EVIDENCE OF GROWING THREATS TO OUR ELECTRIC GRID
(Since November 2015)

- On December 23, 2015, the world witnessed 225,000 electricity customers lose power after a sophisticated Russian cyberattack struck the Ukrainian grid.

- On April 14, 2016 the U.S. House of Representatives held a hearing titled: "*Blackout! Are We Prepared to Manage the Aftermath of a Cyberattack or Other Failure Of The Electrical Grid?"* In this hearing, the Committee noted:

  The DHS reports that the energy sector is the target of more than 40 percent of all reported cyberattacks. In 2014, the National Security Agency (NSA) reported that the agency had tracked intrusions into industrial control systems by entities with the technical capability "to take down control systems that operate U.S. power grids, water systems and other critical infrastructure." [i]

- On April 25, 2016, the U.S. Government Accountability Office (GAO) published a report that concluded: *"[U.S. Department of Homeland Security] DHS and [U.S. Department of Energy] DOE, in conjunction with industry, have not established a coordinated approach to identifying and implementing key risk management activities to address EMP risks."* [ii]

- In December 2016, the U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) publicly reported on the Russian military/civilian intelligence-developed malware tool that took down the Ukrainian grid in 2015: "BlackEnergy." In 2018 comments for the FERC Docket RM18–2–000, *Cyber Security Incident Reporting Reliability Standards*, national security experts noted:

  This Joint Analysis Report (JAR) titled "GRIZZLY STEPPE – Russian Malicious Cyber Activity" was proof of the real and direct danger to electric grids by malware, since BlackEnergy was previously identified by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of the Department of Homeland Security (DHS) as being present in America's energy sector. [iii]

- On March 28, 2017, the Senate Committee on Homeland Security and Governmental Affairs reported about critical grid infrastructure:

  The United States depends on its critical infrastructure, particularly the electric power grid, as all critical infrastructure sectors are to some degree dependent on electricity to operate. A successful nuclear electromagnetic pulse (EMP) attack against the United States could cause the death of approximately 90 percent of the American population. Similarly, a geomagnetic disturbance (GMD) could have equally devastating effects on the power grid. [iv]

- On October 12, 2017, the U.S. House of Representatives Committee on Homeland Security Subcommittee on Oversight and Management Efficiency, held a hearing titled "*Empty Threat or Serious Danger: Assessing North Korea's Risk to the Homeland."* During this hearing, the Chairman and Chief of Staff for the Congressional EMP Commission provided written testimony that:

  In the event of a nuclear EMP attack on the United States, a widespread protracted blackout is inevitable. This commonsense assessment is also supported by the nation's best computer modeling:

--Modeling by the U.S. Federal Energy Regulatory Commission (FERC) reportedly assesses that a terrorist attack that destroys just 9 of 2,000 EHV transformers--merely 0.0045 (0.45%) of all EHV transformers in the U.S. national electric grid--would be catastrophic damage, causing a protracted nationwide blackout.

--Modeling by the Congressional EMP Commission assesses that a terrorist nuclear EMP attack, using a primitive 10-kiloton nuclear weapon, could destroy dozens of EHV transformers, thousands of SCADAS and electronic systems, causing catastrophic collapse and protracted blackout of the U.S. Eastern Grid, putting at risk the lives of millions.

Thus, even if North Korea has only primitive, low-yield nuclear weapons, and likewise if other states or terrorists acquire one or a few such weapons, and the capability to detonate them at 30 kilometers or higher-altitude over the United States, as the EMP Commission warned over a decade ago in its 2004 Report: "The damage level could be sufficient to be catastrophic to the Nation, and our current vulnerability invites attack." [v]

- In December 2017, the Trump Administration published the National Security Strategy of the United States of America, stating that:

  The vulnerability of U.S. critical to cyber, physical, and electromagnetic attacks means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and means of communication.[vi]

- On March 23, 2018, The U.S. Department of Justice charged nine Iranians with conducting a massive cyber theft campaign on behalf of the Islamic Revolutionary Guard Corps. Hundreds of American universities and private sector companies as well as the Federal Energy Regulatory Commission which regulates the interstate transmission of electricity, natural gas and oil and maintains the details of some of this country's most sensitive infrastructure.

- On May 20, 2018, the National Weather Service, National Oceanic and Atmospheric Administration and U.S. Department of Commerce published a Request for Information (RFI), seeking input from the public on ways to improve government coordination and on long-term guidance for Federal programs and activities to enhance national preparedness for space weather events. This RFI noted:

  Space weather, a natural source of electromagnetic pulse (EMP), can disrupt, degrade, or damage infrastructure and technology systems, including the electric power grid. This makes preparing for space weather events critical to national security, infrastructure services, space missions, and technology innovations (such as autonomous vehicles) that rely on communications systems and GPS for positioning, navigation, and timing services. Preparing the Nation for space weather events will contribute to addressing many priorities identified in the 2017 National Security Strategy (NSS). [vii]

- Throughout the Summer of 2018, the DoD released numerous reports of the Congressional EMP Commission completed the previous year. For example, the Chairman's report observed:

  China: *A January 2016 article "General Trend of the Worldwide Revolution in Military Affairs and the Form of Future War" by China's National Security Policy Committee sees "electromagnetic pulse bombs" among the new "disruptive technologies" that "can change the 'rules of the game'" by disrupting U.S. military "precision warfare capabilities centered on*

information technology" thereby sounding "the horn of a new round of revolution in military affairs."

North Korea: *North Korea in 2012 and 2016, amidst threats to annihilate the United States and a rapidly advancing nuclear missile program, orbited two satellites in polar orbits that cross over the U.S. on trajectories consistent with practice or preparation for a surprise nuclear EMP attack.*

On January 6, 2016, North Korea provoked another nuclear crisis with its fourth illegal nuclear test of what it claimed was an H-Bomb. On February 7th, again amidst threats to make a nuclear missile strike on the United States, Pyongyang orbited another satellite, the KMS-4, on the same polar trajectory as the KMS-3.22

Kim Jong-Un has threatened to reduce the United States to "ashes" with "nuclear thunderbolts" and threatened to retaliate for U.S. diplomatic and military pressure by "ordering officials and scientists to complete preparations for a satellite launch as soon as possible" amid "the enemies' harsh sanctions and moves to stifle" the North. North Korean press asserts readiness for "any form of war" and includes their satellite with "strengthening of the nuclear deterrent and legitimate artificial satellite launch, which are our fair and square self-defensive choice." Moreover: "The nuclear [weapons] we possess are, precisely, the country's sovereignty, right to live, and dignity. Our satellite that cleaves through space is the proud sign that unfolds the future of the most powerful state in the world." The same article, like many others, warns North Korea makes "constant preparations so that we can fire the nuclear warheads, which have been deployed for actual warfare for the sake of national defense, at any moment!"

On September 3, 2017, North Korea conducted its sixth underground nuclear test. The test produced a seismic signal of 6.3 on the Richter scale, indicating a yield of over 100 kilotons. Shortly after that test, North Korea released an article titled "Kim Jong Un Gives Guidance to Nuclear Weaponization," which contained the following paragraph: "The H-bomb, the explosive power of which is adjustable from tens kiloton to hundreds kiloton, is a multifunctional thermonuclear nuke with great destructive power which can be detonated even at high altitudes for super-powerful EMP attack according to strategic goals." On September 4, 2017, Pyongyang published a technical report "The EMP Might of Nuclear Weapons" accurately describing what the Russians and Chinese call a Super-EMP nuclear weapon.

These warnings leave little room for wishful thinking by the U.S. leadership. [viii]

---

[i] https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg99931/html/CHRG-114hhrg99931.htm
[ii] https://www.gao.gov/products/GAO-16-243
[iii] https://www.federalregister.gov/documents/2017/12/28/2017-28083/cyber-security-incident-reporting-reliability-standards
[iv] https://www.hsgac.senate.gov/imo/media/doc/HSGAC%20Activities%20Report%202016.pdf
[v] https://docs.house.gov/meetings/HM/HM09/20171012/106467/HHRG-115-HM09-Wstate-PryP-20171012.pdf
[vi] https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf
[vii] https://www.federalregister.gov/documents/2018/04/20/2018-08336/developing-an-update-to-the-national-space-weather-strategy
[viii] http://www.firstempcommission.org/uploads/1/1/9/5/119571849/report_final_amended_emp_commission_chairmans_report_08222018.pdf