Charley English

President, National Emergency Management Association
Director, Georgia Emergency Management Agency

STATEMENT FOR THE RECORD

On behalf of the
National Emergency Management Association

Submitted to the House Committee on Homeland Security
Subcommittee on Emergency Preparedness, Response, and Communications
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

United States House of Representatives

Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management

October 30, 2013

National Emergency Management Association
444 N Capitol Street, NW, Suite 401
Washington, D.C. 20001
202-624-5459

Introduction

Chairman Brooks, Chairman Meehan, Ranking Members Payne and Clarke, and distinguished members of this panel - thank you for holding this hearing today on one of the most critical issues currently facing our nation. Cybersecurity and the resultant vulnerabilities and consequences could easily match the impact of any significant natural disaster, so we must analyze these threats carefully and plan to manage them accordingly.

The establishment of this committee came about more than a decade ago in the wake of an attack which came from an under-appreciated threat. This morning, we stand at the precipice of another such attack – one from a potentially nameless, faceless, and equally under-appreciated adversary. The threat of a cyber-attack not only surrounds us, but also poses the additional threat of compromising the response and recovery efforts to the consequences of such an attack.

Last summer, the Chairman of the House Intelligence Committee said he expects what he called "a catastrophic cyber-attack in the next twelve to twenty-four months."

Earlier this year, former Secretary Napolitano said an incident on the scale of September 11 could happen "imminently."

The Defense Science Board went even further saying "coming cyber-attacks could present an existential threat to the country."

As emergency managers, we operate in a world of consequence management. Accordingly, we must understand threats, protect vulnerabilities, and know how to manage consequences. As we examine the cyber-threats facing this nation, we cannot fall into a September 10, 2001, mindset. Our actions must be pro-active and consider all potential outcomes. We must never say, "it cannot happen here" nor shall we fear being labeled an "alarmist" by merely acknowledging the potential devastating consequences of this already validated threat.

The Threat

Plenty of experts remain ready and willing to provide thoughts and hypotheses regarding the current cybersecurity threat. The vulnerabilities and resulting consequences we face in these threats represent the "bottom-line" for the emergency management community. Vulnerabilities are points of attack and weaknesses to be exploited. The emergency management community must address the consequences of vulnerabilities being exploited, not just the existence of vulnerabilities themselves. In his report to Congress of March 12, 2013, Director of National Intelligence James Clapper outlined how "we are in a major transformation because our critical infrastructures, economy, personal lives, and even basic understanding of – and interaction with – the world are becoming more intertwined with digital technologies and the Internet."

Such analyses are especially concerning as we continue witnessing a metamorphosis of the cyber-threat. Once a means by which to conduct espionage and steal information, the realm of cybersecurity must now include an analysis on the security and viability of our critical infrastructure. At the RSA Cybersecurity Conference on March 1, 2012, former FBI Director Robert Mueller stated "to date, terrorists have not used the Internet to launch a full-scale cyber-attack. But we cannot underestimate their intent. In one hacker recruiting video, a terrorist proclaims that cyber warfare will be the warfare of the future." Only through good fortune have organized terrorist groups not yet taken a greater interest in cyber-attacks. But such a day is certainly coming.

Earlier this year, Anonymous petitioned the White House to recognize hacking attacks as a legitimate form of protest. Their solicitation argued hacking is no different than marching in an Occupy Wall Street protect. We must consider how such an approach can be combatted through our current systems and processes. Even though some experts believe Anonymous represents no true threat, others believe such an organization could bring down part of the U.S. electric power grid. Most recently, the homeland security community has been concerned with and has devoted significant resources to combatting Homegrown Violent Extremists (HVE). It is reasonable to conclude that these individuals, acting alone or in small groups, certainly have the motivation and expertise to conduct a cyber attack.

Unfortunately, cyber-threats represent risks far more diverse than most any other we face. While nation states like Iran present a significant cyber-threat, the greatest cyber-threat from a nation likely comes from China where hacking stands as an official policy. Just recently, the Chief of Staff of the People's Liberation Army put the cyber-threat into perspective when he suggested such an attack could be as serious as a nuclear bomb. Even though in his report to Congress Director Clapper said "advanced cyber actors – such as Russia and China – are unlikely to launch such a devastating attack against the United States outside of a military conflict or crisis that they believe threatens their vital interest," the threat alone should be enough to garner the attention of the homeland security and emergency management community.

Addressing Vulnerabilities & Consequences

Emergency managers stand increasingly concerned regarding the inter-connectedness of the threat and everyday life in America. Citizens can evacuate in anticipation of a hurricane. Strong building codes and safe rooms can protect lives in anticipation of earthquakes or tornadoes. But as we consider the breadth and depth of our reliance on the cyber-infrastructure, the emergency response efforts regarding consequence management could easily overwhelm local, state and federal assets due to the interdependencies of critical infrastructure and key resource protection as well as the ease of vulnerability exploitation from a cyber-attack. Consider this short list of potential hazards and vulnerabilities:

- Computer-controlled dams protecting a low-lying community,
- National power grids and nuclear power plants,
- Emergency Alert Systems (EAS) and 911 systems,
- Traffic systems utilized to evacuate a population,
- Banking systems ranging from Wall Street to basic online transfers and ATM withdrawals,
- The national airline and air traffic control network,
- Complex and simple communications systems from Emergency Operations Centers to the basic smartphone, and
- Water supply networks and waste management systems.

Even many of today's commonly-used Global Positioning System (GPS), which relies heavily on a cyber-structure, represents a potential target vulnerable to attack. Taken by themselves, each of these threats could have devastating effects. But emergency managers must consider a potential event impacting any number of combinations of these systems.

The connectivity of systems today makes the consequences of a cyber-attack more significant at all levels of government and throughout the private sector. Admittedly, emergency managers often defer cyber-security issues to information technology (IT) officials; yet state IT professionals and other leaders will rely on emergency managers to respond to the consequences of an attack. The emergency management and IT communities must establish relationships and engage in coordinated planning and information sharing long before an event occurs.

States such as Michigan continue taking a keen interest in how to manage the cybersecurity threat. Through robust coordination and planning at the state level, Michigan approaches cybersecurity with the same concepts as those employed when preparing for and responding to natural or terrorist threats.

The Michigan Cyber Initiative brings together many state agencies including the Michigan National Guard, State Police, and Department of Technology, Management, and Budget in a coordinated effort to enhance detection of cyber-attacks and integrate response systems. The Michigan Cyber Initiative integrates the Michigan Cyber Command Center, Michigan Cyber Defense Response Team, and Michigan Intelligence Operations Center to enhance prevention, early detection and rapid response, and control, management, and restoration. The Michigan Online Cyber Toolkit raises awareness and preparedness for all the components of the cyber-ecosystem. The toolkit provides best practices and easy steps for safeguarding a vulnerable environment. It also offers the chance for users to quiz themselves, download posters and calendars, and obtain tip sheets on how to solve online problems. The toolkit is broken down by sectors including homes, businesses, government, and schools.

Michigan is clearly working hand-in-hand with various components in ensuring the addressing of cybersecurity across all disciplines. Even as these relationships continue developing in other states, however, we must examine how the consequences of a cyber-attack will be addressed. Furthermore, we must complete an honest assessment of necessary authorities and whether they represent adequate resources to respond to such an attack.

Current Authorities

As NEMA received briefings on the Quadrennial Homeland Security Review (QHSR) of the Department of Homeland Security (DHS), we inquired as to whether the department would examine physical impacts of cybersecurity. They informed us that while the QHSR would include some examination of the consequences of a cyber-attack, the department's analysis of past cyber-attacks reveal very few physical impacts constituting a significant threat to safety and life. We want to ensure that all potential consequences of a cyber-attack are thoroughly considered. We feel like anything less is short sighted and underestimates the ability and creativity of the enemy whether the enemy is foreign or domestic. Our country has on several occasions witnessed the creativity of those who are intent on harming us. There have been shoes, printer cartridges, under ware and pressure cookers used as bombs and, of course, airplanes used as missiles.

But even states struggle in addressing this threat. In a survey completed in February of this year, NEMA learned:

- 79.1 percent of states interpret the consequences of a cyber-attack under statutes as "All Hazards" versus 20.9 percent which list it as a specific hazard.
- 62.8 percent of states do not maintain a law enforcement-specific component to any of the state statutes relating to cyber-response.
- No clear best practice exists in assigning responsibility of coordination of resources to prepare for, respond to, or recover from a cyber-attack with only 41.9 percent of states citing such a directive. Of the 41.9 percent responsibility ranges from the emergency management to IT, homeland security, and the fusion center.

With states remaining somewhat unclear on the appropriate course of action, the current lack of a cohesive national strategy at the federal level is not surprising. We hope that the response strategy matures the federal government will not over-bureaucratize the process and bury state and local governments in a sea of reports, guidance documents, and processes.

We think it is prudent to continue the insistence of metrics and return on investment calculations on the millions of dollars in initiatives funded at DHS. Some organizations, however, such as the Office of Cybersecurity and Communication (CS&C) within DHS continue admirable work in their outreach to state and local officials. The effort must be comprehensive and coordinated in order to ensure all the nuances of the threat receive appropriate attention. Federal efforts must be structured in concert with states and locals rather than adopting a top-down approach.

But underlying statutory authorities are equally unclear. During the NEMA Annual Emergency Management Policy & Leadership Forum in Seattle, Washington last year, a panel of experts addressed the statutory issue. According to the panelists including a former Adjutant General, a DHS Deputy Assistant Secretary, and several state Homeland Security Advisors, the Civil Defense Act of 1950 (81-950) represents the only law potentially applicable to a potential cyber-attack. Since the original intent of this Act provided for the response to a nuclear attack from the Soviet Union, the time to explore the efficacy of our current statutory authorities is now. Current statutory authorities are lacking regarding cyber-attacks and are currently under revision; however, the recent remark by President Obama that a cyber-attack can now be classified as an "act of war" significantly changes the "environment." This recent change should be taken into consideration when speaking of statutory authorities and can be used to further illustrate the fluid and uncertain nature of the issue.

Most emergency managers will turn to the Robert T. Stafford Disaster Relief and Emergency Assistance Act (PL 92-288). Unless the consequences of a cyber-attack truly have catastrophic and physical consequences, however, the Stafford Act will be limited. Unfortunately, too many of the legislative fixes currently under consideration in Congress only address the prevention and preparedness side of cybersecurity. While the pre-event aspects of cybersecurity maintain a high level of importance, so too will the post-event considerations.

Moving Forward

The purpose of this hearing is to ensure consequence management resulting from a cyber-attack is recognized as a priority with emphasis equal to preparedness measures. As Congress considers legislative options, the needs of the state and locals ultimately responsible for the consequences of a cyber-attack must be first and foremost. In May of last year, NEMA joined with the American Public Works Association, Council of State Governments, International City/County Management Association, National Association of Counties, National Association of State Chief Information Officers, National Association of Telecommunications Officers and Advisors, National Conference of State Legislatures, the National League of Cities, and the International Association of Emergency Managers to ask Congress for your consideration of key principles and values when considering cybersecurity legislation. The outlined principles and values include:

1. State and local governments must be viewed as critical stakeholders in national cybersecurity efforts. Both execute programs overseen and funded by federal agencies, and frequently are custodians of federal data. They also operate and manage critical infrastructure including data centers and networks which are necessary for basic homeland security and emergency management functions. Therefore, the federal government must work with state and local government to share threat information and to provide technical support to protect computer networks and other related critical infrastructure.

2. The federal government must avoid unfunded mandates on state and local partners. Public budgets are still strained at all levels of government, and while state and local stakeholders wish to contribute to the overall cybersecurity effort, the ability to independently fund initiatives at this

time is unlikely. Likewise, federal program requirements and directives have traditionally hindered state and local governments from potentially achieving economies of scale.

3. Federal, state and local governments should collaborate to invest in cybersecurity awareness, education and training for public sector employees, contractors and private citizens.

4. The civil liberties and privacy of all citizens must be maintained while also establishing the safety and stability of the internet and electronic communications. This is especially critical as governments continue to expand online and electronic services. Safeguarding public sector data that includes personal information of citizens will require cooperation and collaboration on data standards and cybersecurity methodology at all levels of government.

5. Many federal initiatives fund internet and information security programs. However, without cross-cutting communication and coordinated assets, the efforts will not realize maximum efficiency and impact. If there are privacy and security requirements that are preconditions of federal programs and funding they must be uniformly interpreted and implemented across all agencies and levels.

Earlier this year, NEMA attempted an effort to address cybersecurity consequences simply from the emergency management standpoint. A workgroup comprised of many NEMA members has worked since March in developing a doctrine for emergency management directors to consider. Unfortunately, even this effort proved more difficult than originally anticipated, and instead of continuing alone, NEMA has since joined forces with the National Governors Association (NGA) in their cybersecurity efforts.

NGA recently released a "Call to Action for Governors for Cybersecurity." The document outlines guiding principles, immediate actions to protect states, provides multiple examples from various states, and discusses a path forward. The guiding principles include supporting governors, remaining actionable, reducing complexity, protecting privacy, employing technologically-neutral solutions, promoting flexible federalism, generating metrics, and promoting the use of incentives. NEMA looks forward to continuing our work with NGA as this complex issue gains increased attention.

The combined capacity of federal, state, and local governments to adequately safeguard the Nation's critical infrastructure systems remains essential to ensuring effective operations across the full spectrum of the threats we face. Furthermore, in order for communities to effectively manage emergency situations, cyber systems must be resilient to acts of terrorism, attacks, and natural disasters.

Conclusion

Cybersecurity represents the most complex threat and advanced vulnerabilities we as a nation face. We must ensure consequence management resulting from a cyber-attack is recognized as a priority with emphasis equal to preparedness measures. The challenge for all of us will be to examine it through a new prism, for we will fail if we respond the same way as always. This is not a traditional threat and reaches across sectors of our society which may have never before worked together. Cyber-threats can only be addressed through collaboration, planning, and a deep understanding of the potential consequences. For if we fail either through prevention or response, the impacts truly could be disastrous.

Thank you.