

**TESTIMONY OF
PAUL A. SCHNEIDER
FORMER DEPARTMENT OF HOMELAND SECURITY
DEPUTY SECRETARY
BEFORE THE U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON MANAGEMENT, INVESTIGATIONS, AND OVERSIGHT
*February 3, 2012***

Thank you Mr. Chairman, Congressman Keating and members of the Subcommittee. It's a pleasure to appear before you today.

It has been approximately three years since I have left office as the Deputy Secretary of the U.S. Department of Homeland Security (DHS). Since that time, I been consulting for the U.S. government (except for DHS); am a Principal in The Chertoff Group which is a company that provides consulting, security and merger and acquisition (M&A) advisory services for clients in the security, defense and government services industries around the world; and, I also currently serve on several boards and advisory groups, including as Chairman of the Board of Directors of the Applied Science Foundation for Homeland Security. My role with the Foundation and other small companies is done on a pro bono basis.

Since leaving my position at DHS, I have had the opportunity to observe the changing and challenging budget environment and assess its impact on DHS operations and those of the homeland security enterprise. Based on my observations, former position and years of experience, I am here today to provide my views about DHS' current strategy and what direction they should consider taking in the future.

Threats

I believe the most serious dangers facing our nation today involve biological, cyber and nuclear threats. As you know it is very difficult to convince the general public of the importance of these threats. I know DHS takes these threats very seriously and has instituted several programs to address these dangers, but I am concerned that in some cases, fiscal reality will limit the financial resources that are available to counter these threats.

Biological is at the top of the list in terms of risk because of the relative ease of accessibility to the materials and know how; the potential consequences; and relatively low level of national preparedness. Cyber because of its pervasiveness and difficulty in pinpointing attribution has rapidly emerged as a threat to all critical infrastructure areas.

For both nuclear and biological threats (and the wider range of catastrophic threats) what we need is a very strong national preparedness posture comprised of a highly integrated group of stakeholders supported by realistic plans and frequent exercises that provide confidence in our preparedness and ability to respond.

I think it is appropriate for DHS to accelerate “fixing” critical infrastructure issues. The tiered approach to identifying the critical facilities can serve as a map to developing and implementing a mitigation plan.

Emphasize Cyber Security in Private Sector with Practical Help

I am pleased that cyber security continues to receive the political and financial support it does from the Congress. However, the extent of this problem is huge. While the Department of Homeland Security continues to focus its funding on defending the federal government networks (the .gov domain), there is an additional need for investment and support to identify, prevent and mitigate threats to our mostly privately-owned critical infrastructure and key resource systems, as well as State and local governments and infrastructure providers.

I find it amazing that within a 50-mile radius of this building there is a nexus of expertise in this area that is without peer: the Ft Meade complex, major cyber security centers set up by the major corporations, cyber incubators in the state of Maryland, the University of Maryland Cyber Research and Development Center, etc.

To support the constantly evolving and persistent cyber threat, I would recommend establishing a public-private partnership in order to perform the following:

1. Create and institute IT portals that easily convey government requirements to large and small businesses that enable them to easily explain what they have to offer. The rigid small business methods and forums cannot match the near real time speed that is required to keep up in this world; and yet there is a tremendous amount of innovation and capability that can be tapped.
2. Set up programs with/for small and mid-size businesses, as well as state and local governments, to educate them about what they can do to protect their networks.
3. Help in the creation of private-sector-run security operations centers to provide cyber security services for small and mid-sized business, and for certain public sector entities, that will allow them to protect their networks.
4. Establish a more robust modeling and simulation effort that allow relevant parties to strategize the threat space, model the implications and determine risk mitigation approaches.

5. Consistent with the Critical Infrastructure Protection (CIP) implementation program, focus on resilience to look at means to quickly recover from a cyber-incident.
6. Examine the need for more agile contracting strategies that work inside the stimulus-response cycle needed for cyber issues.

Restructure the focus of Science and Technology

The budget cuts imposed on the Department's Science and Technology Directorate (S&T) have led me to conclude that that S&T must change its entire nature in order to reflect its new budget reality. After accounting for the existing manpower levels, major laboratories that are funded by these appropriations and the University Centers of Excellence, very little discretionary funds are remaining.

Therefore I believe the focus of DHS S&T should be as follows:

1. Emphasize a more focused and deliberate test and evaluation program to inform users of the right equipment and systems to deploy for the right mission. Work with the users to understand the threat environment, their operational concepts for operations to make sure the test procedures and environments are relevant. Right now we have public and private institutions around the country buying stuff and it is not clear if any competent technical authority knows if it is any good.
2. Based on an aggressive T&E program to meet users' needs, develop standards for devices and systems that could be procured by the private and public sectors, not the devices themselves, because it is impractical to think that the government will get enough procurement dollars to field the equipment themselves. This means using T&E and threat based standards as the basis to inform users of the right equipment for the right mission application. This moves away from the standards based (industry driven) approach which is not the correct approach for this situation.
3. Recognize that state and local governments and the public sector, not just the DHS operational components, are the recipients of S&T investment dollars and include their priorities in the resource allocation process.
4. Aggressively harvest the enormous amount of technology that the Department of Defense has been/is developing and with the correct set of innovative people look at how to adapt it to DHS uses. In this regard I recommend that consideration be given to forming a team with representatives from Department of Defense (DoD) laboratories and Federally Funded Research and Develop Centers (FFRDCs) and the DHS Systems Engineering FFRDC with DHS operational personnel to evaluate specific scenarios that DoD technology could be readily adapted to enhance mission effectiveness.
5. While DNDO is a separate organization, these recommendations also apply to the work and RDT&E they do. Within DNDO, the process was and I believe still is to work with State and local law enforcement to determine how they would use detection systems and then to test them using those

Concepts of Operations (CONOPs) against threat material and in operationally relevant environments.

6. Readjust funding allocations from manpower, laboratories and University centers to S&T that directly and more immediately supports the users.

Consolidate Information Technology (IT) under the Chief Information Officer (CIO)

The Under Secretary for Management and the Chief Information Officer (CIO) has made DHS the leader in data center consolidation and the migration to the cloud. Once you have worked with the IT underpinnings of DHS, you realize it is one massive IT system that many different operational users use, with the bulk of the data bases serving multiple users under multiple systems and many are interdependent.

So, whether it is E-Verify, US VISIT, TECS, and TTAC with all of its component systems, there is interlocking because many of the same databases are accessed in order for the government to make adjudication. Yet, observing on the outside, as I have, systems modifications, modernizations and upgrades are executed by individual components that happen to be responsible for their programs and systems.

While coordination and oversight can be effective, I think the current environment dictates a different business model of centralized command and control.

The IT area has and will continue to sustain large financial cuts due in some part to the belief that IT is an enabler and therefore iris investment ought to achieve savings. I agree that IT is enabler, but the business management model that governs is as much of an enabler as the technology itself.

Therefore I recommend the following:

1. Consolidate all of the IT funding under the DHS CIO
2. Empower the CIO and the Under Secretary for Management to determine how best to incrementally phase in a new IT infrastructure building on what they have done with the data center integration and cloud migration, by using the appropriated funds for the individual systems, modulating individual program priorities for the overall good of the Department and the betterment of the overall IT infrastructure.

For this to succeed DHS will have to continue to make substantive and sustained progress in developing a functional command and control, communications, and requirements development.

Change the Business Model for Scanning Equipment

Scanning is an essential part of the security architecture for aviation security and in my view the technology is dynamic, driven in large part to significant advances in the medical field. And as nano technology emerges, to an even greater extent technology enables enhancements in fidelity for screening in terms of quality and speed of the throughput which will be highly desired and valued by DHS. Now, these systems are procured and upgraded by the Government.

Given funding realities and the speed of which the commercial sector can quickly develop and respond, this dictates shifting to a business model whereby the Government specifies the requirements and leases the equipment with stated service level agreements regarding performance like commercial IT contracts, including upgrade and refresh requirements. DHS would essentially pay for this as a fee for service lease. I am acutely aware that OMB has definite views of this type of arrangement that may not be as supportive because of scoring considerations.

In my view however, the changing nature of the technology, evolving threat scenarios and the budget realities, demand that the current business model be changed to one of a more commercial nature.

Consolidate Operations

While serving as the Deputy Secretary, I was frequently asked by those members of Congress who were on Homeland Security Committees and Department of Defense Committees whether or not DHS needed “Goldwater Nichols (GN)” legislation.

The Goldwater-Nichols Department of Defense Reorganization Act of 1986 Pub.L. 99-433, made the most sweeping changes to the United States Department of Defense since the department was established in the National Security Act of 1947 by reworking the command structure of the United States military. It was subsequently followed by the Defense Management Review of 1989 which fully implemented the Packard Commission’s recommendations and the Goldwater- Nichols Act to substantially improve the performance of the defense acquisition system; and to manage more effectively the Department of Defense and our defense resources.

I replied that the time was definitely not correct to do that because DHS was still in its infancy, not all the requirements of GN were appropriate to be considered for DHS, and that the Act’s operational and acquisition fundamental changes should ultimately be considered and adapted for use by DHS, but timing was key.

At this point in time I think it is appropriate to start thinking seriously about how to accomplish a modified version of GN for DHS, since I think only a few major provisions as discussed below are applicable at this time. The factor that drives me to this conclusion is that I believe currently, no unified command structure

exists for DHS components in the field. Each component has individual field structures with unique geographic boundaries and independent chains of command. These lines of authority do not converge until they reach the Secretary/Deputy Secretary.

Practically speaking, in the field, there are independent operating components. I think this hampers operational effectiveness. While I am aware there are several informal teaming arrangements in various ports and cities, it is not the same as an integrated command and control structure.

Therefore, I recommend:

1. Develop a unified field structure with appropriate command and control or coordination authority. This would provide an opportunity for greater stability in state/local relationships and ability to better coordinate DHS operations in the field.
2. Consideration should include various alternatives, such as states, regions, ports, interfaces with DOD and unique state and local considerations and authorities.
3. Maximizing the collective effectiveness and use of joint assets, both operationally and in the planning and execution of logistics support functions.

I am aware that certain operating component statutory authorities need to be addressed to make this work, but integration of assets at the pointy end of the spear is essential in order to maximize effectiveness in addressing the evolving threat scenarios.

The second major element of a GN move would be to examine centralizing major acquisition programs in a "DOD Systems Command" type of structure separate from the Operational Components. This would enable operating components to focus on operations and build upon the critical acquisition mass currently available, while ensuring major cross-component acquisition initiatives are executed in an integrated manner (as many current operations are actually executed). As part of this effort a total review of the acquisition process, its successes, lessons learned and next steps would be a useful step to help shape the structure of this organization. All of this will eliminate redundancy, while complying with an integrated enterprise-wide architecture and offers the potential for tremendous financial economies.

The basis for this recommendation is simple. The majority of DHS operational people wears badges and carry guns. Is it smart to hold a major component head, for example the head of CBP, with approximately 65,000 people, responsible for his 24hrX7 day law enforcement responsibilities around the world and at the same time, ask him to be responsible for developing and fielding complex systems that must integrate with other complex systems? Is this the correct model for the future? I think the answer to both questions is no and that is

why I think this different structure is much more conducive to enhancing effective operations.

In DoD they learned this a long time ago. That is why the Air Force's Air Combat Command deploys planes and does not develop the F-35, and why the Navy's COMSUBLANT operates submarines but does not develop the Virginia Class Submarines.

I am aware that many organizations within DHS will disagree with these recommendations and argue vociferously against any changes to the status quo to protect their legacy functions and independence. So, it would be the challenge to leadership to steer changes of this magnitude. The DOD was created in 1947; GN was authorized in 1986, but really didn't happen until the DMR in 1989 when the majority of the GN changes took effect. It would be unreasonable to assume that this type of change would be any different in timescale in DHS.

Overlaps in the Assignment/Interpretation of Homeland Security Roles

I think the issue of ambiguities and overlaps in the assignment/interpretation of homeland security roles, responsibilities, and authorities among federal stakeholders are a continuing obstacle to unity of effort within the federal government and our allied countries. These overlaps and ambiguities also have the effect of fundamentally undermining the credibility and ability of federal agencies to effectively engage with state and local governments and the private sector.

As you're well aware, this is a very difficult and politically charged issue that is difficult to rationalize. While, barring some major catalyst, a holistic attempt to comprehensively frame and address all roles/responsibilities/authorities issues is near impossible.

What is needed is a systems approach to identifying the overlaps and ambiguities having the most significant implications for our strategic outcomes (e.g., DHS/DOJ re terrorism prevention and borders; DHS/HHS re Bio/mass casualty event preparedness & response; DHS/DOD re catastrophic response support to civil authorities). The challenges with these issues is that agencies and components would rather live with and work around current ambiguities than risk losing equities they consider vital. Yet these same ambiguities significantly undermine unity of effort, and increase risks of failure in preventing or responding to potentially catastrophic events. I doubt many in the administration or congress have energy on this, but it is a necessary factor that should be addressed.

Conclusion

I think DHS has come a long way since its inception and will continue to improve over the next few years. I believe as we look to the future we need to make

refinements along the lines I have recommended before you today to meet the many challenges that lie ahead.

I urge you to adapt these recommendations and direct their implementation.

Thank you for your leadership and your continued support of the Department of Homeland Security and its programs, and your support and commitment to the thousands of men and women who dedicate themselves to the defense of our great country.

Thank you for this opportunity to be here today and I am happy to answer any questions that you may have.