
- [The White House](#)