



Rhode Island Emergency Management Advisory Council
THE MEETING OF THE COUNCIL WILL BE HELD:

October 14, 2014

2:30 PM

MINUTES

I. Call to Order - Lt. Governor Roberts

Attendance

Lieutenant Governor Elizabeth H. Roberts
Adjutant General Kevin R. McBride
U.S. Senator Sheldon Whitehouse
U.S. Representative James Langevin
Colonel Steven G. O'Donnell
Rhode Island U.S. Attorney Peter Neronha
Captain John Kondratowicz
Jamia McDonald, Executive Director, RI Emergency Management Agency
Paul McGreevy, Rhode Island Department of Business Regulation
Kurt Huhn, State Chief Information Security Officer
Thom Guertin, State Digital Officer
Molly Donahue McGee, SENEDIA
Dr. James Ludes, Salve Regina Pell Center
Shad Ahmed, Higher Education
Jim Ball, Rhode Island Department of Environmental Management
Erin Lambie, United States Coast Guard
Brian Pires, U.S. Attorney's Office
Joseph Baker, Rhode Island Department of Transportation
Pamela Marchant, Rhode Island Water Resource Board
Gregory Scungio, Rhode Island E 9-1-1
Jeff Hatcher, Rhode Island Architects Engineers Emergency Response Task Force 7
Alan Seitz, Department of Homeland Security
Peter Ginaitt, Lifespan
Peter Marinucci, Providence Emergency Management Agency
Denis Riel, Chief of Staff, Rhode Island National Guard
Lieutenant Colonel Michael Tetreault, Rhode Island Air National Guard
Marian Juskuv, EMA North Smithfield
Elizabeth McDonald, Rhode Island Red Cross

Armand Randolph, Rhode Island Emergency Management Agency
Steve Morley, Rhode Island Emergency Management Agency
Donna DiMichele, Office of Library and Information Services
Sue Earley, Dept. of Behavioral Healthcare, Developmental Disabilities and Hospitals
Ken McCarthy, Rhode Island Public Utilities Commission
Christopher DeGraves, Governor's Commission on Disabilities
Chris Harwood, Johnson and Wales University
Geof Milner, Rhode Island SATERN
Vladimir Ibarra, Office of the Lieutenant Governor

Chair Roberts opened the meeting by making a motion to approve the minutes. The motion was seconded and the minutes were approved. Chair Roberts continued with a discussion of the Ebola epidemic. She highlighted some key messages from HEALTH including:

1. To date, no one has become infected with Ebola in the state. The Providence videographer, who contracted Ebola while covering the crisis in Liberia, has been recovering according to a spokesman for the Nebraska Medical Center in Omaha yesterday.
2. HEALTH activated its Incident Command System, as activation enables HEALTH to provide additional resources to planning and communications efforts and to incorporate stakeholders in their preparedness efforts.

For further inquiries she advised calling the HEALTH information line at 401.222.8022/RI Relay 711 or visit <http://health.ri.gov/diseases/ebola/>

II. Rhode Island Emergency Management Agency Update

There was no Rhode Island Emergency Management Agency update. Chair Roberts discussed how the August 12 meeting provided a general overview of our strengths and weaknesses in regards to cybersecurity. That meeting was a scenario-based cyber attack to the State and illustrated how the different agencies would deal with it. Members of the Rhode Island Cyber Disruption Team, the Fusion Center, State IT, RIEMA and other stakeholders attended.

The meeting today was the continuation of laying the groundwork on the Cybersecurity posture of the State. EMAC invited a distinguished cybersecurity panel comprised of Congressman Langevin, U.S. Senator Whitehouse, Superintendent/Colonel O'Donnell, General McBride, private industry and academy to provide a global perspective culminating the discussion and setting up actions steps for the state to implement.

IV. Cyber Discussion – Senator Whitehouse, Congressman Langevin, General McBride, Col. O'Donnell, Academia and Private Industry members.

Chair Roberts introduced Senator Sheldon Whitehouse who has been active in efforts to draft comprehensive legislation to protect America from the threat of a cyber attack. He has been leading bipartisan cyber discussions including chairing the Senate Intelligence Committee's Cyber Task Force. Also, as chairman of the Judiciary Subcommittee on Crime and Terrorism, Senator Whitehouse has held a number of hearings on the cyber threat, including hearings on the

role of law enforcement in responding to cyber attacks and the risk posed to American businesses by the theft of intellectual property/trade secrets by cyber criminals. The Senator is a member of the Budget Committee; the Environment and Public Works Committee; the Judiciary Committee, the Health, Education, Labor, and Pensions Committee; and the Special Committee on Aging.

Senator Whitehouse opened his remarks by praising the work that Congressman Langevin has been doing in this field. Senator Whitehouse discussed the cyber capabilities in Rhode Island and how they need to be leveraged as we have a growing cyber workforce, military assets and top-notch academic institutions. The Senator spoke about some of the concerns with privacy and security, and what the nation is doing to address the growing cyber threat. He discussed how foreign governments steal intellectual property worth billions of dollars from American businesses and of the need to raise awareness in order to combat these attacks. He highlighted the need for greater partnerships with private industry and how we can turn this liability into a growth sector.

Chair Roberts introduced Congressman Langevin, who is a founding member of the Congressional Cybersecurity Caucus and served as Co-Chair of the Center for Strategic and International Studies' Commission on Cybersecurity for the 44th Presidency. He was the primary author of the first comprehensive cybersecurity legislation to pass either chamber of Congress, and is one of the first Members of Congress to speak about the need to address the growing threat. Congressman Langevin is a member of the House Armed Services and Intelligence Committees, and a former member of the Homeland Security Committee.

Congressman Langevin agreed with his colleague in the Senate on the need to integrate the private industry. He discussed how the current structure of the Internet makes these companies vulnerable to breaches and attacks since security was not a major consideration. The Congressman related how technology is constantly evolving and basically doubling every eighteen months. He expressed concern about attacks to the power grid and critical infrastructure as these systems relay heavily on technology. He saw as a major challenge managing and closing the vulnerability gap. However, a silver lining was how Presidential Executive Order 13636 charged the National Institute of Standards and Technology with developing best practices so that industries can look at best models to adopt to manage cybersecurity risk.

Director McDonald also pointed to the Commerce Department's National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity. The Framework will help organizations charged with providing the nation's financial, energy, healthcare and other critical systems better protect their information and physical assets from cyber-attacks. She mentioned how Rhode Island has led the way with the creation of innovative relationships between business and government, namely the Cyber Disruption Team. Also, RIEMA continues to develop their cyber security infrastructure and is expanding work with universities and colleges that provide cyber security development programs. She discussed a recent New York Times article pointing to the data breach of JP Morgan Chase compromising seventy-six million households and seven million businesses. In the article JP Morgan Chase CEO provided a grave warning about the need for help and their projections to spend \$250 million a year to increase

security in prevention. Director McDonald stressed the need to build alliances, contacts and connections as we rally the private sector in a proactive manner. Director McDonald provided recent examples of collaboration with private industry including an issue paper recently released by the Pell Center around the potential of professionalizing the workforce development component of Cyber. Also, the Southeastern New England Defense Industry Alliance (SENEDIA) hosted a Defense Innovation Days highlighting Rhode Island's robust defense industry and the advancements made, but asked how it translates to cyber. She then asked the panelist what should the state be doing and whether there are support structures needed.

General McBride emphasized how the Cyber Disruption team was the first in the country and efforts to increase capabilities through warfare warriors, the need to create frameworks and memorandum of understanding to enhance support and address legal issues under Title 10. He expressed the need for greater collaboration with private companies to build capacities and address vulnerabilities.

Colonel O'Donnell discussed how hackers are going around security firewalls through third party vendors. The Colonel provided the example of the Cryptolocker ransomware and efforts to increase capacity with the National Guard, the Fusion Center and the U.S. Attorney's Office.

Ms. Donahue Magee, Executive Director of SENEDIA expressed how government has been a good partner and needs to continue lobbying people facing the risk. Because NIST is voluntary it is difficult to know what does regulation look like. Sharing best practices might be a solution, and there is a sharing working group with Raytheon that continues to strengthen the network. Ms. Donahue Magee stated how SENEDIA will continue enhancing relationships with local communities, elected leaders and federal government to inform and educate citizens on the importance of these issues.

Mr. McGreevy interjected as to ensure we are a secure state, incorporate the insurance side. His agency has been working closely with the National Insurance Commissioners on addressing cyber security risks. Mr. Ginaitt also mentioned the need to include not for profit hospitals as they provide very critical care and need the same level of protection.

V. New Business, Member Comments, Suggestions

Chair Roberts announced that RIEMA, along with RI State Police and the RI National Guard would conduct an extensive Cyber Tabletop Exercise in December. The Tabletop Exercise will be the first dedicated to banking and finance, as well as continuing consumer-level education.

The meeting was adjourned at 3:50 p.m. The next meeting will take place on Tuesday, December 9th