

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)
)
Carrier Current Systems, including) (ET Docket No. 03-104)
Broadband over Power Line Systems)
)
Amendment of Part 15 regarding new)
requirements and measurement) ET Docket No. 04-37
guidelines for Access Broadband over)
Power Line Systems)

COMMENTS ON NOTICE OF PROPOSED RULE MAKING

To The Commission:

Since the NPRM touts homeland security as a justification for putting up with negative aspects of BPL – – radio interference – –, and FEMA has deferred to the wisdom of the FCC to prevent harmful interference, and nobody more qualified than me seems to have addressed this particular issue, I thought I'd at least offer some public input based on a book from the public library that anybody can obtain: Cyber-threats, Information Warfare, and Critical Infrastructure Protection¹: Defending the U.S. Homeland, which since published in cooperation with the Center for Strategic and International Studies, Washington, D.C., it should have a degree of credibility. According to this book, it is not just physical attacks to the infrastructure that we should be concerned about.

While physical damage to the nation's infrastructure remains a problem, information systems can be attacked electronically from anywhere in the world, posing a new kind of threat to both the nation's critical infrastructure and the American homeland. ... U.S. military and defense officials involved ... in cyber-offense ... do not minimize the risk of cyber-attacks, but they feel they will have limited impact and that many if not most critical systems are isolated, difficult to identify and enter in concerted attacks, and can be reconstituted within an acceptable time frame and cost.²

¹ Anthony H. Cordesman with Justin G. Cordesman, Cyber-threats, Information Warfare, and Critical Infrastructure Protection (Westport, CT: Praeger, 2002)

² Ibid., p. 3.

That may be a rosy assessment as my supplemental material from FEMA will indicate, but I do note that isolation of a system can be an asset, and I suppose that a utility company using a BPL system to run its functions may have sacrificed some of that isolation in the process. Let's take an example which is also alluded to in the supplemental material from FEMA attached.

"Recreational " Hackers³

Virtually every day we see a report about "recreational hackers," or "crackers," who crack into networks for the thrill of the challenge or for bragging rights in the hacker community. ...

... A well-known example of this involved a juvenile who hacked into the NYNEX (now Bell Atlantic) telephone system that serviced the Worcester, Massachusetts area using his personal computer and modem. The hacker shut down telephone service to 600 customers in the local community. The resulting disruption affected all local police and fire 911 services as well as the ability of incoming aircraft to activate the runway lights at the Worcester airport. Telephone service was out at the airport tower for six hours. The U.S. Secret Service investigation of this case also brought to light vulnerability in 22,000 telephone switches nationwide that could be taken down with four keystrokes. ... This case demonstrated that an attack against our critical communications hubs can have cascading effects on several infrastructures. In this case, transportation, emergency services, and telecommunications were disrupted. It also showed that widespread disruption could be caused by a single person from his home computer.

I'm not trying to be a wet blanket or even pessimistic, but if it turned out that a fancy utility control system using BPL "could be taken down with four keystrokes," then I don't think we'd have improved homeland security at all. I would hope that would never happen, and all I'm trying to show is that fancier control & monitoring systems are not necessarily synonymous with better homeland security.

When I was growing up, my Dad sometimes took me to the telephone office where he worked and I could see the switchboard network of rows and rows of relays in stacks. Of course, I would hear stories of telephone vandalism from time to time, but nothing on the order of what happened in Worcester, Massachusetts. Yes, the system was primitive, but then some kid couldn't shut it down with four keystrokes from his home either.

I go over to my local electric utility company and I see an active display mounted on a wall showing their lines and where they go, with lights of various colors indicating their system's status at the various junctions. They do it without BPL. It has just the defense that's needed of being "isolated, difficult to identify and enter in concerted attacks, and can be reconstituted within an acceptable time frame and cost." Make it fancier on VDT's networked here and there, and the vulnerability is increased.

I think this perceived need for BPL-dependent control systems stems from "the

³ Ibid., p. 20.

common fallacy of equating sophistication of computer equipment with the sophistication of the decision or information system. A technologically complex computer system does not necessarily mean that a complex decision is supported. Technically sophisticated on-line systems are frequently dedicated to operational control applications."⁴ The operational control applications of running an electric utility are probably manageable with their low frequency control signals, and while BPL would be a more sophisticated approach to the task, what is actually accomplished is no more sophisticated.

Let's move on to:

Executive Order 13010⁵

The Clinton administration issued Executive Order 13010 on July 15, 1996. This order recognized that⁶

Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electric power systems, [etc.] Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats") and threats of electronic, radio frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber-threats"). Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation.

We've looked a bit at "computer-based attacks on the information or communications components that control critical infrastructures" which *could* under certain circumstances become more vulnerable with BPL, but there is at least one more cyber-threat, "radio frequency attacks" which EO 13010 also cautions against. Now, I know there have been numerous comments pointing out the susceptibility of BPL systems to transmissions from nearby transmitters in the same frequency bands, so I shall not repeat them. No, I want to look at something bigger:

TERRORISM RISK INSURANCE ACT OF 2002⁷

BUILDING VULNERABILITY ASSESSMENT SCREENING

Electromagnetic Pulse (EMP).

⁴ Henry C. Lucas Jr., assoc. prof. in the Grad. School of Business Administration, New York University, Why Information Systems Fail (New York: Columbia University Press, 1975) p. 9.

⁵ Cordesman & Cordesman, p. 56.

⁶<http://www.ciao.gov/PCCIP/eo13010.pdf> accessed June 20, 2000.

⁷ http://www.fema.gov/txt/fima/429/fema429_appendixes.txt

A sharp pulse of energy radiated instantaneously by a nuclear detonation which may affect or damage electronic components and equipment. EMP can also be generated in lesser intensity by non-nuclear means in specific frequency ranges to perform the same disruptive function.

According to the TERRORISM PLANNING COURSE TOOLKIT⁸

EMP/T Bomb

Electromagnetic Pulse Transformer Bomb. Operates similarly to a HERF Gun, but is many times more powerful and causes permanent damage. According to a 1980 FEMA report⁹, the following hardware would be most susceptible to failure from EMP:

- * Computers, computer power supplies, and transistorized power supplies.
- * Semiconductor components terminating long cable runs (especially between sites).
- * Alarm systems and intercom systems.
- * Life support system controls.
- * Telephone equipment.
- * Transistorized receivers, transmitters, and process control systems.
- * Power control systems.
- * Communications links.

Pay particular attention to "semiconductor components terminating long cable runs (especially between sites)" which is near the top of the list of "hardware most susceptible to failure from EMP." Both businesses and residences have umpteen semiconductor dependent devices connected to wall plugs which go to a power line out to a distribution transformer. Since the distribution transformer is a poor gateway for electromagnetic energy, it limits the susceptibility of all those devices to EMP. However, it is just that poor rf transfer that BPL would negate with high pass filters to get around those transformers connecting those lines at rf to the power grid. This makes for long cable runs between devices, just the ticket for EMP susceptibility.

The power control systems are also on the list making them susceptible to damage from EMP, especially when the lines are extended by BPL.

Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP) ... The Executive Order also established an Infrastructure Protection Task Force ("IPTF") within the Department of Justice ... The IPTF was to undertake an interim coordinating mission ... to:

- Provide training and education on methods of reducing vulnerabilities ... to critical infrastructures.

⁸ http://www.fema.gov/txt/onp/toolkit_app_d.txt

⁹ FEMA. EMP Threat and Protective Measures. Report for public distribution. April 1980, p. 11.

...¹⁰

We've already looked at a couple methods to reduce vulnerability: having an isolated (albeit primitive) control system hard to access, and not bypassing distribution transformers so as to keep cable runs shorter at rf frequencies. That brings us up to October, 1997 when:¹¹

The President's Commission on Critical Infrastructure Protection ... categorized the threats to national infrastructure as being both physical and cyber, but focused on cyber-threats because they were "new and not well understood." The report found that:

- The U.S. growing dependence on information systems to run critical infrastructures leaves the country more vulnerable to both physical and, more importantly, cyber-threats.
- ...
- There is a lack of awareness concerning the vulnerabilities faced
- ...
- Infrastructure assurance is a "shared responsibility" and calls for the adoption of infrastructure protection best practices ...

... The commission found that the growing role information systems played in the running of critical infrastructures leaves the U.S. with a growing list of vulnerabilities and threats. Added to this, the commission found this dependence could be more easily exploited with the growth and spread of computer technology.

Most importantly, the commission found that there "is a lack of awareness" on the part of both the public and government officials. ...

From these findings, the commission concluded that the government should adapt its thinking to the new rules of cyberspace, act now to protect from future threats, and come to the realization that infrastructure protection is a "shared responsibility" in which government and private industry share the burden for infrastructure protection.

... The review of laws concerning infrastructure protection was recommended in order for the law to catch up with the pace of technology.

Even without any threat of radio interference to licensed services (which we will get to), there remains a question of whether the old Part 15 rules are really made for BPL

¹⁰ Ibid., p. 57.

¹¹ Ibid., pp. 57-9.

which is more vulnerable to cyberthreats than some other means of sending data. By 1998 the interference potential of BPL enters the big picture.

Presidential Decision Directive-63 (PDD-63)¹²

Largely as a result of the PCCIP's recommendations on critical infrastructure protection, the Clinton Administration set forth a national "Policy on Critical Infrastructure Protection," also known as Presidential Decision Directive-63 (PDD-63) on May 22, 1998. PDD-63 defined critical infrastructures [to] include, but are not limited to, telecommunications, energy, [etc.] It recognized that increased automation of infrastructure is so dependent on information systems that critical infrastructure protection must be tied to information warfare.

The white paper the White House issued along with PDD-63 gave the following rationale for the new PDD:¹³

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, [etc.] ... As a result of advances in information technology and the necessity of improved efficiency, infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber-attacks. ...

No later than the year 2000, the U.S. shall have achieved an initial operating capability and not later than five years from the day the president signed Presidential Decision Directive 63 the U.S. shall have achieved and shall maintain the ability to protect our nation's critical infrastructures ... to ensure the general public health and safety ...; the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services. ...

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the U.S.

New Federal Guidelines¹⁴

¹² Ibid., pp. 59-60.

¹³ WHITE PAPER: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive-63, May 22, 1998, as quoted in Anthony H. Cordesman, Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland Published in cooperation with the Center for Strategic and International Studies. Washington, D.C. (Westport: Praeger Pub., 2002) pp. 60-61.

¹⁴ Cordesman & Cordesman, pp. 60-61.

The directive laid out the guidelines for the federal effort to address potential vulnerabilities.

...
Frequent assessments shall be made of our critical infrastructures' existing reliability, vulnerability, and threat environment because, as technology and the nature of the threats to our critical infrastructures will continue to change rapidly, so must our protective measures and responses be robustly adaptive.

The incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection; regulation will be used only in the face of a material failure of the market to protect the health, safety, or well being of the American people. In such cases, agencies shall identify and assess available alternatives to direct regulation, including ... providing information upon which choices can be made by the private sector.

...
Close cooperation and coordination with state and local governments and first responders is essential for a robust and flexible infrastructure protection program. All critical infrastructure protection plans and actions shall take into consideration the needs, activities and responsibilities of state and local governments and first responders.

This "close cooperation and coordination" rings a bell, as the NPRM states, "To the extent possible, we encourage potential BPL providers and BPL equipment manufacturers to work with amateurs and other existing licensed services to develop such appropriate mitigation requirements" (FCC 04-29, ¶ 42). Ham radio operators are often enough de facto first responders, as recognized by Congress—PUBLIC LAW 103-408—, and other agencies like FEMA (letter of Jan. 8, 2004) who are willing to follow the lead of how the FCC protects their interests. This is troubling because from the many comments of hams and BPL industry, we don't see very much an atmosphere of cooperation. Let's try to unite against terrorism by looking into the mindset of a terrorist.

The document was a part directive. Katukov removed his bonnet and then looked at each of us individually, while Dark Star stood in the shadows behind him. "This says, 'Our task is to create unbearable conditions for the German invaders, to disorganize their lines of communication, supply, and military units, to paralyze all their measures, to destroy the hoarders and collaborators—'" There Katukov looked at each of us with an excited expression on his face. "We must make the people fear us more than they fear the Fascist Bandits." He looked at Dark Star, who said, "Go on."

Katukov continued, "'—to destroy all collaborators, to spread the wide network of our Bolshevik organization in order to carry out all measures against the Fascist Occupiers.'"

After a silence Jan Bierzanek said, "We have only rifles."

Dark Star spoke. "Four guns in the hands of four good men may mean eight, twelve dead Germans. You will have your explosives and machine guns, but for now you must do what you can. . . ." ¹⁵

The terrorist wants to create mayhem in many ways, and at the top of his list, above disrupting their supply is to "disorganize their lines of communication." Sure, the terrorists would like to disrupt our electricity supply, but they would like it better if at the same time they could make it hard to communicate out of the stricken area, and that means somehow interfering with HF communication. If they had the wherewithal to connect a battery of low power broadband HF signal generators to the overhead powerlines across America when the power is out in a major city, do you think they wouldn't do it? Let's not do their work for them, and that means we need to cooperate: hams, government, BPL industry.

Using the above allegory, let's look at how each of the players perceives the potential harm to communications from BPL. Well, the BPL providers themselves are like the insurgents who are offered a truce if they turn in their weapons. They can't come up with any. No interference, potential or actual or in other countries. No weapons to turn in, not to speak of.

The FCC doesn't see how these insurgents pose much of a threat because all they've got is rifles. They can't destroy a whole army with just rifles. These are low level signals that can't go very far. A threat to be sure, but a minor one.

Then there's the hams who are going to be interfered with. The Germans who are getting shot at might look at it from a whole different angle. Four rifles in the hands of good shooters could easily mean eight to twelve dead Germans. Those small signals are going to be connected to good wire antennas; a little goes a long way.

The first ingredient in cooperation is the ability to see the other guy's viewpoint.

Okay, from the standpoint of the guidelines of PDD-63, "The incentives that the market provides are the first choice for addressing the problem." The first choice is to let the market decide. If BPL is not competitive with other means, then the problem is solved and nothing more needs to be done. We have our broadband Nirvana without the purgatory of interference to deal with.

Next, "regulation will be used only in the face of a material failure of the market to protect the health, safety, or well being of the American people." Under Part 15 as it now stands, "the health, safety, or well being of the American people" is not adequately protected from the interference from BPL, as it moves forward. "In such cases, agencies shall identify and assess available alternatives to direct regulation, including ... providing information upon which choices can be made by the private sector." Rather than banning BPL outright, you've proposed making information available in a database of BPL providers, where they are operating, which mode, and what frequencies. Based on this information they can select frequencies that do not interfere, or stop using frequencies causing interference, or as a last resort cease altogether.

That approach is consistent with PDD-63; we just need to enhance cooperation. Going back to the earlier allegory, the fault of the BPL providers is not being very forthcoming on owning up to interference. Even with a database, the information may not be

¹⁵ Ian MacMillan, Orbit of Darkness (San Diego: Harcourt Brace Jovanovich, Publishers, 1991) p. 70.

current, interference is hard to pinpoint, and BPL will have a harmonic and spurious content due to its harsh waveform and nonlinearities in junctions in the power lines. We need for them to produce more information to enable the amateur— —and other radio users— —to pinpoint interference. My suggestion is to let them identify their signals once an hour somehow using some form of tone modulated International Morse Code (MCW). That way, those rifles get laid on the table.

The hams are complaining about the reluctance of power companies to resolve their interference complaints, which doesn't bode well for having a less understood interference mode on those same power lines. They see themselves being ignored even more. I suggest, since BPL is highly software dependent, let each BPL provider have a hotline listed under the power company they use, where the ham identifying the signal can simply call in and enter the i.d. he copied on the touch tone pads of his phone and the BPL frequency agility will move their signal off that band, either that or terminate its use. Let the BPL companies program a different i.d. for each frequency band at midnight, and have the whole system reset itself then. Voilà, cooperation!

That brings us to your question, "We seek comment on the appropriate period of time that we should allow for BPL systems to come into compliance with any new requirements that we may adopt pursuant to this rule making proceeding"(FCC 04-29, ¶ 42). This necessary cooperation that should become part of the new rules should have already been in place: "No later than the year 2000, the U.S. shall have achieved an initial operating capability and not later than five years from the day the president signed Presidential Decision Directive 63 the U.S. shall have achieved and shall maintain the ability to protect our nation's critical infrastructures ... to ensure the general public health and safety ...; the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, ..." PDD-63 was signed on May 22, 1998. Five years after that would be May 22, 2003, which is right about the time your 03-104 came out. The time to establish necessary cooperation is over a year ago. To the degree the new changes to Part 15 incorporate this needed cooperation, these changes should go into effect immediately upon the change being made.

You state, "We further seek comment on whether Access BPL systems currently deployed should be required to be brought into compliance with the new rules, and if so, what period of time should be afforded for them to come into compliance" (FCC 04-29, ¶ 42). According to PDD-63, "Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the U.S." As I understand it, the test installations of BPL currently deployed are pretty much small fry, in geographically isolated places where interference from them would be brief, infrequent, manageable, and minimally detrimental to the radio spectrum users, in which case we shouldn't worry too much about it. If they want to get bigger and expand, sure, make them comply; otherwise let sleeping dogs lie.

Your assertion: "Given that there is significant investment in the deployment of the service, we agree with several commenters that Access BPL providers would have a strong incentive to exercise the utmost caution in installing their systems to avoid harmful interference and ensure uninterrupted service to their customers"(FCC 04-29, ¶ 39) is largely based on the premise that interference problems would be few and far between, in which case, sure they would somehow work around it to keep the service going. If interference

were so widespread that their only solution would be to cease operation, then they would have a strong incentive to ignore complaints or drag their feet. I think, therefore, that Part 15 radiation limits for such services need to be set at a lower, more reasonable threshold, so that there would be only those few complaints. See the Reply Comments of Leonard H. Anderson, 4/7/2004, pp. 11-12 for a more workable set of limits.

National Infrastructure Assurance Plan¹⁶

The principals committee was also tasked with creating a National Infrastructure Assurance Plan with milestones for accomplishing the following subordinate and related tasks.

- Research and Development: Federally sponsored research and development in support of infrastructure protection shall be coordinated ... to ... take into account private sector research, and ... minimize our vulnerabilities on a rapid but achievable timetable.

Your "research" as far as it goes on how to set radiation limits in Part 15 to protect first responders and their radio contacts from BPL interference is supposed to be "coordinated to take into account private sector research," but it seems to me you've lightly regarded ARRL's strenuous efforts to document the effects of BPL on the spectrum users. To "minimize our vulnerabilities on a rapid but achievable timetable," it would seem to me prudent to allow a bit of a time extension for comments on this proceeding in order to make use of NTIA's study about to come out.

Conclusions and Recommendations¹⁷

There is a disturbing gap between the military focus on asymmetric warfare and the civil focus on cyber-crime and cyberterrorism. There is a flood of uncertain and poorly defined data on the threat, much of which is anecdotal. Incidents tend to be exaggerated while the overall pattern in the threat may be understated or missed altogether. Cost and risk estimates are issued that are little more than guesstimates, often using dubious methods and data. There is a critical lack of technological net assessment of the trends in offense and defense, and of the relative capabilities of governments and the private sector.

There was a bunch of data from the commenters on 03-104 supporting BPL as an asset to homeland security, but we hear stuff all the time, and how reliable is it?

The U.S. should consider the following recommendations to for homeland defense:

- ¹⁸*The U.S. needs to determine what its real vulnerabilities are, and what action is needed to deter attacks, provide*

¹⁶ Cordesman & Cordesman, p. 67.

¹⁷ Cordesman & Cordesman, p. 167.

¹⁸ Ibid., p. 169.

defense, and to respond. Homeland defense does not consist of expanding the federal role in critical infrastructure protection at random—an effort that may well prove counterproductive by creating false priorities and promising capabilities the government cannot deliver. Homeland defense does, however, consist of clearly identifying critical vulnerabilities and taking well-focused and prudent federal action. At present, there seems to be little coherent vulnerability analysis, little prioritization, and little effort to distinguish what level of federal role is really involved.

It just seems to me you're sort of shooting from the hip in promoting BPL as a homeland security asset. It may open us up to more cyberterrorism, EMP is certainly a clearly defined vulnerability which I didn't see you consider, and cooperation with first responders is a big deal in national security which has been sadly lacking from BPL companies, at least in their comments.

- ¹⁹*The U.S. government should work closely with information system providers and manufacturers to assure adequate security features in new products.* Review is needed to better ensure that information system providers can be persuaded to give proper weight to protection, prevention, mitigation, and reconstruction capabilities. At present, market forces tend to emphasize speed of change, features, and open access rather than the provision of adequate protection.

It seems to me that as a government entity you need to "give proper weight to protection, prevention, [and] mitigation" of interference rather than be overawed by BPL demonstrations that "emphasize speed of change, features, and open access."

- ²⁰*Equally important, state and local governments and all elements of the private sector—business, utilities, and NGO's—need to explicitly assume responsibility for the vulnerability of their systems and activities, the ability to ... provide alternative back up systems.*

So here's the thing. BPL control of utility lines is vulnerable on several levels. Even should a utility company employ it, they would need to have at least one alternate system to do the job as well. That alternate could probably do the job in the first place.

This may seem to be a daunting list of requirements, and related issues and complications. The fact is, however, that the U.S.—like other nations—has little choice. It must learn to cope with the impact of fundamental changes in technology, information systems, communications, government operations, and the global economy. Given the pace of change, both the threat and the U.S. reaction will be in an almost

¹⁹ Ibid., p. 177.

²⁰ Ibid., p. 178.

constant state of evolution, and "business as usual" is simply an impossible alternative.

The key to success may ultimately be for the U.S. government to focus on only those threats that truly threaten the nation.²¹

I do think that for BPL, "'business as usual' [with current Part 15 rules] is simply an impossible alternative." Part 15 needs to be changed to reflect the sheer scope of intended BPL deployment, that it will seem to be everywhere on all frequencies on all wires.

I don't think that running the power grid through BPL is where our focus should be for national security. If it ain't broke, don't fix it. That could cause more problems than it solves.

There's even a precedent where the safer d.c. power was replaced by 60 cycle a.c. which is better suited to a power grid than d.c., although a.c. is more dangerous to people. "Electrocution from low-voltage current is common in the home. The danger in the home is often underestimated."²² We've traded off home safety for the extreme utility of a.c. If we find that the power grid isn't really very suitable for carrying HF to low VHF, then I don't think some nebulous cause of homeland security should be used to justify proceeding with it.

Respectfully Submitted,
Earl S. Gosnell III

²¹ Ibid.

²² Advanced First Aid and Emergency Treatment (Washington D.C.: American Red Cross, 2nd ed., 1979) p. 300.