Cohen, Dippell and Everist, P.C.

Before The
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Revitalization of the AM Radio Service	)	MB Docket No. 13-249

Comments
on Behalf of
COHEN, DIPPELL AND EVERIST, P.C.

The following comments are submitted on behalf of Cohen, Dippell and Everist, P.C. ("CDE") and is in response to the Further Notice of Proposed Rulemaking ("FNPRM") and Notice of Inquiry ("NOI") released by the Federal Communications Commission ("FCC") on October 23, 2015. CDE and its predecessors have practiced before the FCC for over 75 years in broadcast and telecommunications matters. The firm or its predecessors have been located in Washington, DC since 1937 and performed professional consulting engineering services to the communication industry.

The undersigned is licensed as a Professional Engineer in the District of Columbia and has been in continuous employment with this firm or its predecessors for over fifty (50) years.

He was the Chairman of the AM Broadcasting Service Working Group preparatory to the 1979 World Administrative Radio Conference and an Industrial delegate for the United States to the International Telecommunications Union Regional Administrative Medium Frequency Broadcasting Conference in Buenos Aires, Argentina. He, as the Chairman of TF:F Planning Methods; was a U.S. delegate of the Fourth Panel of Experts meeting in Geneva, Switzerland; was Chairman of the Working Group on Inventories, Incompatibilities, Negotiations and

Strategy to the Advisory Committee, all preparatory to the Second Session of the Regional Administrative MF Broadcasting Conference for Region 2 (Western Hemisphere) held in Rio de Janeiro. He was an industrial delegate for the United States to the Regional Administrative Radio-Conference (BC-R21) sponsored by the International Telecommunications Union in Geneva, Switzerland. All time was voluntary and all expenses were paid by the firm of Cohen, Dippell and Everist, P.C. CDE applauds the FCC for its continuing effort to revitalize the AM radio service.

Change Nighttime and Critical Hours Protection to Class A AM Stations

It is the opinion of this firm that Clear Channel Class A stations were created to serve large areas of the continental United States in an era immediately after World War One continuing through the Great Depression and World War II. In World War I, the Federal Government did not have the ability to reach and immediately communicate with the general public. Hence, this lack of immediate communication to the general public is one of the prime movers of developing the Clear Channel Class A stations. These Clear Channel Class A stations were distributed throughout the continental United States. With the protected daytime contour and with the normally protected 0.5 mV/m 50% skywave contour, the general population was assured with some radio reception and hence could be reached on a real-time basis in the event of an emergency. This ability to communicate with the general public includes periods with President Roosevelt's fireside chats, announcement concerning Pearl Harbor through Hurricanes Katrina and Sandy. Clear Channel Class A stations were vital off-the-air service during 9-11 and the Dericho. During the Dericho - Washington, DC area, Verizon service failed for many hours

(if not days). According to the statement by ranking member Frank Pallone, Jr., Congressman from New Jersey, indicated in a hearing that 40% of the New Jersey cell phone service was unavailable during Hurricane Sandy to the New Jersey general public.

The Clear Channel Class A service, whether groundwave or skywave service, is still available in times of absolute need. This need again will occur whether it's a terrorist or weather event and while many new communication avenues are now available none of these newly inaugurated social media systems, to our knowledge, can operate for extended periods of time under no public power conditions. It is almost certain that almost everyone has a battery operated radio.

There even could be an unimagined catastrophe such as power grid failure. See the attached articles which outlines the prospect of a major power outage throughout the continental United States.

Given the current terrorist climate or the recent North Korean pronouncement, the prospect of a massive communication/power outage is real and present.[1] The weather bureau implemented a new 1.2 billion dollar computer system but missed the recent forecast which resulted in cars being stranded on the Washington beltway for over 10 hours. The question arises how did these newly inaugurated so-called media systems assist the general Washington, D.C. commuters and other traveling public? If true, AM radio and in particular Class A stations,

[1]Testimony by the FCC Chairman Wheeler at the hearing before House Communications Subcommittee oversight on November 17, 2015 which provide details of 17 mysterious cuts to fibre links in and around the San Francisco bay, California area.

can fill the communications gap if such a major catastrophe was to occur whether man-made or weather related.

There are three very substantive articles which address the issue of wide-spread electrical grid and the assessment of the catastrophic events that may follow. Two of the three articles are attached. The third article could not be attached as a release from the copyright provisions could not be obtained from the *Wall Street Journal*.

The first is by Peter Vincent Pry, Executive Director of the Task Force on National and Homeland Security and served in the Congressional EMP Commission, the House Armed Services Committee, and the CIA, in an article in the *Washington Times* dated November 18, 2015. Portions of the attached have been extracted.

> "***Securing the electrical grid:*** *(in part)*
>
> *For example, the United States gives high priority to preventing proliferation of nuclear materials because terrorist armed with a nuclear weapon, detonated in New York or Washington, could kill several hundred thousand people – a spectacular asymmetric threat.*
>
> *However, the Department of Homeland Security has neglected to protect the United States from an even graver threat posed by the vulnerability of the national electric grid.*
>
> *America is an electronic civilization. Electricity sustains the economy and the lives of more than 300 million people. A terror attack that collapses the electric grid would black out all the life- sustaining critical infrastructures – communications, transportation, business and finance, food and water – in effect, hitting the "off-switch" for the entire nation.*
>
> *No less than two congressional commissions, the EMP Commission (2008) and the Strategic Posture Commission (2009), and numerous independent studies,*

including the recent books "Lights Out" and "Blackout Wars," warn that an attack on the grid that causes a protracted blackout could kill millions. It would be the ultimate asymmetric threat.

Terrorists armed with rifles could cause a protracted blackout of the North American electric grid. According to a study by the U.S. Federal Energy Regulatory Commission, a terror attack on just nine key transformer substations could black out the nation for 18 months.

Terrorists already know about and have exploited grid vulnerability in attacks on other nations."

The second article published by *The Wall Street Journal*, dated March 12, 2014 by Rebecca Smith is entitled,

*"**U.S. Risks National Blackout From Small-Scale Attack** (in part)*

The U.S. could suffer a coast-to-coast blackout if saboteurs knocked out just nine of the country's 55,000 electric-transmission substations on a scorching summer day, according to a previously unreported federal analysis.

The study by the Federal Energy Regulatory Commission concluded that coordinated attacks in each of the nation's three separate electric systems could cause the entire power network to collapse, people familiar with the research said.

A small number of the country's substations play an outsize role in keeping power flowing across large regions. The FERC analysis indicates that knocking out nine of those key substations could plunge the country into darkness for weeks, if not months.

"This would be an event of unprecedented proportions," said Ross Baldick, a professor of electrical engineering at the University of Texas at Austin.

No federal rules require utilities to protect vital substations except those at nuclear power plants. Regulators recently said they would consider imposing security standards.

FERC last year used software to model the electric system's performance under the stress of losing important substations. The substations use large power transformers to boost the voltage of electricity so it can move long distances and then to reduce the voltage to a usable level as the electricity nears homes and businesses.

The agency's so-called power-flow analysis found that different sets of nine big substations produced similar results. The Wall Street Journal isn't publishing the list of 30 critical substations studied by FERC. The commission declined to discuss the analysis or to release its contents.

The study's results have been known for months by people at the federal agencies, Congress and the White House, who were briefed by then-FERC Chairman Jon Wellinghoff and others at the commission. As reported by the Journal last month, Mr. Wellinghoff was concerned about a shooting attack on a California substation last April, which he said could be a dress rehearsal for additional assaults.

"There are probably less than 100 critical high voltage substations on our grid in this country that need to be protected from a physical attack," he said by email this week. "It is neither a monumental task, nor is it an inordinate sum of money that would be required to do so." Mr. Wellinghoff left FERC in November and is a partner at law firm Stoel Rives LLP in San Francisco.

The actual number of locations that would have to be knocked out to spawn a massive blackout would vary depending on available generation resources, energy demand, which is highest on hot days, and other factors, experts said. Because it is difficult to build new transmission routes, existing big substations are becoming more crucial to handling electricity.

In last April's attack at PG&E Corp's Metcalf substation, gunmen shot 17 large transformers over 19 minutes before fleeing in advance of police. The state grid operator was able to avoid any blackouts.

The Metcalf substation sits near a freeway outside San Jose, Calif. Some experts worry that substations farther from cities could face longer attacks because of their distance from police. Many sites aren't staffed and are protected by little more than chain-link fences and cameras."

The third article by U.S. Department of Defense dated December 15, 2015 entitled,

"DARPA Exploring Ways to Protect Nation's Electrical Grid from Cyber Attack (in part)

Across the United States, 3200 separate organizations own and operate electrical infrastructure. The widely dispersed nature of the nation's electrical grid and associated control systems has a number of advantages, including a reduced risk that any single accident or attack could create a widespread failure frm which it might take weeks to recover.

Since the late 1990's, however, cost pressures have driven the integration of conventional information technologies into these independent industrial control systems, resulting in a grid that is increasingly vulnerable to cyber-attack, either through direct connection to the Internet or via direct interfaces to utility IT systems.

Although utilities are increasingly focused on their cyber-defense needs, the process of identifying, purchasing and installing commercial host-defensive technologies across the industry may take many years."

Therefore, CDE does not object to the change to Clear Channel Class A normally protected contours, if and when, there is a full proof communications system that covers the entire United States and general population in the event of a major catastrophic event.

Change Nighttime RSS Calculation Methodology

This firm supports the return to the RSS calculation methodology used prior to the adoption of the current "Ratchet Rule".

Change Daytime Protection Ratio to Class B, C, and D Stations

This firm supports the return to the first-adjacent ratio of 0 dB used prior to the adoption of the current 6 dB D/U daytime protection ratio.

Change Daytime Protected Contours to Class B, C, and D Stations

This firm supports the change to the normally protected contour from 0.5 mV/m to 2 mV/m. It is recognized that there is a significant effort by industry to undertake a study to understand the nature of radiofrequency interference throughout the RF Spectrum. It was proposed to the Technological Advisory Council ("TAC") last Fall and was forwarded in the committee for future consideration. Last week, the TAC Meeting[2] (first meeting for 2016) adopted an item to make an assessment of noise in the RF Spectrum. Hopefully with the review and possible FCC corrective action, there will not be a future need to change the daytime normally protected contour.

[2]FCC Public Notice, released February 18, 2016, "FCC Announces Technological Advisory Council Meeting on March 9, 2016".

Revised Rule on Siting of FM Cross-Service Fill-in Translators

This firm supports the additional flexibility by allowing the 1 mV/m contour of FM translators from a radius centered at the AM transmitter site be no greater than the AM station's 2 mV/m contour or a 25-mile (40 km) radius.

Modify Partial Proof of Performance Rules

This firm supports the proposed modification of Section 73.154 of the FCC Rules with one exception that one radial be established that defines the major lobe as established in the recent referenced full proof-of-performance.

Require Surrender of Licenses By Dual Expanded Band/Standard Band Licenses

This firm supports the requirement that the 25 remaining dual-band stations surrender one of the two authorizations.

Main Studio

This firm supports retention of the current FCC Rule Section 73.1125.

Summary

CDE expresses its appreciation of the FCC's efforts to further assist the revitalization of the AM radio service.

Respectfully Submitted,

COHEN, DIPPELL AND EVERIST, P.C.

Donald G. Everist
President

DATE: March 21, 2016

Attachments

Securing the electrical grid

ISIS could kill millions by switching off America's power

By Peter Vincent Pry - - *Tuesday, November 17, 2015* – WASHINGTON TIMES (NOV. 18, 2015)

Three vitally important lessons are immediately apparent in the aftermath of the Paris terror attacks:

First, the Islamic State, or ISIS, is planning more attacks against Europe and also the United States. ISIS-affiliated websites threaten that Washington, London and Rome will be attacked next and that their preference is "to taste American blood."

Second, ISIS is adept at waging asymmetric warfare. Their goal is to leverage their limited resources and get the "biggest bang for the buck" by spectacular acts of terror that will psychologically demoralize the civilized world. The victims of Paris are not only the 129 killed and 352 injured, but millions worldwide who were witnesses through mass media.

Third, the combined intelligence resources of the United States and Europe, and police and security forces even when on heightened alert as they were in Paris, cannot prevent every act of spectacular terrorism. ISIS, al Qaeda or other terrorist groups will, sooner or later, achieve another surprise attack.

Therefore, one of the most important parts of U.S. counterterrorism strategy must be to anticipate and protect our nation's greatest vulnerabilities in order to defeat terrorism's strategy of asymmetric warfare.

For example, the United States gives high priority to preventing proliferation of nuclear materials because terrorists armed with a nuclear weapon, detonated in New York or Washington, could kill several hundred thousand people — a spectacular asymmetric threat.

However, the Department of Homeland Security has neglected to protect the United States from an even graver threat posed by the vulnerability of the national electric grid.

America is an electronic civilization. Electricity sustains the economy and the lives of more than 300 million people. A terror attack that collapses the electric grid would black out all the life-sustaining critical infrastructures — communications, transportation, business and finance, food and water — in effect, hitting the "off switch" for the entire nation.

No less than two congressional commissions, the EMP Commission (2008) and the Strategic Posture Commission (2009), and numerous independent studies, including the recent books "Lights Out" and "Blackout Wars," warn that an attack on the grid that causes a protracted blackout could kill millions. It would be the ultimate asymmetric threat.

Terrorists armed with rifles could cause a protracted blackout of the North American electric grid. According to a study by the U.S. Federal Energy Regulatory Commission, a terror attack on just nine key transformer substations could black out the nation for 18 months.

Terrorists already know about and have exploited grid vulnerability in attacks on other nations.

The Knights Templars drug cartel used explosives to temporarily black out Michoacan in Mexico, plunging 420,000 people into the dark so they could execute local leaders opposed to the drug trade on Oct. 27, 2013. Al Qaeda in the Arabian Peninsula temporarily blacked out the entire nation of Yemen, 16 cities and 27 million people, on June 9, 2014. Terrorists blacked out most of Pakistan — a nuclear weapons state — on Jan. 25.

Terrorists might be able to black out the grid with cyberattacks. Turkey experienced a highly disruptive temporary blackout, reportedly from an Iranian cyberattack, on March 31.

The worst threat to the grid would be from a high-altitude nuclear electromagnetic pulse (EMP), which would cause the most widespread and deepest damage to the critical infrastructures. The EMP Commission warned that terrorists armed with a single primitive nuclear weapon and short-range missile, or even a high-lift balloon, could inflict an EMP catastrophe.

North Korea apparently practiced a nuclear EMP attack in April 2013, orbiting its KSM-3 satellite on the optimum trajectory and altitude to evade U.S. national missile defenses and place an EMP field (if the satellite were a nuclear warhead) over the 48 contiguous United States. The KSM-3 still passes over the United States every few days.

The good news is that the grid can be protected against even the worst threat, nuclear EMP attack, for about $2 billion — and this would mitigate all the lesser threats, including from sabotage, cyberwarfare and severe weather.

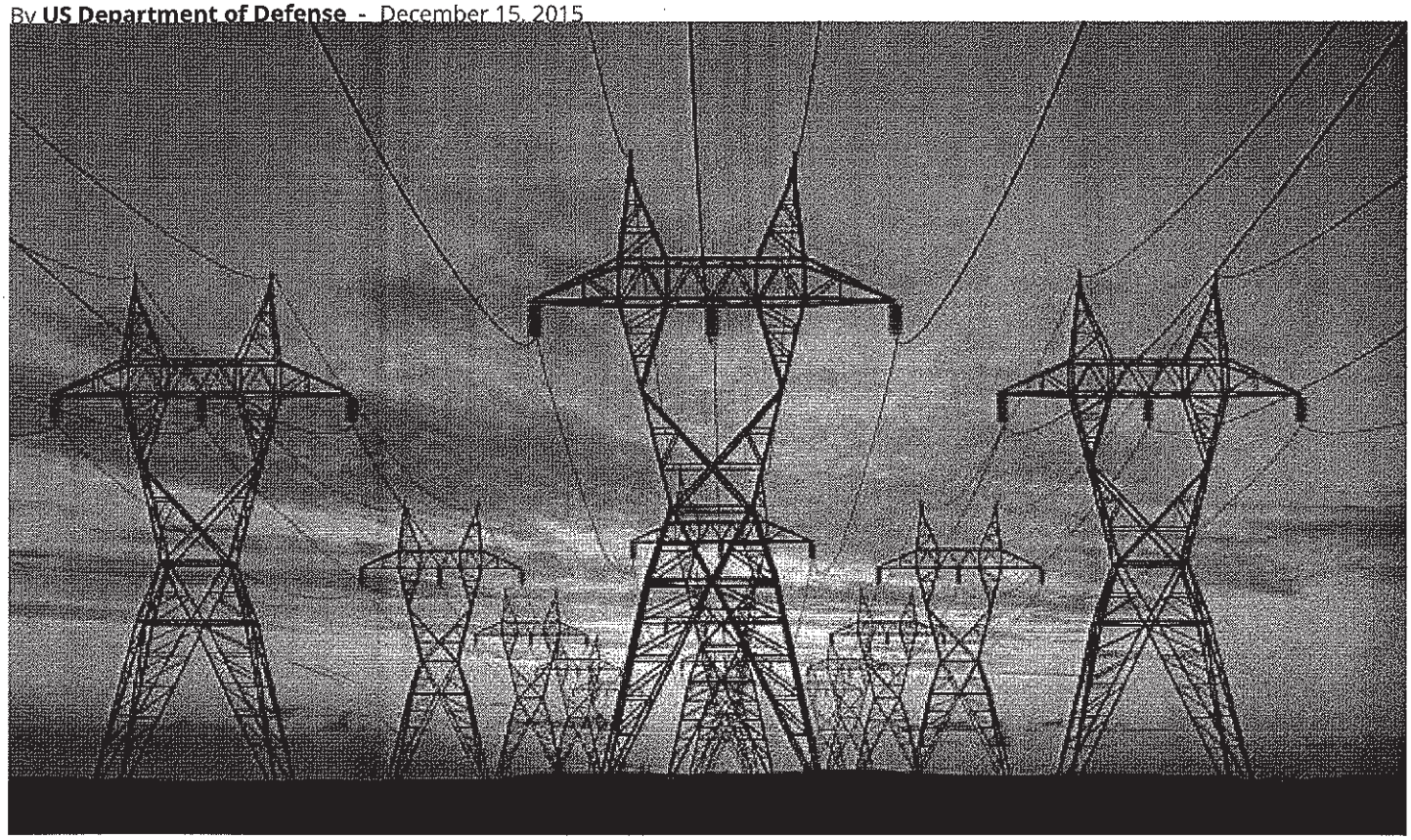
Awaiting passage in the House is the Critical Infrastructure Protection Act (H.R. 1073), a bill to protect the electric grid, sponsored by Republican Rep. Trent Franks of Arizona. Republican Sen. Ron Johnson of Wisconsin has introduced a similar bill (S. 1846).

In the aftermath of Paris, isn't it time to protect the grid?

• *Peter Vincent Pry is executive director of the Task Force on National and Homeland Security and served in the Congressional EMP Commission, the House Armed Services Committee, and the CIA.*

DARPA Exploring Ways to Protect Nation's Electrical Grid from Cyber Attack

By **US Department of Defense** - December 15, 2015



Across the United States, 3200 separate organizations own and operate electrical infrastructure. The widely dispersed nature of the nation's electrical grid and associated control systems has a number of advantages, including a reduced risk that any single accident or attack could create a widespread failure from which it might take weeks to recover.

Since the late 1990's, however, cost pressures have driven the integration of conventional information technologies into these independent industrial control systems, resulting in a grid that is increasingly vulnerable to cyber-attack, either through direct connection to the Internet or via direct interfaces to utility IT systems.

Although utilities are increasingly focused on their cyber-defense needs, the process of identifying, purchasing and installing commercial host-defensive technologies across the industry may take many years.

In an effort to address the cyber threat to the country's electrical grid within a shorter time frame, DARPA has released a Broad Agency Announcement (BAA) detailing research aims for the early detection of cyber-attacks to power-grid infrastructure and seeking ways to reduce the time required to restore power.

The ultimate goal of the program, known as Rapid Attack Detection, Isolation and Characterization Systems (RADICS), is to develop automated systems that would help cyber and utilities engineers restore power within seven days of an attack that overwhelms the recovery capabilities of power providers.

"If a well-coordinated cyberattack on the nation's power grid were to occur today, the time it would take to restore power would pose daunting national security challenges," said John Everett, DARPA program manager.

"Beyond the severe domestic impacts, including economic and human costs, prolonged disruption of the grid would hamper military mobilization and logistics, impairing the government's ability to project force or pursue solutions to international crises."

An early warning capability for power suppliers could prevent an attack entirely or blunt its effects, such as damage to equipment. But the vast scale of the nation's electrical infrastructure means that some number of systems are likely to be in an abnormal state at any given time, and it can be difficult to distinguish between routine outages and actual attacks.

RADICS looks to develop advanced anomaly-detection systems with high sensitivity and low false positive rates, based on analyses of the power grid's dynamics.

Recognizing that in some locations Internet infrastructure may not be operational after an attack, or that hackers may have embedded malicious code in utilities' IT systems during an attack, RADICS also calls for the design of a secure emergency network that could connect power suppliers in the critical period after an attack.

The creation of such a network will require new research into advanced security measures, as well as innovative technologies to facilitate the rapid connection of key organizations, without relying on advance coordination among them.

"Isolating affected utilities from the Internet would enable recovery efforts to proceed without adversary surveillance and interference," Everett said, "and providing an alternative means for online coordination would enable a more orderly restoration of power among affected organizations."

Finally, the RADICS BAA calls for the research and development of systems that can localize and characterize malicious software that has gained access to critical utility systems. These systems will augment the abilities of skilled cyber first responders to triage impacted systems and assist utility engineers with the rapid and safe recovery of power.