Statement for the United States House of Representatives Homeland Security Committee

Provided by: Jeffrey R. Gaynor

Private Citizen
and
Former Director, Emergency Response Senior Advisory Committee
and
Critical Infrastructure Task Force,
Homeland Security Advisory Council

Cannon House Office Building, Washington, D.C.
Wednesday, July 25, 2007

Machiavelli said: "There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success than to take the lead in the introduction of a new order of things, because the innovator has for enemies all those who have done well under the old condition, and lukewarm defenders in those who may do well under the new."

Charles Darwin noted: *"It is not the strongest of the species that survive or the most intelligent, but the ones that are most responsive to change."*

And President Woodrow Wilson – in true American style said: *"If you want to make enemies, try to change something."*

Mr. Chairman and members of the House Committee on Homeland Security, with those words as a preamble, it is a my distinct honor and privilege to provide this statement and to appear before you this day to discuss -- and far-more importantly -- to find immediate and objectively measurable solutions to fully optimize an organization that in my opinion is nothing short of a national treasure. I speak of the Homeland Security Advisory Council and its Senior Advisory Committees of the U.S. Department of Homeland Security.

In the wake of the nationally transforming events of September 11, 2001, President Bush created the Office of Homeland Security. On October 8, 2001, Governor Tom Ridge became America's first Homeland Security Advisor. Given both the President's and Governor Ridge's experience as state leaders and recognizing that Washington cannot and will never have the real-time understanding of the realities of life in our hometowns – a knowledge that is routinely possessed and used daily by their citizens, business owners, elected and appointed officials, and Emergency Responders – President Bush ordered the creation of the Homeland Security Advisory Council or HSAC and directed it be populated by people who could provide to Washington that understanding. Under the leadership of Governor, Homeland Security Advisor, and then Secretary Tom Ridge, the HSAC – as the President intended – became the Nation's principal Homeland Security Advisory Body.

True to its Charter, the members of the HSAC and its Emergency Response, State and Local Officials, Private Sector and Academe and Policy Research Senior Advisory Committees, have leveraged their unique experience and have provided to the Secretary organizationally independent, visionary, non-partisan, and highly-executable recommendations spanning the spectrum of Homeland Security policy, planning, programs and capability creation. All of the HSAC products including the Task Force Reports and recommendations I will address are publicly available at www.dhs.gov/hsac.

In 43 years of Defense and Civil Service, I have had the honor to serve with some of the most patriotic, caring, selflessly committed, innovative, courageous, intelligent, and far beyond intelligent – smartest people on the planet. I count every member of the Homeland Security Advisory Council and its Senior Advisory Committees squarely in that group.
My association with them was inspirational and both a personal and professional learning and growing experience. Prior to my retirement from government service, I served as the HSAC's Director of both its Emergency Response Senior Advisory Committee and its Critical Infrastructure Task Force and actively participated in the efforts of the Private Sector

Information Sharing and Culture Task Forces. I am convinced that their recommendations deserve full and objective consideration and implementation. Unfortunately, over the past couple of years they have effectively received little of either.

In an effort to further validate the value of the HSAC's recommendations and to correct a situation I believe endangers national security, I will cite three examples of HSAC recommendations, the responses to them, and provide a recommendation that relies on objective metrics to correct the situation.

Example One: Private Sector Information Sharing Task Force Report

History is replete with the failures of vision and intelligence and resulting misdirected human action and grave consequence. To the extent this Nation is capable, it must leverage all of its resources to prevent or at least minimize the consequences of any failure of intelligence or understanding. Among other issues that the Private Sector Information Sharing Task Force report focused upon was requirements-based information sharing. Its highest priority recommendation was its first: *"DHS and the Private Sector should work in collaboration to develop a formal and objectively manageable, homeland security intelligence/information process."* The Task Force quite simply, was recommending DHS create the capability for its private sector stakeholders to ask a question and receive an answer. The recommendation was in part designed to assure that the value and success of Homeland Security information reporting is not measured simply by the number of reports generated, but rather, is the product of the assessments of the department's Homeland Security Partners/customers and responsive to the homeland security information requirements of high-consequence enterprises of the private sector and the high consequence critical infrastructure service providers that empower them and the Nation.

From the corporate view, requirements based information sharing is designed to address business resilience issues including "the delta" between infrastructure capabilities and the corporations' need for – beyond protected – operationally resilient critical infrastructure and global supply chain operation. To that end, and after my departure from the Department, I helped coordinate two meetings that were designed to demonstrate to the Department corporate willingness to support requirements-based information sharing.

In December 2006, Terry Tapley, the Chief Information Security Officer of a national icon -- McDonalds, hosted a meeting of Fortune 500 companies. In addition to McDonalds, attendees included representatives of: the Boeing Corporation, Ford Motor Corporation, General Motors Corporation, Cardinal Health, The Bank of Montreal, J.P. Morgan/Chase, Target, Limited Brands, National City Bank, Wal-Mart, Metavante, McCormick Place, American Association of Railroads, Canadian National Rail, Pace Bus, AON Insurance, Progressive Insurance, TIBCO, Affiliated Computer Services, Waste Management, Illitch Holdings, Nationwide Insurance, and Computer Network Services. Also attending were representatives of the States of Illinois and Ohio.

In the presence of Homeland Security Officials from the Information and Analysis and Infrastructure Protection organizations and the Private Sector Office, these corporations,

consistent with information sharing recommendations made by the HSAC (in its Private Sector Information Sharing and Critical Infrastructure Task Force Reports), agreed to participate in Fusion Center development and requirements-based information sharing efforts. Another meeting in Columbus, Ohio in January of this year yielded the same results – corporate willingness to support Homeland Security requirements-based information sharing efforts through the emerging fusion centers. At both meetings, the corporations urged expeditious action to that end on the part of DHS.

These companies – like emergency responders and state and local officials – require the ability to ask questions and receive timely, accurate and actionable answers to drive investment and actions to maximize their all-hazards preparedness. A number of these companies are subject to Sarbanes-Oxley provisions and have a stake in Terrorism Risk Insurance Act issues. Of significance, some of these companies are also involved with current preparation of the City of Chicago's Olympic Bid for the 2016 Games with host city to be selected 2009. If Chicago is selected, the 2016 Olympics will become the single most challenging National Security Special Event since 9/11.

For all of the above reasons, I believe American corporations are prepared to invest in "Due Care" efforts designed to ensure their competitiveness and economic viability in a 21st Century, globally interconnected and "all-hazards" marketplace. Because of the reality of interdependence, corporate investment in their infrastructure fosters improvement in the resilience of critical infrastructure in the cities and regions in which they operate. However, to justify such expenditures, these entities need timely, actionable information that thus far (and quite inexplicably) has not been made available to them.

The reasons for the subsequent withdrawal of DHS support from a continuation of these meetings appear to be tied to "organizational equities" and overheard statements indicating the need to "control" the private sector's apparent thirst for requirements- based, timely, accurate, actionable and frequently updated Homeland Security Information. The corporate representatives attending the meetings in Chicago and Columbus, Ohio, like the members of the HSAC, understand objective measures of performance.

As businessmen and stakeholders in America's security, they recognize the quality and effectiveness of any product – in this case Homeland Security Information reporting – is most appropriately judged by its customers. At this point in time, even though the Government may be unable to answer industry's questions/requirements, just having them makes DHS, and the Intelligence Community, better able to focus existing assets while simultaneously building programs that will gain congressional approval for the resources necessary to develop capabilities to answer them.
An article in the June 17 edition of the Rutland (VT) Herald, and the Department's response spotlighted this continuing information-sharing problem. In that article, the Commissioner of the Vermont Department of Safety and the state's top homeland security official questioned the quality of DHS information reporting. In response, he received a rebuke from the Secretary's spokesman who stated that the Commissioner's concerns were, among other things, "disingenuous." I find this kind of response to the legitimate concerns of a state's Homeland Security principal unwarranted and disturbing. It highlights a perhaps subconscious mind-set or

"bunker mentality" of a headquarters charged with a huge and unprecedented mission, but as a result of missteps, has become all too defensive and reactive.

Again, we are in this fight together. Requirements-based information sharing with at least America's potentially high-consequence producing corporations is an imperative that will synergize Homeland Security capabilities, build greater trust in government, reveal the "dots" that need connecting, build resilient critical infrastructure services to empower businesses and communities, and thereby enhance the Nation's preparedness and the effectiveness of its local, state, and Federal response capabilities. From a Congressional oversight perspective, requirements-based information sharing will provide objectively measurable standards to assess the effectiveness of DHS's Information and Analysis and Infrastructure Protection organization's information sharing efforts and, accordingly, manage resources in providing what the HSAC has consistently and repeatedly recommended: provision of requirements-based, timely, actionable and frequently updated Homeland Security information to the private sector.

Example Two: The Critical Infrastructure Task Force (CITF) Report

Consistent with the Secretary's direction to the CITF to: "Review current and provide recommendations on advancing national critical infrastructure policy & planning to ensure the reliable delivery of critical infrastructure services while simultaneously reducing the consequences of the exploitation, destruction, or disruption of critical infrastructure products, services, and/or operations," the CITF called for the transformation of critical infrastructure protection (CIP) policies and standards from current objectively unmeasurable iterations of "top-down" (i.e., Federally dominated) Cold-War and failed CIP programs (note the consequence amplifying results of protected critical infrastructure failures during Katina) to an objectively measurable, achievable and sustainable resilience standard (i.e., desired time to reconstitution). The CITF recommended: Promulgate Critical Infrastructure Resilience (CIR) as the top-level strategic objective—**the desired outcome**—to drive national policy and planning.

The CITF's principal and subsequent recommendations and the logic behind them reflect the results of highly-disciplined study by Americans of unquestioned vision, intellect, loyalty and accomplishment. They represent the critical infrastructure, business, community, regional and National perspectives and very publicly called for transformation in national Critical Infrastructure policy, plans, programs and objectives to "The Resilience Standard." Thus, in the wake of the next guaranteed failure of protection and resulting consequences that could have been avoided, there will be no cover for supporting the status quo.

While I have spoken throughout the country on "The Resilience Imperative" and have been published on the subject in the United Kingdom's *Defence Management Journal* and *Freight Transport Review*, and somewhat colorfully featured in the Cover Story "Snapping Back" in the June 15 edition of *Government Executive Magazine*, I urge the Committee if inclined not to take my word for anything on this issue to read the People's Liberation Army's paper: "Unrestricted Warfare," Steve Flynn's Book, "The Edge of Disaster: Rebuilding a Resilient Nation" and the reports of the HSAC's Critical Infrastructure Task Force, The Infrastructure Security Partnerships Regional Disaster Resilience Guide (www.tisp.org) and the Council on

Competitiveness's newly released Transformation report at:
(http://www.compete.org/pdf/Transform.TheResilientEconomy.pdf)

In its review of the resilience imperative, the Council on Competitiveness noted that the current policy tends to speak to Critical Infrastructure Protection in isolation – almost as though it were a national good like national security. But the fact of the matter – which is by now almost axiomatic – is that most of the critical infrastructure is owned by the private sector. Current policy and plans seem to ignore the fact that 100% of the private sector and the country depends on the operational resilience of those interdependent cyber and physical infrastructures for their own competitiveness and indeed survival. So an important question is: Why does the market not demand reliability, redundancy and resilience from their supporting critical infrastructure providers? The Council sees three explanations for the lack of market drivers:

First: Companies themselves have traditionally viewed operational risks – like critical infrastructure – as a back office function. Thus, critical infrastructure has far less visibility in the C Suite than financial risks. But, the Council noted, there is an urgent need for companies to become more risk intelligent – to understand that these kinds of business-empowering critical infrastructure realities that are "bet the company" risks to which CEOs and boards must focus their attention.

Second: The Federal Government's critical infrastructure policies and approach work at odds with market drivers. The Council points out that the government tends to focus only on catastrophic failures. But, business investment is driven by a spectrum of risks not just a narrow slice of high-end risks. Ironically, the issues that companies must address to meet the day to day turbulence of operating in a global economy go a long way toward creating the capabilities to cope with catastrophe as well.

Third: The Government's policies have almost uniformly focused on fences and firewalls, not strengthening the market drivers for resilience.
The report notes the need for objective metrics that companies can use to model the impact of critical infrastructure failures on their businesses.

As is evident from the results of the corporate meetings in Chicago and Columbus Ohio, I am confident that once costs of infrastructure failure become more transparent, companies will act. To that end and consistent with the efforts of The Infrastructure Security Partnership and the content of its Regional Disaster Resilience Guide, the Council recommended creation of regional centers for information exchange. The Council noted that linkages to critical infrastructures are almost always local or regional, not national. It therefore stands to reason that discussions regarding critical interdependencies, the potential for crisis and overall preparations, mitigation capacities, and the overall resilience of critical infrastructure services should be regional as well.

Albert Einstein defined insanity as "doing the same thing over and over again and expecting a different result." In other words – iteration over innovation is not an acceptable answer to the Nation's homeland security requirements. In lay terms, it simply doesn't work to leap a twenty foot chasm in 20 one-foot jumps.

The CITF Report recommendations provided the chasm spanning "leap" and advancement in national Critical Infrastructure Planning and policy Secretary Chertoff requested. The resilience standard recommended by the CITF leverages the preparedness "basics" that are CIP policy and efforts. The report's recommendations, as some have defensively suggested, does not abandon protection efforts. Resilience recognizes the lessons of infrastructure protection history and addresses foreign pronouncements and threats including the above mentioned Peoples Liberation Army document "Unrestricted Warfare."

Resilience also provides an objective, universally understood and accepted investment and success metric – *Time***.** Sufficient protection is not objectively quantifiable. It is impossible to answer the question How Much protection is enough? Thus, a proper level of protection is impossible to determine much less achieve and maintain. Since resilience is objectively measurable it advances historic, ongoing, and projected investments in business and government continuity and resiliency and Sarbanes-Oxley Act "Due Care" provisions. The resilience standard also supports the development of Terrorism Risk Insurance Act standards and addresses the physical realities of infrastructure placement and operation which operate in communities not sectors. Resilience is also a proactive rather than reactive and defensive mindset. Unlike the protection mindset that psychologically places an enterprise on the inside looking out, resilience addresses the "predator's view" across an entire enterprise, community, or region and mitigates consequences regardless of their cause. (e.g., terrorist, insider, self-inflicted, accident, nature, cyber, physical).

The resilience standard is also nationally (and potentially globally) empowering.

Because it is built from where the consequences will be felt, resilience is a shared and integrating responsibility and an objectively measurable standard and process for a scalable, technological, economic, social, and a long-overdue investment in America's foundation (i.e., its Critical Infrastructure).
Since resilience is an objectively measurable condition it can be learned. It and the technologies that will support and sustain its achievement will provide a standard, processes and product that can *advance* the human condition throughout the planet.

During the public announcement of its recommendations, CITF member and Former Governor of Massachusetts Mitt Romney summed-up the need to make the policy and national preparedness transformation from protection to resilience: "You know, protection is where we tend to focus in government, but it is very, very clear that protection is not enough . . ."

Unfortunately, no actions have been taken or credible explanations provided for failure to implement the CITF's principal recommendation.

The third example – Recommendations of the HSAC's Culture Task Force

Secretary Ridge was emphatic in constantly focusing his DHS (formerly White House) staff on the reality: "When our hometowns are secure the homeland will be secure."

In my experience, his focus was exactly where it should be -- on where all human, physical, economic, and societal consequences will be felt and thus where all preparations and capabilities for meeting the challenges of the "all-hazards environment" are best known and understood and can be decisively acted upon.

In the wake of DHS's understandable but less than admirable showing in the 2004 Federal Workplace Survey, and with the 2006 results on the horizon, Secretary Chertoff directed the HSAC to form a Culture Task Force to provide recommendations on shaping and improving the department's culture. In the wake of the even less flattering results of the 2006 Federal Workplace Survey, the Culture Task Force provided its recommendations.

Chief among the recommendations were:

- Replace the Federal buzzword "Human Capital," (the last time we considered humans as "capital" we were fighting a civil war);
- provide the opportunity for innovation; and
- establish a Deputy Secretary for Operations within DHS Headquarters

The Culture Task Force's recommendations were designed to:

- **First**: Recast and foster empowerment of the department's workforce. They are all valuable employees, they are not "capital" to be bartered.

- **Second**: Create an integrated Homeland Security Innovation Center to actively track and ensure disciplined review, processing, and response to ideas submitted to the department and its components focused on providing continuous improvement in Homeland Security policies, programs, and capabilities.

- **Third**: Provide the operational expertise and experience necessary to rather than build a "Team DHS" culture, build a unifying Homeland Security Mission Culture. In other words, build a culture with an intense focus on Homeland Security operations and capabilities of the likes we saw and admired in the actions of General Russell Honore and now Coast Guard Commandant Admiral Thad Allen in the wake of Hurricane Katrina.

To the best of my knowledge requirements based information sharing is still being discussed, no action has been taken on the recommendations of the Critical Infrastructure Task Force – although the word resilience was added at the 11th hour to the National Infrastructure Protection Plan. The Culture Task Force recommendation to create a Deputy Secretary for Operations has been rejected – largely for organizational (not operational) reasons.

From my experience, the non-public reception of the Task Force Reports' recommendations reflect fatigue and thus an organizational preference for the status-quo, iteration over innovation and a concentration on "organizational equities" and processes. This is reflective of a headquarters "bunker mentality" that is inconsistent with the imperative of continuous improvement in the Nation's homeland security capacities and preparedness – the Department's sole reason for existence. As Mr. Frank Cilluffo, the first Executive Director of the HSAC used

to put it: "The purpose of homeland security is to make the Nation not only safer, but stronger and better." I totally agree and thus given the need for continuous improvement in any national security entities operations find the Department's responses to these and other HSAC recommendations a condition that must be corrected.

Recommendation:

Like the objectively measurable standards imbedded in the HSAC's recommendations on requirements-based information sharing with the private sector, critical infrastructure resilience, creating a mission-based culture, and empowering innovation within DHS, it is imperative that objectively measurable standards be applied to the operation of the HSAC and all Homeland Security Advisory Committees.

Given the "all-hazards environment" in which we live and the resulting the need to:

- Provide requirements-based, timely, accurate and actionable information to all homeland security stakeholders,
- Arrest the catastrophic and even consequence amplifying failures of critical infrastructure protection that have witnessed and will occur again,
- Establish continuous innovation and a mission-first culture throughout the department,

I urge the Congress to create a quarterly HSAC and perhaps DHS Committee reporting requirement. The report would detail the public recommendations made by the HSAC and perhaps all Homeland Security Advisory Committees operating under the Federal Advisory Committee Act, the actions taken on them, recommendations not acted upon, and why and by whose authority.

In order to demonstrate work actually performed, I would include in the report the program and budget resources being applied to making recommendations reality. I would also urge the Committee to engage the resources of the Government Accountability Office and the DHS Inspector General in this reporting effort to ensure process and organizational reactions to questions posed to it (i.e., discussions, intent to act) is not confused with objectively measurable progress.

In closing, and at the risk of demonstrating a solid grip on the obvious, let me emphasize, that America is in a fight with morally if not intellectually inferior causes and people who are unfortunately creative, adaptive, dedicated, patient, imbedded and self-sacrificing. These adversaries have proven themselves effective in the godless acts of terrorism they inflict on both Muslim and non-Muslim societies. Thus, we are all in this fight for our existence. The Government does not have all the answers (not even all the questions at this point), but it does have the Constitutional responsibility to ". . . provide for the common defense." The President and the Congress realize that Government and the Department of Homeland Security cannot do it alone. The HSAC – composed of people from both sides of the aisle – has repeatedly provided sound and executable recommendations throughout its history. Those that I highlighted above have, consistent with its Federal Advisory Committee Act responsibilities, been clearly and convincingly articulated in public venues. Thus, there will be no logical, ethical, moral, political or legal cover in the wake of the next catastrophe resulting from an "all-hazards" failure of intelligence, infrastructure protection, and/or organizational culture.

Mr. Chairman, I again thank you and the entire Committee for the opportunity to have my thoughts captured for the record and to appear before the committee on this most fundamental of homeland and national security issues. After 43 years of Federal service, it is difficult to stop working in the public interest and I do not intend to do so. In whatever capacity I may, I am at your and the Department's service.

In closing, I offer a quote from Abraham Lincoln: "The dogmas of the quiet past are inadequate to the stormy present. The occasion is piled high with difficulty, and we must rise with the occasion. As our case is new, so we must think anew and act anew."