NATIONAL HOMELAND SECURITY CONSORTIUM
SUMMARY

January 17-18, 2013 ♦ San Diego, California

January 17, 2013

Welcome & Introductions

Tri-Chairs Tom Sands (NEMA), John Madden (GHSAC), and BG Scott Legwold (Representing MG Don Dunbar – AGAUS) welcomed participants and conducted self-introductions

The Adminsitration's Second-Term Priorities for Homeland Security

Richard Reed, Deputy Assistant to the President for Homeland Security
The White House

Reed thanked the NHSC for their past input and said it has had an effect on administration policy. Moving forward, the White House will continue the "All of Community" and "All of Nation" approach to resilience. Papers such as the NHSC white paper give the administration the opportunity to see how various associations are addressing national issues.

Storms such as Sandy underscore the need for us to address resilience and explore lessons learned. In the Executive Order, creating the Hurricane Sandy Rebuilding Task Force, the President directed that the aging infrastructure of the affected area be not only repaired, but updated against future loss. The task force is designed to specifically help the impacted area and ensure proper use of supplemental funds. One of the most difficult issues to address is those assets that should not necessarily be rebuilt. Such a question has been challenging for the locals to consider.

The National Preparedness Report provided the White House valuable information in the current status of preparedness across the country. In addition to the larger preparedness issues, cybersecurity continues to be a priority for the administration. The major challenge of cybersecurity is the broad involvement of various agencies within the government as well as different sectors of state and local governments and the private sector. The National Cybersecurity Integration Center (NCIC) is meant to bridge the gaps between the government and private sector. All of the efforts by the White House through these strategies and integration efforts are meant to bring together various players to demonstrate a unified front against resilience challenges, preparedness efforts, and protecting critical infrastructure. The latter will be one of the highest priorities for 2013 as the administration presents an updated HSPD-7. The new document will change the federal focus from one of "protection" to "resilience."

Reed also gave an outline of some of the larger issues being addressed by the White House including immigration reform, gun control policies, an Arctic strategy, baseline cybersecurity requirements for critical infrastructure, reducing legislative impediments to cybersecurity, and an updated executive order on emergency communications.

Reed accepted a few questions and comments. A summary of which includes:

- Containing the flu this year is a significant challenge for the public health community. The Pandemic All-Hazards Preparedness Act provides the authorization for funding to state and local health departments.
- A question was posed regarding the requirements placed on state and locals through the cybersecurity Executive Order. Reed assured that requirements would be limited and the EO is meant more as a collaborative document to help bring stakeholders together.
- A member recommended focusing more on pre-disaster mitigation as a means by which to reduce overall costs and improve resilience.

Update on Efforts at the Federal Emergency Management Agency

The Honorable Tim Manning, Deputy Administrator for Protection and National Preparedness
Federal Emergency Management Association

Manning started by providing an update on some personnel issues including Administrator Craig Fugate and Secretary Janet Napolitano staying in their current roles. The most significant issue for 2012 was the roll-out of the new HSPD-8 including the overall plan and frameworks. He reassured members that the process is the same as how state and locals have been operating, but the frameworks help bring the federal government up to the same level. The hope is that the frameworks will be released soon.

DHS is currently beginning the second Quarterly Homeland Security Review (QHSR). The hope is to utilize the first review as a baseline to learn how the department is progressing. The review has already been opened internally, and the intention is to engage stakeholders the same as the last iteration.

Through 2013, FEMA will begin working with stakeholders, industry experts, and the public to work through issues of preparedness and ensure all advice given is accurate, timely, and up-to-date. The primary example he provided was the instruction for drivers during a tornado. Experts have found the adage of getting out of the vehicle and finding low-lying ground is not necessarily still the best advice. FEMA wants to begin developing methods on how to collect data on preparedness while also updating and communicating back out to the public.

The Integrated Public Alert and Warning System (IPAWS) and national alert system is coming online and starting to deliver messages to the public in regard to local alerts. Some Consortium members offered examples of how the program has begun to be seen in action while others were less impressed. Manning explained that the effectiveness of the messages depend on where an event is occurring and how robust the system is in that general area.

A national concerted effort is also underway to reexamine the state preparedness reports and how they integrate into larger federal priorities. A new reporting tool was constructed, but it failed quickly. FEMA will begin a renewed effort to collect the necessary data and improve the tool. Another programmatic improvement will be seen in the National Exercise Program. Exercise design and evaluation will see some changes in the coming year after a great deal of study at the federal level. The National Level Exercise will now be a biennial effort utilized as the culmination of two years of lead-up.

The federal budget situation has not gained any further clarity. Manning does believe a continuing resolution will be utilized until the end of a fiscal year. The administration's 2014 budget has been delayed and tied-up in the overall 2013 chaos. He does not see any major changes to the 2014 budget aside from continued austerity measures.

The FEMA Qualifications System (FQS) is a new effort to try and better define the qualifications necessary to do a specific job within FEMA. This will be tied primarily to response officials, and in line

with National Incident Management System (NIMS) requirements. The program is starting to realize some successes.

Manning accepted a few questions and comments. A summary of which includes:

- A member posed a question regarding FEMA's ability to utilize smartphone applications for alert systems. FEMA does have some "apps" available, but they are not currently part of the IPAWS system. They are also struggling with the ability to utilize apps to retrieve the vast amount of information necessary for families to receive FEMA assistance.
- No further clarity has been given to HLS grants. The issue is clouded between continuing cuts and an unwillingness to accept any meaningful changes to the system. A member brought-up the possibility of a new cybersecurity grant. Manning was not aware of such an effort and doubted the ability for a new program to be started.

Facilitated Discussion: Lessons Learned from Super Storm Sandy (Moderated by Tri-Chair Tom Sands)

Trina Sheets, Executive Director
National Emergency Management Association

Tim Manning, Deputy Administrator for Protection and National Preparedness, FEMA
Roundtable of NHSC Members

Sheets began the discussion by providing an overview of Emergency Management Assistance Compact (EMAC) efforts during the Sandy response. Deployed resources included A-Teams, search and rescue, generators, donations, Emergency Operations Center (EOC) staff, fuel trucks, emergency medical support, law enforcement, building inspectors, mass care, individual assistance, and public assistance among others. Some issues encountered through Sandy were similar to Hurricane Irene. An after-action planning workshop identifying issues to be addressed will be held in March.

Many states had A-Teams deployed before the storm even arrived. Once the storm passed, states quickly changed their status from "requesting state" to "assisting state." While this change is often normal, it happened much faster during Sandy than during previous events. Requests were very specific and stayed relatively close in terms of geographic dispersion. Integration with FEMA was also vastly improved than previous experiences. Training and education at all levels, including elected officials, is one area where improvements could be realized. Mission Ready Packaging has also improved cost savings, estimating processes, and the speed at which assistance can be offered.

Manning labeled Sandy as the first catastrophic disaster since Katrina and the Post-Katrina Emergency Management Reform Act (PKEMRA). Many of the successes in Sandy were a result of changes seen since Katrina. A full after-action is currently due to be completed around March/April of this year. The scale of the storm was unprecedented and in the wake, a massive amount of debris was moved. Some programs such as qualifications for credentialing, Operation Clean Sweep, and methods by which to provide a temporary living environment while larger repairs are taking place will be reevaluated as a result of the storm. Specifically the housing issue was a challenge in the aftermath of Sandy due to the dense housing environment in the Northeast. Conducting damage assessments was much easier and expedited during Sandy by utilizing GIS data. This helped FEMA develop a closer relationship with Google and move aid quickly.

Sands then facilitated a roundtable discussion was then facilitated to highlight lessons learned from other members of the Consortium:

- Michigan deployed personnel to the affected area and they felt the assignments went well overall. Obtaining credentials did take an inordinate amount of time and some officials lacked a strong knowledge of EMAC processes. Montana also deployed personnel without incident.

- Major City Chiefs utilized an information sharing workgroup to help bring together intelligence fusion efforts and identify those entities that might have a specialty to assist in the response. There are law enforcement assets available for deployment through EMAC, but no such request was utilized during Sandy.
- The Fusion Center Association is looking into how information moved between the affected areas and how much information can be improved.
- From the public health aspect, hospital evacuations were difficult due to the condensed population of the region. There also needs to be more outreach between the various medical facilities such as hospitals, nursing homes, and "quick care" organizations. Anecdotal data was collected from local public health organizations ranging from communications, command and control, situational awareness, and other aspects of disaster response.
- There was a broad difference between the expectations of the public and the capabilities of the federal government. These high expectations were seen among elected officials, the media, and especially the public.
- Some assets are still moved outside the EMAC process. This is due primarily to cultural differences between various sectors and a lack of education on the process.
- Sandy highlighted the need for an inventory of those fuel facilities that are equipped with the ability to run from a generator. While that information is not necessarily public, the public works agencies do already maintain such a database as a requirement of EPA regulations.
- Some states experienced issues with dual-status command and the National Guard, especially when a detachment of Marines had to be pulled back by NORTHCOM. Some within the military are still not clear on the rules of dual-status command structure.
- Throughout state governments, many elected officials are freshmen and lack much experience in the wake of a disaster.
- Public-private partnerships were strong and well-coordinated. The Private Sector Office within DHS, however, lacked significant outreach to the private sector. Fortunately, the FEMA counterpart did well in communicating with the various sectors outside government.
- EMAC sometimes slowed the ability to move EMS personnel quickly especially in the immediate evacuation requirements. Patient tracking while maintaining privacy requirements is also a challenge during transport.
- One of the major successes for a state like Maryland was the implementation of EMAC. Other non-traditional organizations such as building inspectors need to be brought to the emergency management and homeland security table in order for them to better understand response and recovery processes. Smaller issues such as toll collection and death notifications revealed themselves through the response process.
- Public communications systems often get stressed during a major event. APCO has established task forces that aid impacted areas to help handle the major influx of calls.
- Redeployment of staff continues to be a challenge especially in smaller jurisdictions.
- Technology services were affected too much during the disaster. But services such as EMAC support and the ability to utilize smartphone applications (apps) to streamline operations.
- Some local government officials were not thoroughly trained and educated on how EMAC operates. It is difficult to explain to local government leaders that shifting resources unilaterally is not always the most effective course to aid disaster response.

Panel Disuscussion: Dealing with the Consequences of Cyber Attacks (Moderated by Tri-Chair John Madden)

Richard Licht, Executive Director, Integrated Intelligence Center, Center for Internet Security

Doug Robinson, Executive Director, National Association of State Chief Information Officers

Ann Beauschesne, Vice President, National Security & Emergency Preparedness Department, U.S. Chamber of Commerce

Madden opened by outlining some of the current challenges of the cyber landscape.

The source of the threats has changed significantly in recent years. Once thought to be only for lone hackers, cybersecurity is now seen as a weapon by states and governments. The ability for state and local governments to defend against a cyber-attack is becoming increasingly difficult. This is due primarily to a large gap in understanding of the issue and the kind of commitment required to be successful. DHS's National Cybersecurity Review (April 2012) demonstrated a significant lack of progress and many warning signs of where state and local governments are in terms of cybersecurity. In total, most officials do not understand the depth and breadth of the cybersecurity threat.

DHS currently has limited sensors to be able to provide to state and local governments. This is a gap provided for by the Center for Internet Security. Since deployment approximately one year ago, the CIS program is able to monitor systems and alert officials to anomalies.

The US Chamber has a task force of over 200 associations and businesses focusing on legislation and cybersecurity policy. With increased online control of critical infrastructure, the consequences of a cyber-attack are becoming increasingly severe. Simple differences can make the difference, however, such as robust passwords.

Governments are inherently slow in responding to threats, and offensive capabilities are limited given the confines of government functions. Most government resources are roughly half of what experts would expect to be needed in order to effectively combat cyber-threats. Recruitment and retention of government employees are also challenges. The importance of adequate training of personnel controlling cyber systems cannot be understated.

Cyber-attacks are seen as the type that will challenge the system at-large in ways never before considered. No other type of offensive attack requires the type of coordination necessary in cybersecurity. Legislation will ultimately be required to facilitate coordination between the various levels of government as well as between the public and private sectors. In conjunction with legislative requirements, the federal government could be more forthcoming with knowledge of the threats and how best to defend against them. A groundswell of information sharing, specific to declassified data, would also help facilitate improvements.

Facilitated Discussion: NHSC Priorities for 2012 and Beyond

Glen Woodbury, Executive Director
Center for Homeland Defense and Security

The goal of this segment was to develop ideas and recommendations for how the Consortium can better inform and educate its members on these emerging issues identified in the white paper. This is meant to help guide future discussions, speakers, and meeting agendas and policy discussions. Members broke into workgroups to discuss each of the eight topics outlined in the white paper.

- Cyber Hazards.
    - The different parts of the threat must be understood.
    - Who are the appropriate partners?
    - How could the Stafford Act address cyber-attacks after they've occurred?
    - How to measure economic impacts.
    - How is recovery accomplished in a cyber-attack and who is responsible.
    - Will the federal response differ depending on who perpetrates the attack?

    - How is any retaliation managed?
    - A broad range of stakeholders must be engaged in the discussion.
- Climate Change
    - Difficult to separate the science and the politics.
    - What is impacted (ie, economics, change in demographics)?
    - Supply chain management, migration patterns, energy, and effects on the built environment are all subsets.
    - Are we in an era of increasing uncertainty in terms of natural disasters as a result of climate change?
    - When communities are potentially threatened, how are economic decisions made in terms of resilience and recovery? Changes in terrain and expected future changes could impact political decisions regarding rebuilding post-disaster.
- Demands on Global Resources
    - Agro-terrorism would prove a major threat to available resources.
    - Bio-terrorism also impacts policies related to global resources.
    - Aging population within the U.S. could affect demand on global resources.
    - Oil and natural gas use and finding alternatives.
    - Protection of critical infrastructure (such as the Sous Locks in Michigan) could impact the movement of global resources, and thereby their demand.
    - Water is likely one of the most important resources to consider given the importance to human survival.
- Demographic Changes
    - The overarching question is "What is it?" What is the demographic change being considered? Outside organizations such as the CDC, Census, and demographers could help assess the potential changes.
    - What are some good guesses?
        - Gentrification in cities can be expected to gentrify; Shrinking middle class; Life expectancy will continue to change in the U.S., potentially even trending downward
        - These changes have an impact on homeland security issues. For example, men aged 17-34 commit the majority of crimes. How does a shift in that specific group change law enforcement strategies?
    - Methods to combat such changes include preparedness education, improved contingency planning, better prioritization, more openness and information sharing, improved sharing of responsibilities, and educational priorities tailored to the future and needs of homeland security.
- Emerging Technologies
    - From the perspective of the NHSC, we need to specifically identify the most important emerging technologies that impact homeland security.
    - Each sector of homeland security will have varying priorities in terms of technology needs.
    - People do not need to be "experts" in technology to be able to keep abreast of emerging technologies.
- Terrorism
    - Terrorism must be defined in the context of existing capabilities and sphere of influence
    - Violent homegrown terrorists likely pose the most likely and pressing threat to state and local officials. Members must consider how they can influence the lone wolf phenomenon.
    - Consequence management and interdiction must be planned for appropriated and trained for and exercised rigorously.

    - The HLS community must not shy away from bringing in a broad range of experts in order to maintain a current and fresh outlook as well as consider alternatives.
- Weapons of Mass Destruction
    - The first question must be "is this issue even current anymore?" If so, how is it defined in terms of known and current threats?
    - Could cyber-attacks be classified as a WMD?
    - Are we any safer today than we were in 2001 against WMD threats? It's a low-probability, low-consequence event, but must still be taken seriously. How does it rank among other priorities?
    - Regardless of the perceived threat, what are the capabilities of the terrorists to launch such an attack?
    - Preparedness for WMD must not be ignored as other threats are considered or grant dollars continue to diminish.
- Mega Disasters and Cascading Effects
    - Events are not necessarily bound by the boundaries of a specific jurisdiction or a state. Therefore, interdependencies and supply chain must be considered.
    - Global impacts are realized economically as well as resource availability.
    - Many different disciplines (including NGOs) must be brought in to address potential impacts of a major event.
    - The planning paradigm must be changes to think more globally and consider the sharing of resources.
    - Leverage the THIRA and other methodologies to address resource allocations and planning shortfalls.
    - More robust training and exercise program to meet capability gaps.
    - Find innovative ways to leverage the resources of other partners (such as public health)

Business Session

- Elections were held for the new tri-chairs and the American Public Works Association (APWA) and Governors Homeland Security Advisory Council (GHSAC) were selected.
- John Madden was honored for his service as an outgoing tri-chair.

◊◊◊◊◊

January 18, 2013

Technologies that Will Change the World this Century: Implications for Security

Rocco Cassagrande, Ph.D, Managing Director
Gryphon Scientific

Cassagrande discussed emerging technologies with the understanding that predicting the future is difficult. In the past, most major technological advances were unforeseen. Examples of such technologies of the past include Lasers (thought to ultimately replace bullets), ARPA-NET (precursor to the Internet), and the birth control pill (meant to be a niche product used by few).

The best ways to predict the future include focusing on what new technologies are just emerging; understanding the advantages the new technology provides; the market forces; and how life sciences impacts the technology. He then laid out some issues in the field of life sciences due to the speed at which that industry is expanding.

Much of the life sciences field is being pushed by "synthetic biology" which is the application of engineering principles to biology. Synthetic biology has given us the ability to cheaply and quickly synthesize any genetic material desired. Such practices have given society results in products such as modern day corn and the domestic house dog. Much of the modern pharmaceutical industry is a result of similar technologies. Recent changes have made genetics faster, cheaper, and more extensively while also being more easily to manipulate.

Once new technologies are discovered, consideration must be given to how it will fit into the current market. How can it be produced, acquired, disseminated, and marketed? The process by which to develop a true chemical or biological weapon is fairly complicated, but unfortunately not much agent is required in order to cause significant deaths. Cassagrande then outlined a variety of weapons both actual and conceptual.

If the goal of a terrorist is to execute a biological attack, currently available technology can be used to kill or incapacitate hundreds of thousands of people. So the question becomes one of what the "pull" is of new technology from the standpoint of terrorists and criminals. There are 5 "pulls":

- Synthesis of Microorganisms is utilized to repair vaccine strains and synthesize almost any pathogenic virus. This is particularly dangerous because control of the most dangerous pathogens is no longer about securing a few laboratories and protecting existing stockpiles.
- Another "pull" technology is the manipulation of behavior. The pharmaceutical industry is constantly improving the ability to subtly affect neurochemistry. Therefore, other products become possible to help change attitudes. On the military side, these advances enable a greater range of weapon affects instead of simply lethal. Repressive countries could develop these weapons to control a restive population.
- Microbial Production of Illicit drugs is being done regularly. The pharmaceutical industry is engineering microbes to produce complex chemicals that are derived from plants that are hard to expensive to cultivate. The same technologies could be used to create varying strains of harmful pathogens. Overall, a requirement is still the combination of scientific skill and depravity to acquire the weapons and have the willingness to use them. These two aspects are often at odds with one another in the spectrum of rational behavior.
- Sex selection is likely to become easier in the coming years. Sonograms are inexpensive, and some cultures have a preference for male babies (a reasonable "pull"). Such a shift in population would result in fewer females to marry and a possibly increase in military adventurism or decreased socio-economic stability.
- Increased longevity in human life expectancy is increasing at an increasing rate. To significantly increase you and lifespan, interventions will become more personalized and expensive. In 15-20 years, the life expectancy is due to increase every year by one year.

Effective Information Sharing Through Fusion Centers (Moderated by Tri-Chair Tom Sands)

W. Ross Ashely, III, Executive Director
National Fusion Center Association

Ray Guidetti, Captain
New Jersey Regional Operations and Intelligence Center

Guidetti discussed how after years of discussing the "all-crimes" and "all-hazards" nature of fusion centers, Super Storm Sandy recently revealed the try meaning of those terms and what it means for information sharing. Sandy changed the landscape of how officials wanted information and how the

fusion center had to operate. They found five areas of conducting information sharing during a disaster and how to plug into an incident command system:

- Know the key decision-makers who need information including mutual aid partners. Once the customer was established; the fusion center had to enhance the information-sharing environment through improved dissemination. The EOC alone was not able to handle the immense amount of information moving through the system, so the fusion center became the primary distribution point during the storm and subsequent response.
- Gathering information was also critical for the fusion center before, during, and after the storm. Social media platforms were valuable resources to aid in the process of gathering. Concurrently, intelligence officers had to be sent out into the field to meet with local responders due to break-down in communications systems.
- The fusion center also needed to find ways to influence senior leadership. This task was especially important due to the mistakes of Hurricane Katrina and the risk of lawlessness still being fresh in the minds of many. The fusion center was able to work with senior leadership to help make critical decisions with the help of good intelligence.
- Once the senior leadership is informed, the fusion center can also help to influence the resource allocation decisions. Both police and fire responders needed critical information in order to secure locations out in the field.
- The fusion center was also able to influence the preliminary damage assessment process. This was particularly in communicating the condition of significant buildings such as schools and police stations. Already collected information on pieces of critical infrastructure proved to be valuable before and after the storm.

The challenge for fusion centers today is being able to elevate from simple information gathering, but to consider second and third order effects of an event. For example, a local power outage is an initial impact, but the second and third order effects include closed gas stations, shortages, and law enforcement challenges.

Ashley reviewed how the fusion center community has not had the luxury of dissecting disasters as the emergency management profession has spent decades analyzing. For some, this was the first time the fusion center was relied upon in a storm-related incident. In recent years, increased interest and scrutiny has been placed upon the existing fusion centers. The key in analyzing fusion centers in today's environment is ensuring leaders fully understand how these centers operate and work with the various disciplines. There continues to be a misperception that fusion centers are actually "counterterrorism centers."

Moving beyond just counterterrorism has been difficult to explain to policy makers. Fusion centers must continue to examine the full range of crimes since terrorists will often be revealed through indicators long before a significant event occurs. Such indicators would include a routine traffic stop, petty crime, or call for service. Fusion centers now support the broad range of homeland security functions including border patrols, drug interdictions, and customs issues. Reduced funding will continue to present challenges, but such reductions will require officials to work more closely with one another to share responsibilities.

Business Session

- The white paper analysis will be circulated to the membership. Associations will be asked to consider how those themes are integrated into their issues and meetings.
- Associations should ensure the appropriate people are present during NHSC meetings so as to facilitate decision-making capability.