Testimony of;

James W. Terbush MD MPH

To the Colorado House Transportation and Energy Committee

IN SUPPORT OF REP. JOANN GINAL'S BILL

"FORTIFICATION OF COLORADO'S LIFELINE INFRASTRUCTURE TO WITHSTAND LARGE-SCALE ELECTROMAGNETIC DISTURBANCES"

29 April 2015

Thank you, Mr. Chairman for asking me to take part in this important discussion. Up until April of last year I was actively involved in domestic disaster preparedness and response for the military working at NORAD and US Northern Command. Prior to that I was fortunate in my career to be able to participate in International Disaster Preparedness and Response and specifically the 2010 Haiti Earthquake response. Since leaving Government I have enjoyed teaching disaster public health and consulting on a variety of health and disaster related topics. I am delighted to be able to speak with you today on a topic I consider to be of key importance to our nation that is, **Resilient Hospitals in a longer-term power outage.**

Resilient Hospitals: in the opening chapters of the celebrated book, Five Days at Memorial, the author Sheri Fink recounts in detail the horrifying facts of "life and death in a storm-ravaged hospital" post Hurricane Katrina. She describes a major medical center without electricity, clean water, waste water treatment, ventilation and only limited communications, supplies and transportation. Patients deprived of lifesaving technology, lingered and then died in the heat, a nightmarish scenario indeed. Of the 16 critical infrastructure sectors, Healthcare and Public Health is certainly important in immediate disaster response and recovery. The populations we serve, those critically ill and injured hospitalized patients, are arguably the most vulnerable segment of our society. The other reason perhaps we need to focus on resilient hospitals today is that the sector is one of increasing complexity and relies on a combination of support from the other sectors, especially the power grid and increasingly a reliance on moment to moment connectivity with Information Technology (IT) and the Internet.

Resiliency: for our purposes, a working definition of resiliency is "the ability to take a blow and come back". Resilient Hospitals are able to prepare for and adapt to changing conditions and

withstand and recover rapidly from disruptions. Not just hospitals should be considered but healthcare facilities of all types are vulnerable and need to be "resilient". Patients receive care at a variety of different facilities to include long term care, (nursing homes) and clinics. It is not just the physical structure which must withstand a blow and come back, but we need resilient staff, resilient management, resilient plans and planning. A Naval Aviator friend told me once that "Truly superior pilots plan ahead to avoid those situations where they might have to use their superior skills". Hospitals and their staffs have repeatedly shown superior skills in disasters, but we would prefer to have less heroics and more routine activity carried out "according to the plan".

Hospitals have unique vulnerabilities: patients are more sensitive to changes in environment; temperature, humidity, noise, etc. The very young and the very old, (and of course the very sick) often have very different requirements. Some patients have to be isolated from others and need separate ventilation systems, changing rooms, etc. Some patients rely on ventilators or other specialized technology with a limited battery supply of perhaps several hours when the power goes off. If back-up diesel generators are tasked to perform beyond their limits, these devices eventually run down as well. Another vulnerability common to devices connected to the Internet is that some medical devices, to include some life-sustaining medical devices can be "hacked" remotely, either turned off or the settings changed. When the power goes completely off, hospitals quickly become dark and dangerous places. Most back-up electrical generators are designed for no more that 48-72 hours of continuous operations. After that they probably need routine maintenance and certainly re-fueling. Another unique issue is the evacuation of critically ill patients connected to life-support to another healthcare facility. When only one or two facilities are no longer able to care for patients, the option remains to evacuate. When health-care facilities across an entire region are affected, we have to be able to continue to provide for these patients in place.

Electronic medical records and data stored in the "Cloud" can be both a help and a hindrance in a disaster: when IT systems and access to the internet stop, modern medicine, as we know it, ceases to exist. Although valuable patient records and other data may exist somewhere "out there" on a server, inability to access or retrieve data stops our business as usual. The ability to record and store patient demographic and clinical information on a secure hand-held device, especially in a mass casualty, is essential. The data can be downloaded later or sent to another device when internet connectivity is restored. Tracking of patients and accompanying family members is particularly important when facilities are being evacuated. Otherwise we may have to revert back to paper records and clipboards, which were both used in the mass shooting incident in Aurora Colorado, a couple of years ago. Less effective perhaps, but that ability to revert back to another legacy system is also an indicator of resiliency.

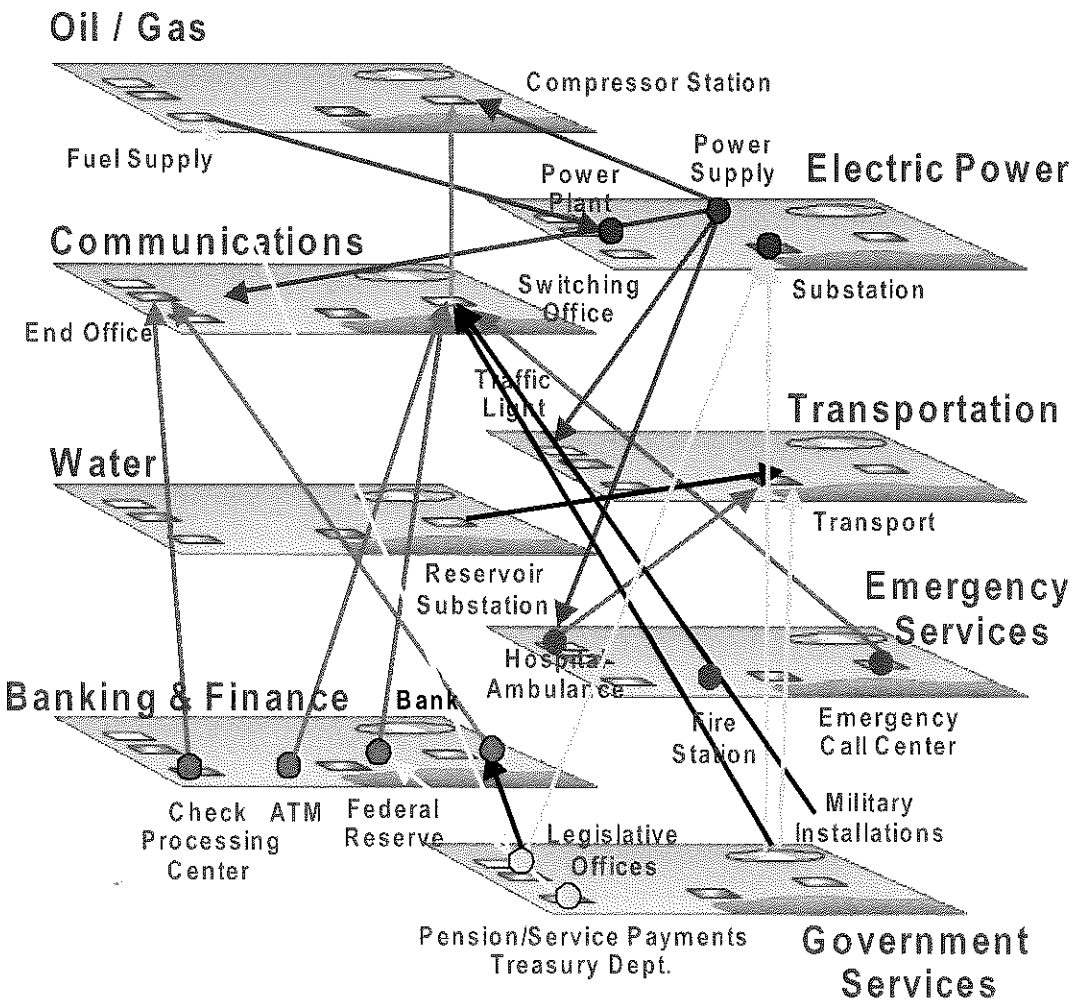
A "just in time" supply chain complicates disaster healthcare delivery: the need for cost effectiveness complicates resiliency. Because it is more cost-effective to have vendors deliver supplies "just in time" there is less waste and less wasted shelf space. The days of large stocks of IV fluids, pharmaceuticals and "disposables" are gone. Instead vendors may obtain supplies from multiple sources, both domestic and overseas, and those vendors in turn have a supply chain from even more obscure sources. IT systems connect them all. As systems become increasingly complex they are often increasingly fragile. For no-fail missions (such as disaster healthcare, communications, ICU/CCU's, life-support and emergency rooms) we need redundancy and additional capability. This may include more trained staff, equipment and supplies in-house. Functions within the hospital are then prioritized as mission critical or non-mission critical such as we do in the military. Functions of lower priority may then need to be turned-off in an orderly manner, as in the phrase "failing gracefully". All this adds to business costs; staff hours, overhead, liability and represents an additional "risk" to the hospital.

Alternate technologies can be useful in disaster, if they are "baked in": PPD -21 promotes research and development to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber-technology. An architectural firm based in Boston is designing hospitals "from the ground up" which have more natural ventilation and lighting, are more sparing in the use of water and have a reduced requirement for waste water treatment. Some of these hospitals include a thermal tower which pulls air through the facility without electricity. They have large fans in common areas in case this does not work. The day to day electricity requirements for these hospitals are much less, more of the hospital is on the ground level and patients can be moved more easily without the use of elevators. Why is this technology not used more commonly, because these hospitals are being designed for third world situations in Africa. Certainly these countries which experience disasters and loss of life more frequently than we do here, benefit from this technology. Maybe certain adaptations of this type of technology are needed here to make our hospitals more resilient? These technologies are appropriate and resource-saving all of the time and do not have to be "turned on" in disaster.

Cyber-secure micro-grids: another example of technology useful "all of the time", is the use of a back-up electrical generation system, incorporating conventional diesel generators, renewables, batteries and the ability to push power back into the grid, with possible associated cost-savings. These micro-grids are less susceptible to hack attacks and electromagnetic disturbances (EMP) as well. I've seen one of these systems seamlessly transition from providing power for a large portion of a military base, to putting power back into the grid, and then storing energy in batteries. They also have the ability to have parts of the system go off-line for

maintenance or re-fueling, which was a problem we saw in Super-storm Sandy. Currently the Department of Defense has such a Joint Capability Technology Demonstration (JCTD/SPIDERS) which could be adapted for use in a large medical campus, for example. I can discuss this subject of cyber-secure micro-grids in greater detail if you are interested.

A "System of Systems" approach is needed: a favorite slide I like to use when giving similar talks is one showing the critical infrastructure sectors, stacked on top of each other, with lines of interconnectedness. The power grid relies upon transportation, transportation is connected to water, the water sector needs electricity and IT seems embedded in all sectors. Healthcare may not directly affect all the other sectors but it is fair to say all the other sectors affect healthcare. Especially vulnerable in a disaster are patients at home or in a long-term care facility which must have an electrical outlet for life-sustaining technology; ventilators, oxygen generators and renal dialysis.



A culture of preparedness: finally, individuals and families need to take on more responsibility for their own needs in advance of disaster. This includes a family disaster plan. For obvious reasons the fewer persons needing assistance from hospitals for disaster related illness and injury, more of the limited medical resources can be directed toward those in greatest need. Despite numerous examples and warnings, individuals and families still fail to prepare for even "predictable surprises", such as power outages, stores closing, and bad weather. The normalcy bias or "fallacy of normalcy" as one author put it, makes us assume that tomorrow will be very much like today and what we are seeing on television, or hearing on the radio, or hearing from neighbors is exaggerated and causes some of us to drastically underestimate the effects of the disaster.

Thank you for the opportunity to address this committee on Resilient Hospitals in a longer-term power outage.

References:

Beyond Hurricane Heroics, Sheri Fink;
http://sm.stanford.edu/archive/stanmed/2013summer/article5.html

Five Days at Memorial;

http://www.randomhouse.com/book/203207/five-days-at-memorial-by-sheri-fink

PPD-21: https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resilience

http:/www.dhs.gov/critical-infrastructure-sectors

http:/www.dhs.gov/healthcare-and-public-health-sector

Cyber-secure Micro-grid; http://energy.gov/eere/femp/articles/spiders-joint-capability-technology-demonstration-industry-day

Barnett, Daniel J.; Sell, Tara K,; Lord, Robert K.; Jenkins, Curtis J.; Terbush, James W.; Burke, Thomas K.; "Cyber Security Threats to Public Health", *World Medical & Health Policy*; Volume 5, Issue 1, Pages 37-46, March 2013.