

*Statement for the Record*

*Ensuring Effective and Reliable Alerts and Warnings*

*Peter T. Gaynor CEM, Director, Rhode Island Emergency  
Management Agency*

*Before the House Committee on Homeland Security: Subcommittee  
on Emergency Preparedness, Response, and Communications*

*Washington, D.C., February 6, 2018*

Good morning Chairman Donovan, Ranking Member Payne, and distinguished Members of the subcommittee. It is a pleasure to appear before you today to discuss the critical importance of reliable alert, notification, and communication systems at the local, state and federal levels that we depend on within the State of Rhode Island to successfully achieve our mission. These systems, the plans and policies that shape their use, and the personnel that train, maintain and operate them, are a core function of preparedness and response across the country.

My name is Pete Gaynor and I am the Director of Emergency Management in the State of Rhode Island. I am also Chair of the State's Interoperable Communication Committee (ICC) responsible for ensuring alert, notification and communication systems are properly governed, aligned, and integrated. As the Director and a professional emergency manager, I am responsible for preparing for emergencies, coordinating the activation and use of resources, ensuring an integrated and unified response, and managing the recovery effort in support of our local and state governments, citizens and businesses.

I am pleased to be testifying before the subcommittee today. I have submitted my full statement to the committee, which I ask to be made part of the hearing record.

Today, I want to briefly provide the subcommittee with, first a snapshot of those alert, warning and communications systems and their use within the State of Rhode Island, second, what we have done since the Hawaii false alert; and finally, some insights and recommendations for a stronger more resilient alert, warning, and communications system nation-wide.

Let me describe our system from the local level up. In 2015, the State of Rhode Island invested in a commercial mass notification system called CodeRED. Using the Emergency Management Performance Grant, we purchased on behalf of all 39 municipalities and selected State agencies, a singular common system in order to remove duplication of effort, improve operational efficiencies and to save precious local, state and federal funding resources. Authorized and trained agents at the local level can launch any public safety related alert within their jurisdiction. The State has the capability to launch on behalf of a single municipality, multiple municipalities, or the entire state depending on the threat or hazard.

With the implementation of the Integrated Public Alert and Warning Systems – IPAWS, we have been able to seamlessly integrate CodeRED in order to complement the federal Emergency Alert System (EAS) and Commercial Mobile Alert System (CMAS).

In August 2017, we completed a long overdue update of the State's EAS Plan. We have spent significant energy to ensure plans, procedures, equipment, training, safeguards, and testing are up-to-date and fully operational. This remains an ongoing process.

Since 9-11, Rhode Island has been fortunate to receive federal funding to build and maintain what we believe is a first-class, border-to-border, interoperable Land Mobile Radio (LMR) system called the Rhode Island Statewide Communications Network, or RISCON. RISCON allows thousands of our first-responders to seamlessly operate in any corner of the state, to include cross-border to many of our Massachusetts and Connecticut communities.

To ensure redundancy and interoperability throughout the State, we have a VHF system called the Emergency Management State Radio System (EMSTARS) which connect all local emergency managers. That system is being refreshed this year. We also have the Rhode Island Law Enforcement Telecommunication System (RILETS) which is a data system mainly dedicated for daily coordination of local and state police departments.

We continue to rely on other core federal systems such as FEMA's National Warning System (NAWAS) and the FEMA National Radio System (FNARS) to ensure we have multiple communication paths, such as non-switched terrestrial voice circuits and High Frequency (HF) radio for both voice and data.

Since the January 13, 2018, Hawaiian false ballistic missile alert was issued, we have redoubled our efforts to review plans, procedures, policies, redundancies, training, authorized users, functionality of equipment, interoperability and safety measures to ensure we fully understand the strengths, weaknesses, and potential gaps of all of our alert, warning and communication systems. We have re-validated our internal launch and approval process, ensured pre-scripted messaging is common across all of our platforms, to include recall messaging should an erroneous alert be triggered. This review process continues today.

In New England, at both the state and federal level, we are in the process of reviewing past practices for alert and notification procedures, such as those outlined in the July 2016 FEMA Manual 211-2-1, NAWAS Operations to make sure published guidelines and instructions are logical, executable and reasonable after what occurred in Hawaii.

As outlined in the manual, "threats posed by natural and manmade disasters or enemy attack make it imperative for state, local, territorial, and tribal governments to have access to an effective and reliable means of communication with which to warn the public of impending emergencies so that they may take protective actions." My fellow New England Directors and I completely support this premise and are working diligently to ensure we all have a safe, secure, and reliable alert and warning system.

We also rely on a host of social media platforms like Twitter and Instagram to share and collect information. We also look forward to the deployment and use of FirstNet, however in the light of recent events and the growing complexity and interdependency of many of these technologies, we must proceed with caution and apply applicable lesson-learned to avoid past missteps.

In conclusion, in addition to reviewing and validating our current systems, I believe we have created what I call the Technology Trap. I believe our problem is similar to the challenge the military has with GPS and the digital mapping world – will our soldiers still be able to navigate with a pencil, paper map and magnetic compass should our GPS constellation be disrupted? Can we as emergency managers communicate in a world where any combination of a cyber-attack, power disruption and/or natural hazard takes out our digital alert, warning, and communications networks? Are we ready to communicate, alert and warn in an analog world? Can we communicate to our citizens without cell phones and the internet? The harsh reality is if you can't communicate, you can't govern.

Some recommendations:

-Ensure FEMA alert and warning procedures are aligned to present day threats and shifts in technology to include clearly defining responsibilities between all levels of government for alerts and warnings.

-Develop a national concept of operations on how to better use General Mobile Radio Service (GMRS), Family Radio Service (FRS), Travelers' Information Station (TIS or Highway Advisory Radio), service with a focus on how to network these systems with state and federal systems in order to enhance our ability to communicate with the public in an austere environment.

-Encourage additional training and exercises at every level to ensure leaders and operators are familiar with every detail of every communication, alert and warning systems, procedures, and shortfalls. I would encourage a more robust and regular nationwide IPAWS testing program focusing on the fundamentals of communicating in a degraded environment.

-Review the DHS Security Clearance program to ensure the right decision-makers, throughout every level of the emergency management system have the correct clearance level, so matters like threat briefs and time-critical secure communications can seamlessly, rapidly, and securely occur.

Thank you, Chairman Donovan and subcommittee members, for the opportunity to appear before you today.

I stand ready to answer any questions you might have.