Testimony before the House Committee on Homeland Security

"A Time of Transition: Supporting DHS's Evolution to a Risk-Based Security Model"

A Statement by:

Rick "Ozzie" Nelson
Vice President for Business Development
Cross Match Technologies

Friday, February 15, 2013
311 Cannon House Office Building

A Time of Transition:
Supporting DHS's Evolution to a Risk-Based Security Model

Rick "Ozzie" Nelson
Vice President for Business Development
Cross Match Technologies, Inc.

Testimony before the Committee on Homeland Security
U.S. House of Representatives
Friday, February 15, 2013

Since its creation a decade ago, the Department of Homeland Security (DHS) has been tasked with variety of missions but one primary focus; protecting the United States of America from al Qaeda and its brand of Islamist terrorism. Following the horror of 9/11, we vowed to never again let such an attack take place on American soil, and so we created DHS and gave it the mandate to prevent any and all terrorism in the United States. For much of the last decade we were willing to largely maintain this approach, given the continued threat posed by al Qaeda and relatively robust federal budgets. We didn't make hard choices regarding what was or wasn't working or where to focus our efforts and resources because we didn't need to and we thought we were safer in not doing so. However, in recent years our budgets have shrunk, and the threats we face have shifted. Times have changed, and DHS will, by necessity, need to change with them.

In order for DHS to continue to protect the homeland during this period of limited budgets, we as a nation will need to accept the basic but vital fact that we cannot guarantee and cannot afford to try to provide absolute security from all things for all people at all times. Instead, we must embrace an approach to protecting the nation through risk-based security. This will require identifying where the greatest risks to our security are, and allocating limited resources against those risks. In doing so, we will allow DHS not only to better adapt to shrinking budgets by cutting spending on low-probability, low-consequence threats, but increase our security by better utilizing available funds to prepare for those threats that pose the greatest risk and consequence. Risk-based models are not a new concept, and have been proposed in some form by every recent administration. However, in the past we simply have not had the political will to implement such models, given that they do carry with them an inherent degree of risk. Yet the silver lining of the current fiscal climate is that it has forced us to look past these political hurdles, presenting us with an opportunity to fully embrace a risk-based approach.

The first step in the path towards implementing an effective risk-based model for homeland security is recognizing the fact that al Qaeda, which has consumed our attention and the majority of our homeland security resources for the past decade, likely no longer constitutes the threat to the Homeland that it once did. Al Qaeda has been decimated by the death of bin Laden and dismantling of al Qaeda core, and while recent events in West Africa have made clear that affiliated groups such as al Qaeda in the Islamic Maghreb remain cause for concern, the threat of another terrorist attack in the United States approaching the scale of 9/11 has been vastly diminished. Yet even as the threat of al Qaeda recedes, new challenges are emerging that will require shifts in the Department's resources and focus. As such,

DHS will need to continue to find new efficiencies in its efforts to protect the United States by focusing on identifying emerging risks while refining its calculus regarding existing risks.

In order to do so, DHS will need to continue to accelerate its focus on information and intelligence sharing. A risk-based model of security is inherently driven by information and intelligence, which enables policy-makers and analysts to make informed decisions on where risk is highest. Therefore, as DHS increasingly transitions to a risk-based model, the concept of homeland security intelligence must be refined and the Department's role as the primary conduit for information sharing with state and local governments and the private sector must be further solidified. This begins with the network of fusion centers

Fusion centers, established since 9/11, will become all the more valuable as the Department transitions to a risk-based model. Fusion centers have a vital role to play in supporting information sharing, serving as the primary point of interaction between the federal government, the state and local entities most likely to witness suspicious terrorism-related activity, and private industry, which owns 85% of the nation's critical infrastructure. While the current architecture and number of fusion centers may not be fully optimized, they will continue to play a valuable role in information sharing, and must not be abandoned. As such, DHS must take steps to ensure that increased controversy over how these centers are employed does not threaten their continued utility. The Department and other federal agencies must accept that state and local entities will only be willing to continue to participate in fusion centers if they add value beyond counterterrorism and must work together to strike a working balance between counterterrorism and all-hazards missions. The Department should also encourage state and local partners to participate in standardized intelligence training, in order to equip those on the ground with a better understanding of the intelligence process and equalize some of the disparities between various fusion centers. Additionally, the fusion centers need to find a means to better engage with the private sector. This includes not only finding new avenues for integrating information provided by the private sector, but keeping private companies and businesses informed of potential threats in a useful and timely manner while remaining cognizant of privacy and civil liberties concerns. Fusion centers have the potential to play a vital role in building a risk-based model of security but will be hampered in their mission unless the Department and its partners can come together to address these challenges.

In addition to intelligence and information sharing, the effective screening and credentialing of individuals seeking access to everything from air travel to computer systems is vital to a risk-based approach. An effective, efficient means of screening and credentialing would allow DHS to allocate its resources against those who potentially pose the greatest threat. However, responsibility for screening and credentialing is currently spread across multiple agencies within DHS who employ multiple, unique systems. This diffuse model is inefficient and, as demand rises and budgets fall, will increasingly become untenable. For the Department's screening and credentialing services, which also rely on intelligence and information, the way ahead may lie with an enterprise approach. At present, the multitude of systems being utilized contributes to redundancies. Furthermore, without full integration, there is the danger that vital existing information in one system will be overlooked when making a decision based on information in a second system. Integration of all DHS databases should be accelerated so that all elements of the Department have as much information as possible regarding those they are screening and credentialing. Screening and credentialing processes also could benefit substantially from greater automation. The further introduction of automated processes could significantly reduce the time needed for many tasks associated with screening and credentialing, greatly improving efficiency. Programs like Transportation Security Administration's Pre-Check and Customs and Border Protection's Global Entry should also be expanded to include a greater number of trusted travelers from a variety of

sources. Further, trusted travelers enrolled in one program should be provided an ID number or biometric profile that would be recognized across programs, greatly increasing interoperability while decreasing the resources spent screening those who have already been screened by another program. By streamlining screening and credentialing, DHS can not only increase security, but save limited budget dollars. Secretary Napolitano recently stated a goal of having 50% of travelers enrolled in a Trusted Traveler program within two years. This goal should be embraced and supported by Congress.

Additionally, the Department should examine the creation of a Department-wide targeting center for the analysis of screening data from across DHS. While various component agencies maintain their own analytic targeting centers, no single agency has a complete picture of all the information residing in the Department's many screening and credentialing systems. A DHS-wide center could provide a more complete view, putting together pieces that other, smaller centers might miss, creating a more complete picture of the risks the Department must counter.

Even as the Department attempts to focus on those areas that present the most risk, it must still seek to find efficiencies in areas where threats are relatively low but could be disproportionately costly, most notably with regards to chemical, biological, radiological, nuclear, and high explosive weapons (CBRNE). In recent years, the U.S. has built an extensive network of capabilities, program, and offices intended to detect and respond to these weapons, yet many of these are not well integrated with one another, leading to significant inefficiencies. Integration of all CBRNE research and development under one entity, such as DHS Office of Science and Technology (S&T), would be a logical first step and would reduce costly R&D redundancies. Additionally, the various components involved in CBRNE detection and response would greatly benefit from an integrated information sharing architecture as the National Information Exchange Model (NIEM) as well as integrated technologies that can quickly connect and share data between the various agencies and departments involved. This integration could well serve to both reduce costs and increase security in the long term by reducing duplication and increasing coordination.

As DHS moves into its second decade, it will also face new threats and new risks beyond terrorism. One area where the risks are certainly growing, and which will require a series of new investments, is cyber-security and operations. In addition to the threat posed to our critical infrastructure, General Keith Alexander, Commander of USCYBERCOM and director of the National Security Agency, recently noted that intellectual property theft represents "the greatest transfer of wealth in history," leeching billions of dollars from the nation's economy each year. As such, DHS will need to take a variety of steps to meet this new risk. One cyber-security measure which would be relatively easy to implement would be for DHS to establish a basic training program for federal employees across the U.S. government instructing them on how to identify, understand, and report suspicious cyberactivity. Such training would not only reduce the risk that a given employee would become the victim of a cyberattack, but by emphasizing reporting of attempted attacks, would increase the speed at which information regarding the attack could be disseminated, allowing government and industry to identify the areas of greatest risk more quickly and move to prevent attacks on other systems before they can have an effect. While cyber-education alone is far from sufficient to meet the threat, it would be a valuable and relatively cost-effective step in reducing the emerging risk of cyberattack.

At times, risk-based security will necessitate significant long-term investments in order to meet growing challenges, such as increasing activity in the Arctic. As Arctic sea ice recedes, opening the region to increased traffic, exploration, and territorial competition, the U.S. Coast Guard (USCG) will likely be stretched to the breaking point. In recent years, the Coast Guard has been operating at an increased

operational tempo even as the vessels they rely upon have grown more and more outdated. The average age of a Coast Guard cutter is a worrying 43 years, yet in the past decade the USCG has been called upon for ever-expanding range of missions, running the gamut from protecting fisheries to guarding Iraqi oil platforms.[1] Additionally, the number of icebreakers the USCG maintains, which are vital for Arctic operations, has dwindled to just two. At present, the USCG is expected to fulfill its growing number and range of missions with a shockingly small budget; in 2012 we spent more on the Afghan National Security Forces than we did on our own Coast Guard.[2] As we examine areas in which the investment of our limited resources could have the most value, the Coast Guard is an obvious choice.

Moving to a risk-based model for security will not be without its challenges, and will require that Congress, DHS, and the American people engage in an ongoing dialogue about our priorities and the level of risk we are willing to accept. It is important to emphasize and to understand that no matter how well executed, any adoption of a risk-based model will inherently mean assuming some degree of risk; in implementing them, we must be willing to accept not only the risks, but the potential consequences, and that we cannot simply revert to trying to provide complete protection if and when there is an attack. Furthermore, it means accepting that while some mission areas will see increased resources, others may receive little or nothing. If we as a nation are willing to accept these facts, a risk-based model for homeland security holds the potential to help reorient us towards tomorrow's threats even as budgets are tightened.

[1] "United States Coast Guard 2012 Posture Statement", February, 2012, http://www.uscg.mil/posturestatement/docs/uscg_2012_posture_statement.pdf.

[2] "Justification for FY 2013 Overseas Contingency Operations Afghanistan Security Forces Fund (ASFF)", Office of the Secretary of Defense, February 2012, http://asafm.army.mil/Documents/OfficeDocuments/Budget/BudgetMaterials/FY13/OCO//asff.pdf.