CYBER AND EMP PREPAREDNESS

An Open Letter To
The Honorable Anne Neuberger
Deputy National Security Advisor for Cyber and Emerging Technology

Dr. Peter Vincent Pry
Executive Director
EMP Task Force on National and Homeland Security
May 21, 2021

CYBER AND EMP PREPAREDNESS
An Open Letter To
The Honorable Anne Neuberger
Deputy National Security Advisor for Cyber and Emerging Technology

Dear Deputy National Security Advisor Neuberger:

Congratulations on your appointment as the President's White House "Cybersecurity Czar."

Condolences that your appointment coincides with a looming existential threat to our nation from Cyber Warfare. Russia's cyber-attack on the Colonial Pipeline, that provides 45% of petroleum needed by the eastern U.S. for civilian and military use, preceded by Russia's unprecedented SolarWinds cyber-attack on hundreds of federal departments and agencies, and thousands of industries and utilities, highlights U.S. vulnerability.

Just a few weeks ago, amidst concerns that Russia might invade Ukraine, Russia's state-owned media warned that a Russia-U.S. Cyber War targeting critical infrastructures is "inevitable." Russia threatens it can win a Cyber War decisively by attacking the U.S. electric grid. Russian TV described cyber-attack options ranging from small-scale to existential threats, including: blacking-out part of New York City (Harlem was mentioned), or blacking-out the state of Florida, or blacking-out the entire continental United States.[1]

Now Colonial Pipeline has been hacked, shutdown temporarily. Cyber-attacks can destroy pipelines, causing them to explode. Colonial Pipeline is crucial to fueling U.S. military power projection capabilities from the east coast to protect NATO, or to help Ukraine, during a Russian invasion.[2] That is why the Colonial Pipeline was really targeted, not for the millions paid in ransom, but as a demonstration of Russia's cyber-power.

The Colonial Pipeline cyber-attack proves Russia is not bluffing.

For 20 years or more, at least since President George W. Bush established the Department of Homeland Security, protecting U.S. electric grids and other critical infrastructures has been a high-priority of the federal government. Yet little has been accomplished. When the Texas electric grid fails catastrophically in an ice storm, when the California grid causes wildfires and rolling blackouts because it cannot cope with high winds, citizens and adversaries alike can see that U.S. utilities, negligent of simple precautions, cannot be trusted to prepare for sophisticated threats like Cyber Warfare and EMP. Not even the Colonial Pipeline is safe.

Our grand strategy for protecting critical infrastructures through "public-private partnerships" has failed because the U.S. Government has been content to be the junior partner. The private sector business culture is not a national security culture, nor do they have the technical competence, nor do they want responsibility for national security.

[1] "Russia: 'War Is Inevitable…Cyberwar'" Newsmax (April 19, 2021). "The Coming Electronic Apocalypse" Morning Nuke (May 15, 2021). "These Three Seemingly Unrelated Stories Prove 'Someone' Is Preparing For World War III" ANP (May 14, 2021).
[2] "When Will America Protect Itself Against EMP, Cyber and Ransomware Attacks?" The Hill (May 21, 2021).

National security is the constitutional, practical, and ultimate responsibility of the U.S. Government

The Colonial Pipeline and SolarWinds cyber-attacks are an opportunity for the White House to adopt a new grand strategy where the U.S. Government assumes its natural dominant role, now of necessity much more muscular and assertive, in protecting critical infrastructures vital to national security.

White House Leadership Needed on Cyber and EMP

The Congressional EMP Commission in 2017 recommended a White House "EMP Czar" to lead the functional equivalent of a Manhattan Project to quickly protect the nation from existential threats posed by solar and manmade electromagnetic pulse (EMP). The new White House "Cybersecurity Czar" should also serve as an "EMP Czar" since EMP attack is part of adversary planning for Cyber Warfare:

"Combined-arms cyber warfare, as described in the military doctrines of Russia, China, North Korea, and Iran, may use combinations of cyber-, sabotage-, and ultimately nuclear EMP-attack to impair the United States quickly and decisively by blacking-out large portions of its electric grid and other critical infrastructures…The synergism of such combined arms is described in the military doctrines of all these potential adversaries as the greatest revolution in military affairs in history—one which projects rendering obsolete many, if not all, traditional instruments of military power."--EMP Commission[3]

Protecting from Cyber-attack and EMP the national electric power grid must have highest priority. Electric power is the keystone critical infrastructure that energizes operations of communications, transportation, industry, finance, food, water and all other life-sustaining critical infrastructures. Threats to the national electric grid from EMP and Cyber Warfare are more imminent than climate change and imperil the existence of modern electronic civilization:

"A long-term outage owing to EMP could disable most critical supply chains, leaving the U.S. population living in conditions similar to centuries past, prior to the advent of electric power. In the 1800s, the U.S. population was less than 60 million, and those people had many skills and assets necessary for survival without today's infrastructure. An extended blackout today could result in the death of a large fraction of the American people through the effects of societal collapse, disease, and starvation."—EMP Commission[4]

Natural EMP from a solar superstorm, like recurrence of the 1859 Carrington Event, is inevitable, and could collapse electric grids and other life-sustaining critical infrastructures worldwide, putting at risk the lives of billions. NASA estimates the likelihood of another Carrington Event is 12% per decade.[5]

---

[3] EMP Commission, *Assessing the Threat from EMP Attack* (July 2017) p. 5. See also: General Vladimir Slipchenko, *Non-Contact Wars* (Moscow: 2000); Shen Weiguang, *World War, the Third World War—Total Information Warfare;* Army of the Islamic Republic of Iran, *Passive Defense: Approach to the Threat Center* (Tehran: Martyr Lt. General Sayad Shirazi Center for Education and Research, 2010).

[4] Ibid, p. 4.

[5] Dr. Tony Phillips, "Near Miss: The Solar Superstorm of July 2012" Science@NASA (July 23, 2014).

Fortunately, the existential threats from Cyber Warfare and EMP both have some common solutions that can be part of an "all hazards" strategy for protecting electric grids and other life-sustaining critical infrastructures.

The White House should immediately undertake the steps and strategies outlined below, some of which can advance national Cyber and EMP preparedness at virtually no cost to the U.S. Government, and all at relatively low-cost relative to the magnitude of the threats:

--The EMP Commission made over 100 recommendations to protect electric power grids and other critical infrastructures, including: telecommunications, transportation, petroleum and natural gas, emergency services, space systems, banking and finance, food and water infrastructures. Virtually all of these recommendations would improve resilience not only against EMP, but against all hazards, including against the worst cyber-attacks. The White House should send copies of the EMP Commission report *Critical National Infrastructures* to all relevant Senate and House committees, asking them to launch legislative initiatives implementing the EMP Commission recommendations for the sectors over which the committees have jurisdiction.[6]

--The EMP Commission warned that the U.S. Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) are deeply dysfunctional, hence the need for a White House "Czar" to lead national EMP and Cyber preparedness. U.S. FERC should be reformed by replacing existing commissioners with persons whose highest priority is not the fiduciary interests of electric utilities, but national security: especially protecting national power grids from Cyber and EMP.[7]

--Protecting the over 100 CONUS military bases and their supporting civilian electric grids would create "islands of survivability" that could facilitate a quick national recovery. Electric grid transformers, SCADAs, and other equipment hardened against EMP will also survive worst-case cyber-attacks that manipulate SCADAs to cause system-generated over-voltages (SGOVs). Cyber-induced SGOVs, like EMP, can overload and destroy critical equipment, cause cascading systemic collapse, resulting in protracted regional or nationwide blackout.

--Add a provision to the National Defense Authorization Act authorizing the Secretary of Defense to reprogram monies to help utilities protect from Cyber and EMP local and regional electric grids that support CONUS military bases. For example:

*"**Energy Security For Military Bases And Critical Defense Industries.** Whereas 99 percent of the electricity used by CONUS military bases is supplied by the national electric grid; whereas the Department of Defense (DOD) has testified to Congress that DOD cannot project power overseas or perform its homeland security mission without electric power from the national grid; whereas the Congressional EMP Commission warned that up to 9 of 10 Americans could die from starvation and societal collapse from a nationwide blackout lasting one year; therefore the Secretary of Defense is directed to urge governors, state legislators, public utility commissions of the 50 states, the North American Electric Reliability Corporation (NERC) and the utilities that*

[6] EMP Commission, *Critical National Infrastructures* (2008).
[7] EMP Commission, *Chairman's Report* (July 2017) pp. 39-42.

supply electricity to CONUS military bases and critical defense industries, to protect the electric grid from Cyber Warfare, including a high-altitude nuclear electromagnetic pulse (EMP) attack, from natural EMP generated by a solar super-storm and from other Cyber-EMP threats including radiofrequency weapons, and to help the States, NERC, public utilities commissions, and electric utilities by providing DOD expertise and other such support and resources as may be necessary to protect the national electric grid. The Secretary of Defense is authorized to spend up to $4 billion in FY2022 and every year thereafter to help protect the national electric grid."

--$2 trillion is planned for infrastructure modernization, including $100 billion for electric power. The EMP Commission estimates $2-4 billion could protect the electric bulk power system which, with smart planning, would enable rapid recovery from a nationwide blackout, saving the lives of millions.[8] $20 billion could very significantly advance protection of all critical infrastructures, making recovery from Cyber Warfare and EMP more assured and faster.

Education

Send a letter from the President and Secretary of Homeland Security to the 50 State Governors and 100 biggest electric utilities spotlighting Cyber/EMP as highest-priority threats. The letter should urge action to protect electric grids, and alone might even be sufficient to motivate States and utilities to protect their electric grids without Federal intervention. For the U.S. Government this could be the easiest and most cost-effective strategy:

--Appended to the letter should be supplementary materials providing in depth education on Cyber/EMP threats and technical guidance on how to protect electric grids, including: the EMP Commission Reports, the Cybersecurity and Infrastructure Security Agency (CISA) *EMP Protection and Resilience Guidelines for Critical Infrastructures and Equipment*, the Department of Energy (DOE) approved HEMP waveform, and the CenterPoint Energy briefing on protecting electric power substations.[9]

--The letter should include a list of defense contractors experienced in EMP protection. A chief impediment to national Cyber/EMP preparedness is that policymakers and utilities do not know how to protect against the threat. Let proven experts protect the civilian critical infrastructures.

--The letter should encourage electric utilities to share the Cyber/EMP educational materials with their employees, to have an educational program to raise situational awareness, to conduct exercises responding to Cyber/EMP events, and to solicit from employees "grassroots" ideas for

[8] EMP Commission, *Critical National Infrastructures* (2008) pp. 60-61.

[9] All the unclassified EMP Commission reports are located at www.firstempcommission.org. DHS and CISA, *Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure Equipment* (National Cybersecurity Integration Center: February 5, 2019) www.cisa.gov. Department of Energy, "Physical Characteristics of HEMP Waveform Benchmarks for Use in Assessing Susceptibilities of the Power Grid, Electrical Infrastructures, and Other Critical Infrastructure to HEMP Insults" (January 11, 2021) see also Dr. Peter Vincent Pry *Will America Be Protected?* Volumes I and II (EMP Task Force: March 2021) pp. 153-161. Eric Easton, "EMP Mitigation for Electric Substations" Briefing (CenterPoint Energy: November 11, 2020) see also *Will America Be Protected?* pp. 171-225.

preparing for a catastrophic Cyber/EMP event.[10] The best ideas do not always come from Washington.

--The Department of Homeland Security (DHS) should sponsor an aggressive public service messaging campaign encouraging electric utilities to protect themselves from Cyber/EMP, praising utilities like American Electric Power, CenterPoint Energy, and Duke Energy that are already taking action voluntarily.

Cyber/EMP National Manufacturing Standards

National manufacturing standards for equipment critical to electric grids, like transformers and SCADAs, should require such equipment to be designed and manufactured hardened against EMP and Cyber:

--Defense Department experience over 50 years manufacturing missiles, bombers, communications and other equipment that must survive EMP indicates that incorporating protection into the original design adds only 1-6% to system manufacturing costs.

--Lightning protection (equivalent to nuclear E2 EMP protection) is already routinely built-into most critical electric equipment as part of national manufacturing standards and best practices. So we as a society have, through manufacturing standards and best practices, already proven we can protect ourselves—at relatively low-cost and through a process that is so politically painless as to be unnoticeable—against the natural EMP threat from lightning. The same process can be used to protect against the threat from the "super-lighting" that is Cyber Warfare and EMP.

--The National Institute of Standards and Technology (NIST) could propose Cyber/EMP standards to electric utilities and manufacturers of transformers and SCADAs.

--NIST and DHS could sponsor a design competition. Offer an award and purchase of patents to those who invent the most cost-effective design for transformers, SCADAs and other equipment, incorporating Cyber/EMP protection in original designs, as well as for retroactive protection.[11]

--The Institute of Electrical and Electronic Engineers (IEEE) oversees the National Electrical Safety Code for equipment in the electrical bulk power system, including transformers and SCADAs.[12] Send the letter proposed above from the President to IEEE.

--The National Fire Protection Association (NFPA) oversees the National Electric Code for electricity consumers, including industries and homes, which is codified into law by the States.[13] Send the letter proposed above from the President to NFPA.

---

[10] For scenarios see EMP Commission, *Nuclear EMP Attack Scenarios and Combined-Arms Cyber Warfare* (July 2017).

[11] The Royal Academy of Science, in the 18th century, offered an award for a clock that could operate accurately at sea to determine longitude, resulting in the invention of the chronometer.

[12] "Standards" www.ieee.org.

[13] "National Electrical Code" www.cpsc.gov.

Critical Infrastructure Protection Act (CIPA)
CIPA requires the Department of Homeland Security to partner with utilities and the States in pilot projects demonstrating that electric grids and other critical infrastructures can be protected cost-effectively:

--Developing a plan to protect the electric grid of an entire State can be achieved very inexpensively, depending on the contractor, or even at no cost if the State Public Utilities Commission invites bids for developing Cyber/EMP protection of the State electric grid.

--The Louisiana Public Service Commission began a project to protect the Louisiana electric grid, received several free proposals, including a bid to develop a state-wide plan for $250,000. Unfortunately, the Louisiana EMP project terminated prematurely for political reasons. Perhaps the Louisiana EMP Project could be revived if encouraged by DHS.

--Several States have passed legislative initiatives or tried to move utilities to protect electric grids from EMP, including Arizona, California, Florida, Maine, Texas, Utah, and others, but been stymied by electric power industry lobbyists.[14] Federal political and material support could be the decisive factor reviving these efforts to achieve Cyber/EMP protection.

--Once a State has an Cyber/EMP protection plan describing necessary technical work and costs, especially when costs are found to be affordable, practical and political incentives to implement the plan will increase greatly.

--Once DHS has a pilot EMP protection plan for any State, it can serve as a blueprint for other States. The political and technical process of achieving national Cyber/EMP preparedness would be greatly simplified for States and utilities merely by invoking CIPA to get help from DHS.

Cyber/EMP Protected Nuclear Power Reactors
If the nation's 100 nuclear power reactors are protected from Cyber/EMP, it would eliminate the threat that they might "go Fukushima" and they would become instead "islands of survivability" for quickly recovering the national grid:

--Duke Energy's Lake Wylie Project is a pilot program for protecting a nuclear reactor so that it can survive and continue operating through an EMP.[15] This local "grassroots" project is receiving no help from Washington. Federal funding and technical support from the Nuclear Regular Commission and Department of Energy (DOE) should be provided to accelerate the Lake Wylie Project.

--Nuclear reactors are inherently robust against Cyber/EMP, except their current standard operating procedure in an emergency would be to power down and rely on vulnerable emergency power to cool the reactor while it is "turned off." The goal is to change operational procedures so

[14] Dr. Peter Vincent Pry, *Blackout Wars: State Initiatives to Achieve Preparedness Against an Electromagnetic Pulse (EMP) Catastrophe* (EMP Task Force: 2012).
[15] Ambassador Henry Cooper, "Lake Wylie Pilot Study: Marking Time!" High Frontier (October 5, 2020); "Lake Wylie Pilot Study Video" High Frontier (December 8, 2020); "Lake Wylie Study Status" (June 19, 2020).

nuclear reactors would continue to generate power through any emergency, so they do not become part of the "Black Start" problem but a big part of the solution.

--Small Modular Reactors (SMRs) are under development or ready for manufacture that are designed with EMP protection. SMRs on 100 CONUS military bases would prevent blackout of U.S. military capabilities, and could become "islands of survivability" for recovering the nation from Cyber Warfare and EMP.

--New generation SMRs are "green" as they produce no nuclear waste and have virtually no "carbon footprint" and so are also a potential solution to climate change.

Toward An Electrical Revolution

In the long-term, the United States needs a revolution in the way electricity is generated and distributed, moving toward greatly increased generating power and more decentralized distribution, to meet the energy demands of an increasingly electrified civilization, while better protecting that civilization from a solar or manmade "blackout apocalypse."[16]

The "big grid" that provides electric power to the United States is inherently vulnerable to Cyber/EMP because of its size and antiquity. Constructed haphazardly over the course of more than a century, the national power grid was never designed with national security in mind. Nor has electrical power generation kept pace with increasing demand, so the grid always operates on the verge of failure, another major factor in its vulnerability.

New technologies for generating electrical power and decentralizing distribution can supplement, and perhaps someday replace, the "big grid" to meet a future where nearly everything, including automobiles, may be electrically powered. Solar and wind generation are the focus of most political and financial support for a "green energy revolution" despite their significant technological limitations, costly inefficiency, and unreliability. Examples of some better alternatives include:

--Small Modular Reactors, as noted earlier, are a technological "great leap forward" from existing large nuclear reactors. SMRs are "greener" than wind and solar generation, while offering a much wider range of applications, being able to service a major city, a military base, or a small town. For example, the MicroNuclear "battery" is essentially a micro-nuclear reactor that can fit inside a large room, power a military base or town with 10 megawatts, and is designed protected against EMP.[17] Perhaps someday every city and town can have its own SMR, manage its own electrical power, making FERC and NERC and their often lethal regulatory mismanagement extinct.[18]

---

[16] See my books *Will America Be Protected?* (2021), *The Power And The Light* (2020), *EMP Manhattan Project* (2018), *Apocalypse Unknown* (2013), and *Blackout Wars* (2012) available from Amazon.com.

[17] MicroNuclear LLC "Nuclear Reactor Testing Device Opens Doors To Safe Energy In Idaho, Nation" https://www.uidaho.edu/news/news-articles/news-releases/2020-fall/111920-msnb.

[18] EMP Commission, *Chairman's Report* (July 2017) pp. 39-42. NERC is the North American Electric Reliability Corporation, essentially a lobby for the electric power industry and major impediment to national EMP/Cyber preparedness.

--Hydro-electricity is an underexploited resource, environmentally "green" and inherently one of the sources of electricity least vulnerable to Cyber/EMP, especially if distribution is decentralized into microgrids. 91,457 dams exist in the U.S. but only 3% (2,744) are harnessed for electricity.[19] New technology micro-hydropower turbines could harness some 80,000 dams, thousands of rivers and streams, previously unusable for electric power, making microgrids possible almost everywhere.[20] But DOE seems uninterested in helping small companies and inventors who, as in the past, are the source of most, and often the most revolutionary, technological innovations.

--Battery technology is a revolution awaiting invention. Battery-power would be the ultimate in decentralizing distribution of electricity, and would maximize civilizational resilience to Cyber/EMP threats. At least one small inventor has a prototype design that theoretically could power cars and individual households, making the "big grid" extinct. Again, DOE is uninterested.

The Biden Administration can make practical a "green energy revolution" through Small Modular Reactors and other innovations, and thereby kill with one stone three existential threats: Cyber Warfare, EMP, and Climate Change.

Dr. Peter Vincent Pry is Executive Director of the Task Force on National and Homeland Security, was Chief of Staff of the Congressional EMP Commission, and served on the staffs of the Congressional Strategic Posture Commission, the House Armed Services Committee, and the CIA. He is author of the books ***Will America Be Protected?*** *and* ***The Power And The Light*** (Amazon.com).

[19] U.S. Army Corps of Engineers, "National Inventory of Dams" (2018) https://nid.sec.usace.army.mil/ords/f?p=105:113:3839158335878::NO::: Department of Energy, "Types of Hydropower Plants" www.energy.gov.

[20] John Hull, Eagleaf Enterprises jhull95247@yahoo.com. For another innovation, wireless transmission of electricity from remote dams to the power grid, see www.emrod.energy.