Meeting Summary – Consortium Summer Session
New York City, New York
July 26, 2016

Dr. John Dryzehner opened the meeting with a welcome to all participants and introduction of new members.

Cybersecurity Roundtable

The first discussion of the day focused on an examination of current cybersecurity concerns. Mark Ghilarducci, Director of the California Governor's Office of Emergency Services, facilitated the discussion and kicked off the roundtable by highlighting a few actions his State has pursued in order to address key cybersecurity challenges. He stressed that there won't be a magic bullet, no one solution but that the first step needs to be a recognition that an approach that focuses on single industries or organizations will not be as successful as one that focuses on the whole of community. Two actions California took to address cybersecurity concerns include a Cybersecurity Task Force and a Cyber Integration Center. The task force facilitates cybersecurity outreach to private industry, academic, law enforcement, and government partners both inside and outside of California. The Governor's Cybersecurity Task Force is a public-private partnership that serves as the advisory body to the Cal-CSIC to raise awareness of new threats and mitigation techniques. In addition, the California Cybersecurity Integration Center (Cal-CSIC) carries out a number of critical cybersecurity functions, directly impacting his ability to manage both the homeland security and emergency management portfolios in California: but one of the biggest challenges they face is establishing a blueprint for integrating disparate efforts and mission sets into a unified, coordinated and streamlined operation that reflects the full intelligence cycle from collection, analysis to dissemination, and that supports a robust cyber response.

While great strides have been made, challenges still exist for all levels of government and the private sector to make operational partnerships more actionable. All attendees were asked to come prepared to discuss and identify challenges their organizations or industries face when addressing issues with cyber consequences. A number of organizations participated and they are included below.

- Protecting public health data. Health information vulnerability can compound the effects of a disaster and can constitute a vulnerability that can be exploited in crisis.

- Private businesses often do not want to admit when breaches occur which makes identifying the scope of a problem difficult.

- Prioritization of funding for organizations (public and private) can be very difficult in lean budget times. Specifically, for public works, where the entire industry/discipline is based on technologically connected components, it can be hard to wrap your head around the problem and prioritize funding to keep critical components safe.

- No line item funding for cybersecurity. While actions aimed at increasing cybersecurity preparedness, mitigation, and protection are allowable expenses under Homeland Security

grant programs, the lack of a specific cybersecurity grant often limits how much of already oversubscribed funds can be allocated to the cyber mission.

- Underreporting and misinterpretation of data can be an issue when trying to understand the scope of the problem at hand. Without knowing the range of vulnerabilities you, your systems, or systems you are connected to face and how often, it is hard to justify expenditures that are needed.

- Limited definitions or agreement on specific terminology. Difficult to see what cyber hygiene looks like at the State level. No agreement on who exactly constitutes a "cyber first responder" and there continues to be questions regarding roles and responsibilities at state and local level as well as the private sector.

- How to best leverage the National Guard and their cyber professionals as force multipliers. In some states, the Guard has small assessment teams that can

- How to effectively duplicate tradecraft to tackle transparency/security challenges. Key may be to anonymize data to assure all stakeholders feel comfortable being open and honest about breaches, vulnerabilities, etc. It is critical to identify what you can share and to only hold back when absolutely necessary.

After discussing challenges, the discussion turned to the question of how to best engage through the Consortium and where the group can make the biggest impact. One area the Consortium can have a voice would be on the issue of funding and current needs and priorities across various disciplines. While there may not be consensus to be found on every issue related to funding, the idea that the Consortium would be able to add value to the discussion and drive the conversation towards a solution was shared across many attendees. As evidenced by the conversation during the session, the Consortium is also an incredible resource of best practices, lessons learned, and recommendations for action needed at various levels of government and the private sector. Identification of challenges and gap analysis can be useful for legislators, agency officials, and the incoming Administration.

FEMA Update and Discussion

Tim Manning, Deputy Administrator for Protection and National Preparedness at FEMA, joined the Consortium to discuss a number of critical priorities for FEMA. First, Tim commented on the previous cyber discussion by referencing the National Cyber Incident Response Plan and the push the Administration is making to finalize that document after letting it remain in interim/draft status for years. The critical nature of the NCIRP is evidenced, he said, by the interconnectedness of all of the networks stakeholders access and utilize to accomplish their missions. Manning also weighed into the discussion regarding cyber funding and while he acknowledged Homeland Security grants were flexible enough to address the cyber need, he did highlight the disconnect that exists when cyber gets portrayed as an extra stressor on the budget and not just another need the budget must flex to cover.

Manning also discussed two other issues critical to Consortium members.

- NIMS Refresh – The refresh of the National Incident Management System (NIMS) is an issue that affects a number of stakeholders at various levels of the government and private sector. Over the last few months, FEMA has been aggressive in its efforts to seek input from stakeholders and conducted a formal comment process as well as in person meetings to collect feedback. In FEMA's own words, the draft of the refreshed NIMS retains key concepts and principles from

the 2004 and 2008 versions, while incorporating lessons learned from exercises and real world incidents, best practices, and changes in national policy, including updates to the National Preparedness System. Manning indicated the effort was a natural step to getting on a common plane and to assure that when Federal, State, and local officials need assistance, there is a seamless transition.

- Manning then shifted to the National Qualification System which is an effort to begin the process of bridging all of the disparate qualifications systems into one, cohesive plan in support of the National Response Framework. This idea generated from the NHSC and was an effort to recognize that commonality serves us all well nationally. He referenced the understanding that no one will ever have enough people to surge for a truly catastrophic disaster and that by deliberately identifying positions a State should have and accurately classifying them, the process of assisting and accepting assistance can be smoother. There was some conversation from attendees around the table regarding the phase in of these new qualifications and the need for rightsizing once major decisions are made to reflect the difficulties of transition. Comments were also made regarding the need to highlight the good that IMATs currently do to support response to a variety of situations. Additionally, the question was raised whether recovery teams would eventually shift in this direction.

Energy & Power Restoration and Planning for Long Term Outages

The next session was a panel discussion to highlight the ongoing challenges and opportunities that exist for State and local officials as public and private utilities work across the country to plan, and prepare for long term power outages. The goal of each presentation was to discuss lessons learned and identify key takeaways to guide future actions for critical stakeholders. The session was moderated by Puesh Kumar, Director, Preparedness and Exercise, Office of Electricity Delivery and Energy Reliability at DOE. Mr. Kumar started out the conversation by briefly touching on the release of PPD-41 regarding United States Cyber Incident Coordination. He mentioned that DOE would be developing actions to accompany the PPD as a reflection of the various impacts cybersecurity has in the tech-heavy Department. He then introduced the panelists.

Carlos Torres, Vice President - Emergency Management, Consolidated Edison of NY, Inc. (ConEd)

Mr. Torres highlighted many challenges the industry faces as they strive to secure the grid and response and recover from events that damage infrastructure and hinder power delivery.

- Complacency – During immediate response and recovery, the focus on power issues is sustained and significant but planning, training, and exercising must enjoy that same level of interest and focus.
- Competition for Resources – On one side is the competition for skilled workers to support a robust system and industry on a daily basis. In times of crisis and surge, however, the competition becomes fierce and sharing in these times becomes critical for the survival of the industry.
- Maintaining Relationships – Staying engaged during blue sky times can be difficult but utilizing exercises to keep critical partners engaged is a successful way to address this.
- Identifying Restoration Priorities – This is a common issue across the emergency management community as numerous stakeholders attempt to prioritize funding or the order by which services are restored post-disaster.
- Identifying and Troubleshooting Common Problems – Issues like travel restrictions, road closures, and the identification of staging sites are common and seem to be addressed each time there is a disaster. By planning for those issues, time can be saved during an event.

One best practice he shared was ConEd's decision to hire an in-house meteorologist that could help create impact models and provide them with the most accurate, actionable, and individualized data. In addition, the company reframed their use of employees to assign emergency roles which kept all engaged during an event and put emergency contracts in place to speed up response times.

Martha Duggan, Senior Principal for Regulatory Affairs, National Association of Rural Electric Cooperatives (NRECA)
Mrs. Duggan gave a quick overview of Co-ops in general and the values they share including their ability to speak the same language and the willingness to share resources to help in times of need. She did outline a number of challenges.

- Efforts to Continue to Build on Partnerships – Can't let partnerships developed in disaster be forgotten during the recovery and eventual preparedness/mitigation phase.
- Mutual Aid – Mutual aid for Co-ops is still in its infancy outside of the Co-op community and needs more support moving forward to solidify into a usable option.
- Recognizing the Unique Nature of Rural Communities – Rural communities may not have the massive infrastructure or population but still have critical needs that must be addressed. The challenge is to identify the needs, gaps, and challenges they face in order to educate public officials and encourage that their needs be taken into account.
- Relationship Between Power and Other Utilities – There is a clear nexus between power and other utilities like waste water, gas, etc. The relationships must be leveraged and recognized in all aspects of planning and exercising.
- Waivers for Response – Similar to the issue Carlos raised, often times issues pop up during disasters that require action by various levels of government that may not be familiar with the mission or scope of a utility's role in disasters.

Her key lessons learned included best practices from the January 2016 snow/ice storm. Co-ops initiated a conference call battle rhythm and solidified communication as a key component for success. She also advocates for developing protocol for common data reporting and assure everyone is on the same page. Reporting different data can confuse those who need the information the most. Mrs. Duggan also discussed how their decision to focus on cybersecurity by hiring staff and pushing education will continue to pay dividends moving forward. The issue is only going to be more significant.

Joseph (JT) Flick, Emergency Management Coordinator, New York Power Authority
Mr. Flick seconded many of the challenges shared by the other panelists but added a number of key lessons learned and challenges from the perspective of the NYPA.

- Consistent messaging can support a robust response and can unify various players under common goals and information. This must happen across all levels of industry and government during disasters.
- Not always obvious as to how to best exercise and train in a way that yields results.
- Must identify a way to have candid discussions with critical companies and co-ops and provide enough anonymity to assure honest and open dialogue. Without this level of honesty, questions go unasked and solutions may not be identified.
- Expectation management is huge for the public facing side of utilities and can have a massive impact on disaster response and recovery. In those critical hours and days, managing expectations of all involved must be a priority.
- Like the other speakers, he recognized that credentialing and access is a challenge.

- Understanding codependency and how it impacts other stakeholders, industries, and individuals is key for all involved.
- Transparency is key and this includes protocols or standards being used in a disaster. Mr. Flick specifically mentioned their lesson learned regarding sharing the battle rhythm with those who needed that information so all players understood priorities in those critical times.

After each panelist spoke, Puesh facilitated a short question and answer session. First, he asked how each of them defined "long term" in the long-term power outage discussion. While there was no consensus, mostly because in a planning scenario, it isn't a binary choice. They did agree, however, that the key is to set expectations early then revise as more accurate data comes in. In addition, there should be an effort to make this data customer specific and this strategy could be a model for the emergency management community.

The next question was "What do you, as power stakeholders, need from public safety?" The panelists gave various responses including, (1) resources; (2) specific guidance on where they go to for help and how they offer assistance if they can give it; (3) commitment to information sharing; (4) partnerships that support training and exercising; and (5) cyber mutual assistance.

The last question focused on the ability of the power industry to track back to physical delivery in the event of a cyber incident that affects the connection and automated delivery of the service. This was raised as a challenge by a number of panelists and the solution isn't always clear. What is obvious, however, is that the new workforce may not be trained in manual delivery and this vulnerability will require effort on the part of utilities as older workers retire. The good thing, however, is that there are built in layers of defense and these redundancies can help the system weather any number of threats.

NGA/GHSAC Presentation on School Safety

Perry Plummer, Director of the Division of Homeland Security and Emergency Management, presented in his role as a member of the GHSAC. Tara Shone, National Governor's Association, supported the presentation. This session focused on the work NGA has done to identify issues around school safety and identify the various strategies States are employing to meet this threat. The slides are full of interesting and actionable data (attached) and NGA agreed to continue to keep the Consortium informed as they update the information.

Working Lunch: Consortium Considerations for Supporting a Smooth Transition in Federal Administrations

Alaina Clark, Deputy Assistant Secretary with the DHS Office of Intergovernmental Affairs, spoke during the lunch session on the topic of the upcoming administration transition. She discussed the traditional protocol of political appointees submitting their resignations (regardless of incoming party) and the identification of acting leadership to fill the roles temporarily. She also mentioned that Departments and Agencies would be providing briefings to key campaign staff from both sides early as each candidate made arrangements for their future cabinet and policy initiatives. Internal transition planning is already taking place within each component of the Department, and these plans aim to identify key programs, policies, and ongoing actions as well as identify the current priorities in the works. This planning is done at a granular level and then rolled up in to larger documents with a real focus on the personnel and partnerships that are currently working on significant and impactful initiatives. Alaina expressed interest in the National Issues Brief the Consortium developed and indicated that any organization that has a similar document should share it because these insights are critical in the transition. The Consortium

should also think about what other Departments may benefit from our insight during this time of change.

CVE Emerging Issues and Best Practices
This session was a series of briefings and presentations to highlight the various efforts addressing CVE, domestic terror, and international information sharing. The first examined the various federal initiatives undertaken to advance efforts to counter violent extremism. The State of Illinois also highlighted a program developed to prevent violence and share their best practices. In addition, participants in a DHS-sponsored delegation visit to Paris described lessons learned from international colleagues related to terror attacks in 2015.

- Brette Steele, Acting Deputy Director of the Federal Interagency CVE Task Force, presented before the Consortium to specifically highlight what the Task Force was created to do and how they plan to coordinate on an issue of such consequence to the security of the nation. The new Task Force was created to coordinate across the 10 Departments and Agencies with critical roles to play. There are four lanes of effort the task force will focus on.
    - Engagement and technical assistance: This serves to build trust, improve understanding at the community level.
    - Intervention: Development of tools and resources for use by State and local stakeholders.
    - Research: This is where the most investments from Congress will come.
    - Communications and digital strategy

  Steele touched on the CVE funding through FEMA and the goals of future programs aimed at complex, coordinated attacks. She also took questions from Consortium members about a range of issues. Metrics were a topic of interest as many had questions about how success would be measured within an issue that is often difficult to quantify. While there are a number of qualitative ways to prove success or at least illustrate the impact a program or effort has, there will be additional discussions regarding how to "prove a negative." In addition, Steele touched on a variety of issues related to active v. reactive messaging and the digital strategy that the US employs to combat radicalization. She indicated government isn't always credible on this issue and that partnerships with community organizations are essential. She also mentioned the limitations on domestic covert propaganda. The Federal Government is also working to leverage research into what messages are received best in order to truly make a difference in the ability of foreign or domestic actors to radicalize others.

  Steele concluded with a few recommendations:
    - Partner with the community. These partnerships do not need to be based solely on the issues of radicalization and should be tailored to what issues most affect the community. In some cases, it will be unsolved homicides, access to prayer space, or perceived discrimination.
    - Follow through is key. When local officials show a genuine effort and follow through on the issues that matter most, honest and open dialogue follows.

- Junaid M. Afeef with the Targeted Violence Prevention Program at the Illinois Criminal Justice Information Authority briefed on the efforts the State of Illinois has undertaken to meet a diverse threat within their communities. Their broad charter allowed the organization to quickly

adapt to emerging needs at the state level and their goal is to address ideological violence in whatever form it takes. The group is a resource to the community and they can explore similar strategies with unique approaches for a number of threats. Like any new program, and especially in light of any new grant funding that could make these programs more viable in other communities, partnerships are key. One of the projects Afeef focused on was a pilot called Viral Peace which provides training for young people to develop counter/alternative narratives to radicalization. More detail can be found in the powerpoint presentation attached.

- Abigail Williams, Office of Intelligence and Analysis, DHS and Jennifer Del Toro, Washington Regional Threat Analysis Center, DC HSEMA joined the meeting to discuss a delegation of fire officials from the United States that traveled to Paris, France following the attacks in November 2015. The briefing was a preview of what will eventually be a published report. The slides are not available as they are pre-decisional.

Multi-Agency Collaboration in the Emerging Infectious Disease Landscape
Marissa Raphael, Deputy Commissioner, Office of Emergency Preparedness and Response (OEPR), NYC Department of Health and Mental Hygiene joined the meeting to discuss her experience with emerging infectious diseases. She highlighted the role of the NYC Department of Health and Mental Hygiene (DOHMH) and provided lessons learned and best practices related to their planning for and responses to a number of recent events and threats. Her powerpoint is attached.

Dr. Bradley Dickerson, Senior Biodefense Advisor at the DHS Office of Health Affairs discussed a number of efforts the Department has undertaken to address emerging issues in the public health arena. He began by highlighting DHS's role in public health which is heavy on research, countermeasures, as well as border control issues that play into the spread of diseases. The Department creates, exercises, and executes plans in preparation and response to emerging infectious diseases and Dr. Dickerson specifically referenced examples like H5N1 and H1N1 preparations a number of years ago. With the current focus on Zika, Dr. Dickerson did touch on the efforts DHS is undertaking to address the issue. He continued, though, with words of caution that there is often a disconnect with issues of high risk versus those issues with a high profile. Zika certainly has a high profile, but he cautioned that these issues which may have limited impacts can take funding and attention away from high risk issues like CBRN countermeasures or mitigation for high impact diseases.

Both Marisa and Dr. Dickerson were asked about the current funding issues surrounding public health efforts and the lack of a dedicated emergency funding pool (like FEMA's Disaster Relief Fund). Supplemental funding is not a strategic or long-term approach to critical public health emergencies as it really ends up being like rearranging deck chairs on the Titanic. Both speakers referenced the maturation of the public health response overall and were encouraged by the progress made over time in the connection between the emergency response community and public health.

Cyber Resource Center Work Group Report Out
The work group continues to work with representatives from the Naval Post Graduate School to identify a path forward for the Cyber Resource Center. NPS is in the process of creating a beta version of the center which will then be vetted through a number of groups. The Work Group will be putting together a small assessment team of practitioners (from Consortium organizations) in the coming months and ask that those interested volunteer when that opportunity becomes available.