Metropolitan Washington
Council of Governments

NATIONAL CAPITAL REGION
EMERGENCY PREPAREDNESS COUNCIL (EPC)

Wednesday, May 10, 2017
2:30 P.M - 4:30 P.M.
Ronald F. Kirby Training Center (First Floor)

1) Welcome, Announcement(s), and Approval of Minutes

David Snyder, Vice Mayor, Falls Church; Chairman, EPC

a) Chairman Snyder opened the meeting at 2:30 p.m. at which time he invited all participants to provide self-introductions, and gave an overview of the meeting agenda.

b) Chairman Snyder requested consent to sending formal letters to Major General Bradley Becker acknowledging his continued stewardship and efforts for strengthening collaboration between the Military District of Washington and MWCOG; a letter welcoming Major General Michael L. Howard to the EPC; and a letter thanking Jim Dinegar as head of the Greater Washington Board of Trade for his region-wide prospective as well as his front and center participation in all things related to EPC and emergency issues. With no objections, MWCOG will prepare formal letters for signature(s).

c) Chairman Snyder officially welcomed Major General Michael Howard, incoming Commander, United States Army Military District of Washington and Joint Force Headquarters-National Capital Region. Unfortunately, MG Howard was not available to attend the meeting. He was represented by JFHQ-NCR Deputy Commander Egon Hawrylak.

d) Update on DHS Complex Coordinated Terrorist Attack, Special Grant Request for NCR:
Brian Baker, Interim Director, DC HSEMADC HSEMA noted that DC HSEMA agreed to take the lead in submitting a region-wide grant application for the Complex Coordinated Attack (CCA). They developed and submitted a grant request on behalf of the region. FEMA is reviewing all the CCA grant requests. They have not announced award recipients.

Mr. Kadesch, Director, ONCRC FEMA has received unofficial notification that 29 applicants will receive grants, but unable to confirm that the NCR will be one of the awardees. He indicated that the NCR application submitted was very solid and competitive. Since FEMA received so many requests and they desire to support as many jurisdictions as possible, there will likely be a decrease in the requested amount in the applications.

e) Charles Madden, Chief of Grants Management Division, DC HSEMA presented a brief UASI grants update for FY15, FY16, and the FY17:
There are currently two active grants underway:

I. FY15 UASI grant is a three-year grant slated to expire in August 31, 2018; most of the awarded grants are scheduled to complete by May 31, 2017, with only a few grant extensions. At present, we have received in-house reimbursement requests for 54 percent of the grant with 48 percent of the grant reimbursed to sub-recipients. Given that this is a three-year grant, there will be ample time for project extensions and minor corrective adjustments. Report-outs will continue to be provided to the HSEC and the HSEC Advisory Council until the grant is expended.

II. FY16 UASI awards were disbursed in mid-September 2016 with a 21-month period of performance, and are anticipated to end on May 31, 2018. The end date of the grant is August 31, 2019. Adjustments and project wrap-up can be completed in the third-year. The award is approximately ten-percent expended, consistent with D.C. fiscal year projections.

III. The FY2017 Appropriation Bill was passed by Congress and it was signed into law by the President on May 5, 2017, with significant changes in policy. However, the current appropriations for FY2017 is basically the same as last year. Award applications will be released soon and will require quick turn-around in response(s).

- The pool of applications is basically the same as it was last year, and unless there are significant changes in DHS evaluation of threat or policy, it is anticipation that awards in approximately the same amount in previous years will be distributed this year.
- The non-profit security grant was increased this year, from $20M to $25M. Last year there were 25 successful applicants.
- The SAA for the NCR will submit the NCR application this summer. It is anticipated that sub-awards will be issued in late September.
- The CCTA program was not approved for funding in FY2017 by Congress. CCTA funding may become available through the UASI grant.
- FEMA should release grant application packets in the coming weeks and there will likely be short-turn-around time for application submittals that will be due by the end of June 2017. It is anticipated that FEMA will distribute awards in August and that the NCR will issue sub-awards by the end of September.

Discussion:

1) Grant application materials are distributed around the region by multiple means. Scott Boggs receives the communication releases and will take the lead in notifying appropriate MWCOG members.
2) The formal process for deciding regional proposals and applications start at the committee level.
3) A list of proposals from committees was turned into the Advisory Council for consideration in April 2017 to develop a list of recommended projects/priorities for funding to address capability gaps. The Advisory Council will submit their recommended list of projects/priorities to the HSEC to make regional decisions and the projects that they approve will be included in the NCR application to FEMA.
4) Once awards/application packets are received from FEMA, the region is prepared and on-track for quick application turn-around.

Action:

1) Establish a group of volunteers to review future efforts of EPC to insure its greatest impact going forward.
2) MWCOG was requested to prepare requested letters for signature.
3) Scott Boggs will take the lead for notifying appropriate MWCOG members of grant releases and materials.

f) Chairman Snyder requested a motion to approve the February 8, 2017 EPC meeting minutes. A motion was made and seconded, and the minutes were unanimously approved.

2) NCR CYBERSECURITY AWARENESS

Chairman Snyder introduced Michael Dent, *Chief Information Security Officer (CISO), Fairfax County* and *David Jordan, Chief Information Security Officer (CISO), Arlington County* to discuss cybersecurity awareness in the business community and with the citizens of local jurisdictions, and the impacts thereof; refrained from focusing only on agencies, addressed mass-communication to the public.

Michael Dent, Chair, NCR CISO Committee, Chief Information Security Officer (CISO), Fairfax County

The presentation provided was geared more toward awareness and general guidance on preparedness and public messaging in cases of cyber-incidence(s).

a) All local jurisdictions such as Fairfax and Arlington disseminate messaging differently, based upon available funding. For example, through the Consumer Protection Division, the Fairfax County annual cyber awareness week takes a deeper-dive with educating the public, particularly with cyber experiences that work closely with consumers purchasing items via the internet; there are fewer awareness efforts in the interim, for example, there is no year-round campaign.

b) Internal communications to end-users are working well, but there continues to be a need for improved communications and awareness across-jurisdictions. This is due to limited funding.

   I. The regional CISO committee meets monthly to discuss current cyber issues and communication is dispensed to jurisdictions directly impacted with limited region-wide or external communications.

   II. It is difficult for each jurisdiction to set-up a standard process/plan. There are efforts underway to look at creating a single program that would disseminate awareness throughout the region. A recent example of communication breakdown: The Virginia State Police has had an incident for two-weeks with no communication with the local jurisdictions elaborating the cause of the incident; this had a negative impact with local police departments; obvious communication gaps, for example e-mails and websites went down. There needs to be some form of communication between those who need to know. There is an issue here that needs to be remedied. Consider involving public information officers and those at the executive level.

   III. Agencies should continue to protect themselves and mitigate risk, but be sensitive to notifying other externals agencies that need to know; give them appropriate and timely notices; currently local agencies do not have the funding to make this happen. Public information officers and executive levels need to get involved in the recovery of sensitive communication.

Find ways to appropriately notify the public; some jurisdictions have the luxury of using different multiple notification methods because they have funding available to apply effective messaging, for example, Fairfax and Arlington Virginia have good command centers that are successful with public communication; while other jurisdictions are not fortunate to have such funding.

David Jordan, Communications (RESF-2), Chief Information Security Officer (CISO), Arlington County

a) CISO has been mandated to take a closer inward/outward look at better ways to communicate cyber incidences to the public:

   Inward look: upon completion of a vulnerability risk assessment, it was determined that additional funding is needed for critical infrastructure and cyber awareness for residents and local businesses. Currently, there is not enough funding for critical infrastructure upgrades for self-supporting operations such as with water, traffic signal control, sewage, etc.; many are functioning with antiquated systems, particularly from a cyber-perspective. Also, because breaching the current cyber controls have grown significantly, physical controls for safety need to be instituted.

   Outward look: consider cyber public service announcements. During the annual Cyber Security Month (usually in October), Homeland Security distributes packages that include posters, which are transformed into PowerPoint presentations and are rotated on large screens to attract the attention of constituents; these visuals are kept in place until the following year and then replaced with new ads/posters. This method of getting the word-out can be done on a local level at minimum cost.

b) There are twenty-two governances that actively participate in the CISO Committee and many have not been the beneficiaries of the same level of funding. Currently, it takes too long to obtain funding for state-of-the-art upgrades; applications and/or systems. Arlington has started a small radio station (WERA) and every Thursday at 11am there is a cyber-security discussion on “practical cyber-security.” Opt-in alerts are offered to the public, a place where they can go to get real-time updates; small businesses are more inclined to participate and will set-up workshops and training exercises; a consideration should be given toward developing a CISCO school.

I. Committee participants have been asked to sign-up for Multi-State Information Analysis Group (MSI). The MSI has proven to be successful with communicating up-to-date cyber related information and will conduct free risk assessments upon request.
CISO plans to have a second MSI risk assessment done; a ten-day event where five analysts are sent on-site to closely evaluate network systems, which ultimately creates a recipe for success; analysis can better identify what may have been missed by end-users/developers. The same kind of risk assessment needs to be done for critical infrastructure.

II. Address cyber security awareness early in school systems, between K-12; do not wait until college to begin educating. Start sending children homework assignments focused on cyber security; the parents are likely to get engaged as they help with homework; add to assignments references for county specific websites/links that direct to more on-line information such as protection against credit card and phone scams, for example. Also, local libraries and fire departments can be used for advertising; work to promote awareness nationally not just locally; collaborate with federal government for improved literature.

III. Integrate cyber security into everyday things; currently 21st Century technology devices are out-pacing security solutions that should initially be built-in; it has become too easy for devices to be infiltrated. Build security into new devices by educating product integrity engineers who are willing to put together inherent security systems; removing the need for multi-billion-dollar security systems.

Action:

1) Identify funding avenues for critical infrastructure – give examples of worse case scenarios to improve chances for support; enhance training for personnel running cyber security systems to expand knowledge-base (up-to-date technology; more cyber-security centric). Consider a cyber security table-top exercise and keep RESF5 abreast of upcoming cyber related exercises.

2) MWCOG to investigate avenues for public messaging, i.e., what should be done when phone systems, internet or e-mails go-down? Perhaps form a sub-committee on raising awareness; include DHS, cyber experts, elected officials, military representative (for lessons learned), and CIO's. What is the importance of IT when systems fail – how are systems brought back on-line? Consider tapping into the federal government; develop icons like Smokey the Bear; Ernie Electron for at-a-glance awareness; DHS could assist in developing literature to promote national awareness; perhaps a u-tube skit to get people thinking. There is caution to be sensitive to potential sabotage with public messaging; safeguard information, for example, PDX's should not all have the same passwords or access codes.
   I. What should the publics' response be during an incident?
   II. Leadership and elected officials to participate in cyber awareness discussions and table-top exercises; offer comments on known challenges and significant risks. Identify what role the EPC can play in improving cyber security awareness within the community. Include emergency managers, finance/procurement, CISO, RICCS, PIOs in cyber-security awareness.
   III. Build better direct communications relationships with 3rd party critical infrastructure providers; amend State regulations around water, power, and sewage for example; currently emergency managers are the primary incident commanders.

3) Standardize messaging; draft language clause; develop Standard Operating Procedures (SOP) related to cyber communication. Develop general PSAs that go across jurisdictions – long-term on-going with one subject per announcement; something that resonates with people; don't give too much information that will cause people to ignore or overlook the importance of the message.

4) Bring back to EPC's next meeting September 13, 2017 for review.
   I. RESF-15 should design a campaign around public messaging/awareness that pushes-out basic alerts and information; effective communication after an event has occurred; what does public do if cell phones don't work or email is compromised. Develop a plan of action for preparedness; then submit to

HSEC for regional response guidance; the plan developed should tie-in the big picture.

II. MWCOG Procurement should investigate sharing messaging verbiage regionally for purchasing contracts and notification agreements; develop a standard template of procurement to include cyber-security (there may be existing language in cyber-annex).

5) June 13 MWCOG will host Control Systems Cybersecurity Workshop from 10:00 am to 11:30 am in COG's Ronald F. Kirby Training Center on the first floor (lobby level). The workshop is geared to help anyone involved with implementing cybersecurity in the Control Systems (CS) life cycle learn best practice techniques to better protect their CS. The workshop teaches control system basics, protocols, how to use the NIST Risk Management Framework and the Cybersecurity of Facility-Related Control Systems Design Guidance Unified Facilities Criteria (UFC), and how to use tools and methods to inventory, diagram, identify, attack, defend, contain, eradicate and report a cyber-event/incident. To register and for additional information, please click here: https://www.eventbrite.com/e/control-systems-cybersecurity-workshop-tickets-34289955179.

6) November 2017 the National GridEx will host a nationwide tabletop scenario on how to respond to power outages and attacks. MWCOG circulate details to the EPC.

7) Invite CISO to present at an upcoming PIO committee meeting.

3) UPDATE ON HOMELAND SECURITY EXECUTIVE COMMITTEE 2.0

Scott Boggs, Managing Director, DHSPS, MWCOG
Brian Baker, Interim Director, DC HSEMA

Mr. Boggs and Interim Director Baker provided the EPC an update on the restructured Homeland Security Executive Committee (HSEC) and HSEC Advisory Council. The HSEC, previously known as the SPG/CAO-HSEC, is continuing with an extensive strategic visioning process to help jurisdictions anticipate and prepare for situations that require regional coordination and response. The HSEC Advisory Council was established to share information and intelligence on regional threats and opportunities, and provide recommendations on homeland security, preparedness and response priorities to the HSEC.

a) HSEC 2.0 identified the need to establish an HSEC Advisory Council that will be charged with evaluating proposals that are associated with UASI funding for sustainment, as well as identify those that should not move forward due to funding constraints. UASI funding will not necessarily be the primary source of funding for these and other projects. Each project will be addressed from a regional perspective. The Advisory Council will evaluate new proposals with a two-month commitment for response turn-around. The Advisory Council is comprised of first responders, RESFs, emergency managers, representatives from the States, police and fire chiefs, and communication specialist.

b) The HSEC Advisory Council worked diligently to closely evaluate each project for regional sustainment, as well as new proposals. Each project was aligned with available funding with a focus on the Strategic Plan. There was candid review and feedback for approvals/denials; some projects were sent back for re-evaluation and/or reallocation. The HSEC Advisory Council is positioned to assist with reprogramming of some equipment purchases already in progress. Recommendations will be compiled and presented to the HSEC for consideration and approval. The HSEC is relying on the Advisory Council to ask any clarifying questions on projects prior to submission.

<u>Next Steps:</u>

1) Begin strategic level work and identify gaps and clearly identify how those gaps can be addressed regionally.
2) Focus on regional programs and not just purchasing. HSEC will make UASI funding decisions.

Action:
EPC should be given the opportunity to assist with identifying gaps.

4) NCR HOMELAND SECURITY STRATEGIC PLAN UPDATE

Kim Kadesch, Director, Office of National Capital Region Coordination, FEMA, DHS

a) Mr. Kadesch requested the EPC members review meeting notes from the last meeting for detail on the plan for moving forward. The planning group is well represented, with a noted switch in leadership. Katie Reed has taken a new position, and is now working in a new position at FEMA.
b) A charter to provide guidance to the group has been drafted and is now under review. The June HSEC meeting will likely be a high-level discussion about the strategy of work for the group moving forward. To stay in alignment with HSEC annual established workflow, the Charter has an aggressive timeline to complete the strategy by November 30, 2017. The process for gathering information, assessing risk to establish long-range guidance, which will have limits is expected to be released soon. This guidance will dictate priorities for the year. There will be a focus on whole community via survey input and homeland security as an enterprise and not just on UASI funding. The NCR RESFs are represented and the Board of Trade will become involved later in the process.
c) The HSEC will meet on June 22, 2017 for a high-level discussion around strategy, and annual planning will be based upon priority updates with a focus on whole-community and Homeland Security as an enterprise.
d) Priorities for NCR Homeland Security Strategic Plan are to provide support and assist with identifying gaps; put greater concentration on cyber security; establish region-wide community based CPR programs, and basic-line first-aid trauma training so that public can learn appropriate care during terrorist or active shooter events; stabilize until first responders arrive on scene (stop-the-bleeding before help arrives).
e) Continue “see-something – say something” campaign. Red Cross should be included in awareness initiatives as they are able to conduct public mass-communications. Design awareness for public preparedness and consciousness of cyber-events.
   I. Public training should be focused around the basics; things like what individuals can do to help themselves and their neighbors until help arrives.
   II. Internal government alerts and messaging are usually effective; however, closer attention is needed on finding ways to better communicate to everyday citizens. Because there is concern for reputation damage or lowering of confidence from consumers, many for-profit companies are reluctant to release sensitive information until it is too late for a timely and appropriate response; this continues to be a concern for first responders.
   III. Package communications from a training perspective, what to do in bomb-threat related events; develop scenarios, i.e., “hide from the wind and run from water in a hurricane.” Combine multiple messages in a single package.
   IV. Determine training resource spending related to improvised nuclear device (IND); develop clear and consistent messaging for health and safety, i.e., “everyone stay inside.” Take an all hazard approach to messaging, such as which direction to go in cases of gas leak?
   V. Mr. Lewis with RESF16 has a wealth of knowledge and should be considered during planning process. Look at the D.C. campaign and the regional *Stop-the-Bleed* initiatives; consider CPR training and different ways to empower people.

There was acknowledgment of the April 2017 paper written by students working on Masters in Public Administration with a focus on cyber-security; “*Solutions and Challenges to promoting Strong Public Cybersecurity Practices*.”

Action:
EPC should have an active role in the strategic plan process. Consider aligning future meetings with timelines; perhaps schedule ad-hoc meetings so that EPC is kept informed as they provide value from an

end-user perspective and can easily identify public concerns.

5) LAW ENFORCEMENT COMPLEX COORDINATED ATTACK (CCA) EXERCISE

Patrick Hudgens, Supervisory Special Agent, Tactical Supervisor – Special Response Team, ICE/HSI, DHS

Mr. Hudgens was called away on an operational mission at the last minute and was not available to provide an Initial report on the exercise.

6) NCR EMERGENCY PREPAREDNESS COUNCIL 2017 PRIORITIES

David Snyder, EPC Chairman
Scott Boggs, Managing Director, DHSPS, MWCOG

To be addressed at September 13, 2017 meeting.

7) OTHER BUSINESS

None.

8) ADJOURNMENT

Next meeting, Wednesday, September 13, 2017 -- 2:30 P.M. – 4:30 P.M. at MWCOG Ronald F. Kirby Training Center (First Floor). Topic of discussion will be to identify EPC Focus Areas for 2017-2018.

With no further business, the meeting adjourned at 4:30 PM.

Attachments:

1. Meeting Agenda
2. Draft Meeting Minutes of February 8, 2017
3. NCR Urban Areas Security Initiative Grant Updates of May 10, 2017
4. CyberSecurity Practices
5. Solutions and Challenges to Promoting Strong Public Cybersecurity Practices
6. NCR EPC Membership Roster
7. Draft EPC 2017 Meeting Schedule

A list of reference materials and detailed reports can be obtained from the on-line library link: https://www.mwcog.org/events/2016/?F_committee=128; Click Login Button at Upper Right and use Username: your email address; Password: your personal password provided by COG.