PHYSICAL SECURITY FOR ELECTRIC POWER SYSTEMS--A DRAFT
By Ed Badolato, President, CMS, Inc.
September 27, 2001

Abstract: ***This paper explores the ability of electric power systems to provide essential services during various types of emergencies from the perspective of the physical threat. (Terrorist threats to the IT systems of the US electric power industry will be contained in the companion paper--Electric Power and Cyber Terrorism). This effort traces the history of dealing with threats to electric power systems back to the WWII/Korean War period and outlines how the US has approached the problem. It describes the various potential threats and vulnerabilities to an electric power system with specific discussions of its five basic elements: generation; bulk transmission; distribution; the load (users); and system controls. It discusses the importance of protecting system choke points and the consequences of emergencies at choke points. It provides a phased program for developing a damage mitigation program, and a set of preparedness measures designed to strengthen electric power security and reliability. It recommends the need for Government-Industry cooperation at the local and regional levels.***

BACKGROUND:

Soon after WWII, a panel of war experienced electric power system engineers began a generic vulnerability analysis of domestic systems. Their findings were published in 1950, titled, "Protection of Electric Service from Sabotage and Enemy Action." They directed their attention to, "...the problems which may be met in protecting the present high degree of continuity of electric service from disruption due not only to attacks which may occur after hostilities have been declared, but also resulting from subversive efforts to interfere with this continuity long before war is declared." Their findings and recommendations, some of which are extracted here, are valid today:

> "It is realistic to assume that efforts are now being made to obtain information and formulate plans for disrupting our industrial effort."
>
> "Each location should be studied with regard to its relation to continued war effort to determine probability of attack."
>
> "A good rule is to choose essentials which require a long time to repair or replace. Examples . . operating personnel, turbine generators, large transformers, load dispatching facilities, vital records, maps, and drawings."
>
> "Threats to continuity of service would arise from espionage and sabotage from with~ or without."
>
> "Sabotage is a very convenient tool for delaying (industrial) production... such acts may readily come from agents already within this country."
>
> "The concerted attack would probably come without previous warning similar to that

of the Japanese on Pearl Harbor.""Full coordination of planning activities with local, state, federal and military authorities, and adjoining electric utilities must be accomplished."

In May, 1981, the Comptroller General, in a report to the Congress, stated, "Federal Electrical Emergency Preparedness Is Inadequate." Again in Sep, 1982, he advised the Congress, "The Federal Government Is Still Not Adequately Prepared To Respond To Major Electrical Emergencies."

In Dec, 1982, United States Senators Percy, Tower, Cohen, Thurmond and Denton, signed a joint letter addressed to William Clark, then Assistant to the President for National Security Affairs. They stated:

> "Recent events…have raised concern about the vulnerability of the civilian society to sophisticated terrorist attacks. There is a reasonable likelihood that these attacks will become more frequent and serious in the years ahead.
>
> It is time we directed some of our ablest military and civilian planners to the task of identifying potential problem areas and pursuing remedies in these problem areas. Expertise needs to be tapped to look into a broad range of potential terrorist targets---energy, water, communications, transportation, food, and public health, for example.
>
> "We had considered introducing a Senate resolution requiring study of this issue, but we believe the effort should proceed without a public spotlight. Therefore, we are communicating our concern by letter and asking you to undertake the following:
>
> (1) Identify the most strategically important potential civilian targets for terrorism in the United States;
>
> (2) Project what might be the resulting short-term and long-term consequences to the U.S. economy of a successful attack at each potential target;
>
> (3) Identify what form a terrorist attack on each might take, and what our capacity is to repel it or limit the damage it could cause; and,
>
> (4) Identify steps which could be taken at each potential target to reduce
>
> (a) the risk of attack,
> (b) the consequences to U.S. society such an attack might cause, or
> (c) the time and resources required to repair, replace, or bypass any damage."

Sound familiar? For over 40 years the US government has been involved in a series of analysis and studies on energy emergencies, *but the fact remains that our vital electric power systems are just as vulnerable to attack today as they were in 1950*.

However, today, there is an important difference. Currently, our nation generates and uses as much electricity as Russia, Japan, West Germany, Canada, and the United Kingdom combined. Our society, basic infrastructure, and the new digital age is more dependent on electricity than any other industrialized nation. While all forms of energy are vital, electric power is the fundamental energy which undergirds our modern nation and national well being.

THREAT

Strategic attacks against energy systems can come principally from two different, but frequently linked, quarters. In general, vital electric power systems are completely unprepared to cope with multiple attacks from either quarter.

1) Rogue States have the means to interrupt electric power delivery to essential U.S. assets either by: a) coordinated acts of sabotage; b) by nuclear detonations to generate Electromagnetic Pulse (EMP); c) by employment of conventional weapons, or d) by strategic nuclear strikes. Currently, intelligence estimates indicate that until certain Rogue States have an intercontinental nuclear delivery system, their main threat will be conventional weapons/explosive attacks or sabotage.

2) International Terrorists are capable of conducting significant sabotage attacks against these power systems, either on their own volition or as surrogates.

The threat of coordinated malevolent acts either by domestic "home grown" terrorists, or by international terrorists, is a reality. By destroying relatively few critical nodes on the electric power systems which supply our key defense and infrastructure assets, the stability of the population, the economy, and the security of the nation can be placed in jeopardy.

VULNERABILITY

Electric power systems are susceptible to attack with little risk to the attacker, a fact well recognized by saboteurs and military tacticians. Detailed maps of power systems are readily available in the public domain and on the internet. Selecting points for attack and estimating the consequences is relatively simple. Upgrades in commercial satellite data can be used to readily update and confirm system map information for potential attackers.

Electric systems are of strategic value to power their infrastructure and national defense assets. In most countries of the developed world, electric systems have become so reliable over the past half century, that this form of energy is now taken for granted--like the air we breathe, electrical energy is always there.

National security planners have been slow to learn the fact that electricity must be manufactured and delivered, through highly complex technological systems, at the instant of demand. The systems are constructed and operated to withstand the stresses imposed upon them by nature and by equipment failure. Storm and earthquake problems are usually confined to limited areas. Restoration of service is accomplished in a relatively short time, resulting in mostly minor inconvenience to the customers being served. Most utilities are well prepared to handle a single contingency outage. They are not capable of reliable performance however, when their major components are severely damaged on a widespread basis by deliberately planned acts of man. Virtually none are equipped or staffed to mitigate the consequences of multiple attacks against major components.

To better understand the points of vulnerability, a brief description of system components and function will be useful followed by a brief look at repair and restoration capability. Electric systems consist of five basic elements: generation; bulk transmission; distribution; the load (users); and, a means of system control.

1. Generation: The power for generation is derived mainly from oil, natural gas, coal, and nuclear, each of which heat water into steam which is pressure-fed into a turbine causing it to spin a generator which produces electric energy. Hydroelectric dams impound water, direct it by gravity flow to spin turbines coupled to generator units, which produce the electricity. Generator units are installed within a power house which is usually unguarded. Except for nuclear power plants, site access and security measures are easily circumvented.

2. Bulk Transmission: Electrical energy is fed from the generators through custom built step-up transformers located near the power house, onto extra high voltage (EHV) transmission lines (the "freeways" of electricity) which convey it usually over long distances, to custom built step-down transformers where the voltage is reduced to match those of the distribution system. These transformers and related equipment are located in a substation, normally sited on the surface of the earth. These bulk transmission substations are enclosed within a simple chain link fence, installed primarily as a safety measure to prevent humans and livestock from coming into contact with the hazardous electrical equipment in the substation. Access is easily gained by cutting the fence fabric. It has not been necessary to employ guards at these facilities even though they are usually situated in remote locations. All transmission towers and lines are open to attack at any point. They are not considered lucrative targets however, since lines can soon be restored on temporary structures. Bulk transmission facilities are becoming more redundant.

3. Distribution: From the bulk transmission substation a network of lower voltage transmission lines and substations (similar to streets and roads of various sizes radiating from a freeway interchange) carry the power to all the users "downstream" from the bulk transmission system. Most of these facilities are above ground, with some segments below the surface. Their components are much smaller than on the bulk systems and spare parts are generally in greater supply. Storms take an annual toll on distribution

networks. The utilities are prepared for such emergencies and often pool their resources to aid each other in restoring service. Targeting of distribution system components can cause troublesome outages but the magnitude of the problems will usually be more manageable than attacks on the "upstream" bulk systems or the generation stations. Guarding of distribution system components is not done routinely.

4. The Load: From heavy industries to households, the entire societal infrastructure is dependent in varying degrees upon the reliable function of these electrical systems. Then user demand fluctuates, as it does moment-by-moment, generation must be inc~eased or decreased to keep all elements of the system and the load in precise balance. In northern areas where heating units, controlled by thermostats, are switched on by a sudden temperature drop, demand on the system will rise dramatically. In summer, air conditioning and irrigation pumping place an entirely different set of demands upon the system. While some users, for example key defense industries, post security guards and patrols to protect their plants, the electric systems upon which those plants depend for critical energy requirements go unguarded.

5. System Control Center(s): Major electrical systems rely heavily on their primary system control center where highly trained dispatchers and operations engineers manipulate the system to satisfy the varying needs of both the system and the load. As indicated earlier, all components must be kept in operational harmony. Computers, telemetry, radio, and dedicated telephone lines, continually monitor major system elements and transmit vital information to the control center. Immediate action, either by computer or manually, is taken to protect the system and serve load demands. When routine faults occur the system is designed to take certain remedial measures instantly close to the point of fault, and automatically report these conditions to the control center staff. Major faults often require quick decisions and reaction on the part of the staff to prevent widespread havoc.

   At times it is appropriate to isolate segments of the system by shutting it down to prevent "cascading" of the problem to other parts of the effected system or to those which are interconnected with it. System Control Centers are often protected by contract guards of varying capability. They do not present a significant deterrent to a determined attacker.

REPAIR AND RESTORATION:

In assessing vulnerability, repair and restoration capabilities must also be considered. Electric utility systems have an outstanding record of reliability due to their maintenance policies and ability to restore or bypass common outages quickly. The pooling of equipment and manpower contributes greatly to this record. Experience has proven that a manageable vulnerability-risk is acceptable on any power system. The degree of risk is balanced against past ability to repair equipment and restore service in an acceptable length of time. Repair personnel and equipment inventories are maintained to meet historic requirements.

Should widespread damage be caused on many systems by deliberate acts of man (e.g. war or sabotage), managers would be hard pressed to rapidly restore service. Following an HEMP* event, for example, system components which appeared serviceable immediately upon re-energization can be expected to fail at a sporadic and unpredictable rate, due to minute flaws caused by the EDP generated effects. Replacing miles of insulators would be time consuming, and this assumes that replacements are available.

[* HEMP = High Altitude Electromagnetic Pulse, generated by a nuclear burst about 300km above Earth. Detrimental to power and communications systems.]

Should coordinated sabotage of major components occur, replacement of damaged equipment could take many months or years. For example, major transformer banks require at least 16 months to construct under ideal conditions. Transporting, installing, and testing them would take another several weeks. The availability of special transportation equipment itself could pose serious delays. Utilities neither have enough skilled personnel nor equipment at their command. Further, the skills required to safely repair this kind of electrical equipment are not to be found just anywhere. Several years are invested in developing journeymen.

It has taken many years to engineer and build these systems in peacetime. It can be predicted that widespread damage will require many years of highly skilled effort to reconstruct them, assuming that the United States has the capability to manufacture or acquire the requisite components. At this time, due to regulatory, economic, and other constraints, the strategic electric power systems of the nation are, from a national security viewpoint, critically short of vital major spare components. Further, our domestic ability to manufacture these components has eroded and moved offshore over the past twenty years. In the next decade major systems, now stressed beyond prudent design limits, may begin to fail. This will further place our national security and our essential infrastructure into jeopardy.

TYPES OF CHOKE POINTS:

Overall vulnerability must include an identification of the types of choke points lucrative to the attacker. Power systems principally have four: 1) generators; 2) step-up transformers; 3) bulk transmission step-down transformers; and, 4) the system control center. While damage to other components can certainly cause great harm and moderate-term disabling of system elements, identifying the four above as lucrative targets, in the sense of producing long-term and widespread consequences, is realistic.

Generic Vulnerability Assessment of Choke Points:

Lucrative Choke Points are easily located either on the ground or from system maps. They can be damaged or destroyed by a number of means. Some government energy experts have advised the author not to describe these vulnerabilities, but the techniques are already

very well known to international terrorists, surrogate agents, and to special operations military forces. From simple pipe bombs, shaped and platter charges, to stand-off rifle and rocket attacks, choke points on the electric systems of the modern world are completely vulnerable.

1. Failure of equipment at each type of choke point can be caused by short-circuiting or by causing mechanical failure, employing any of the following means:

a. Generators: Sand in the bearings; removal of oil; shaft misalignment; short-circuit of windings; explosive blast; a wrench dropped into a maintenance port; denial of start/re-start power. EDP can also cause significant failures.

b. Bulk Transmission: Step-up and step-down transformers, and circuit breakers can be attacked with any device which will penetrate the 5/8-3/4 inch mild steel tank and short circuit the windings or destroy internal equipment. Such an attack will usually require complete replacement. EDP can also cause significant failures which are difficult to quantify at this time due to insufficient research. A more knowledgeable attacker can target other equipment causing system failure. Major transformers and circuit breakers however, are easily identified by non-technical personnel, spares are seldom on hand and, lead time to manufacture is over a year.

c. Distribution: Attacks on components can be accomplished by small arms fire, a length of chain tossed onto buss works, or by use of greater force. While such attacks can cut power to specific loads, it would require a greater number of attacks to measurably effect an entire cluster of targets. Here again, EDP can cause significant damage.

d. The Load: Destruction of selected loads requires site specific targeting. For example, bombardment of a ball bearing plant could impair its ability to produce those components vital to the function of other machinery. By simply attacking the bulk electrical transmission system choke points, power can be denied not only to the ball bearing plant but also to other key national security assets "downstream" of the choke points.

e. System Control Center(s): Highly qualified and experienced system operations personnel are clustered, together with highly technical control and communications equipment, at these centers. Any attack which would destroy such a center would significantly impair the operation or restoration of a system by eliminating vital command, control, and communications(C3) functions and capabilities. Some system segments could be manually controlled from individual sites. However, personnel skilled in such operations are dwindling in number as a result of automated control installation. EDP would also cause significant long-term damage to

these C3 centers and the remote microwave facilities they depend upon.

2. Ease of Attack, by Choke Point Category:

    a. Generation: Generating systems are easier to defend with local security forces once such forces are emplaced and trained. Currently, sufficient forces and the supporting contingency plans to back up local security are lacking on most systems, except at nuclear power plants. Defense against the insider threat is nil, except at nuclear plants. Step-up transformers are fairly easy to target since they are located outside the power house. However, they can be included within the local security envelope for the entire plant once it is put in place. However, they can easily be hit by insiders, with slightly more difficulty for an outsider.

    b. Bulk Transmission Substations: These stations present the most accessible targets for the attacker. They are often sited in remote areas, can be entered in 7 seconds by cutting the chain link fence and, contain the major long-lead time EHV transformer banks and circuit breakers. They should be classed as top priority choke points since they present the least risk and most lucrative target on the entire electrical system to the attacker. They are of equal value to the insider and the outsider.

    c. System Control Center(s): If only these centers are targeted the system can still be operated from other locations, as indicated earlier. Command, Control and Communications (C3) is significantly degraded, however. Such centers can easily be sabotaged by insiders either to effect C3 loss or to support a broader system attack by outsiders. Many utilities provide nominal local security for these centers which can easily be overcome. They should be classed as high priority choke points.

    d. Key Personnel: Hostage taking usually places the attacker at greater risk than the mere destruction of facilities or equipment. However, it should not be overlooked by security planners as a tactic historically employed when coercive control is desired. Contingency plans and prior briefings of key personnel have proven effective in these situations and should be considered.

    e. Major Materiel Yards: Central supply points, and sites where major repair vehicles and EHV spare components are stored, present valuable targets. While of lower priority, security plans should include these sites.

CONSEQUENCES:

Since our modern society is almost totally dependent upon electrical systems, the wide spread loss of choke points on systems which serve clusters of key defense and infrastructure assets and major metropolitan areas would have the most detrimental effect.

The loss of non-cluster-serving choke points, however, should be weighed against the value of specific "downstream" loads being served and must not be overlooked.

Pumping of potable and irrigation water, sewage treatment, food storage refrigeration, banking, communications, refineries, shipping, transportation, commerce, and home/commercial life support systems (heating, ventilation, and air conditioning), all depend on the continued energy throughput of system choke points. Should they cease to function for an unacceptable length of time, the consequences to national security, public health and safety, and the economy, would be huge. A 25 hour snapshot" of actual consequences occurred in 1977 when New York City was blacked out due to lightning strikes. It may illustrate the kind of problems to be expected.

GOVERNMENT

The Federal government is deeply concerned about the existing condition of domestic electric power system vulnerability from an overall national security viewpoint, primarily due to the threat posed by international terrorists. The White House has provided briefings to industry of its concern. The Department of Energy has been desirous of initiating a relationship with industry. Efforts to integrate national security into electrical system reliability has been discussed, and industry has looked at its ability to weave low cost security measures that would strengthen bulk power supply systems, particularly those which serve key national defense or infrastructure assets.

Various organizations and agencies involved in Homeland Defense have been in the process of identifying all Key Assets which the nation must rely on in time of national emergency. An objective is to develop plans designed to assure Key Asset protection and continued functioning. Planners must realize that no matter how well protection plans for Key Assets perform when the day of emergency arrives, all of those Assets are electric energy dependent.

They must also recognize that the electric power systems require protection at certain locations. At this time, however, there is little national consensus for which choke points require what level of protection. With cooperation from the power industry, the Homeland Defense effort can assist in the development of plans to protect utility choke points which have probably been targeted as lucrative targets by a potential aggressor.

MITIGATION

The United States must be committed, as a matter of national policy, to ensure the protection and reliability of those electric power systems upon which its domestic infrastructure and national security depend. Industry has made the investment in facilities, has the technical knowledge and skills, holds the franchise, and has a proven record of providing reliable service to all of its customers, on demand. Industry has met the reliability challenge under historic conditions of stress without government regulatory

involvement. So it should remain.

A new dimension of "national security reliability" should be used in the planning for reliability. New protocols should be developed and adopted to provide preparedness and mitigation measures designed to meet the current terrorist threat. No entity is better qualified or staffed to address these issues than the electric power utilities. Industry must retain its independence from government and yet serve the broader national security reliability requirements which are identified by those in government charged with national security emergency preparedness.

PHASE I:

A single point of contact ("Interface") organization, qualified to receive highly classified Government documents, should be employed by industry to receive the classified list of "defense and infrastructure key assets" which are identified and prioritized by the respective Federal agencies. lnterface could group the Key Assets by geographic cluster and work directly with the respective Key Electric Power System (KEPS) which serves each cluster.

PHASE II:

A Government-Industry coordination team, in conjunction with input from each KEPS, could perform a confidential analysis to locate vital choke points on that system. This team would then prepare confidential contingency plans for the protection of choke points and nominate each vital choke point to the Homeland Defense staff. The Homeland Defense staff could then coordinate the protection plans with the utility, local law enforcement, and State and Federal military commands.

PHASE III:

Government-Industry coordination could provide a two-way communication link. This communication would allow KEPS Dispatchers to alert the National Command Authority (NCA), The Homeland Defense staff, and DOE to Aberrant National Security Events (ANSE) when detected on their system. This information would immediately be collated and used to initiate pre-agreed action. Government-Industry coordination would also allow the NCA to communicate ANSE to a range of KEPS Dispatchers as a warning of potential multi site attacks.

PHASE IV:

a) A coordinating Government-Industry group could collect, collate, and maintain, on behalf of each KEPS, an inventory of all spare EHV components and handling equipment owned by any electric power entity (to include contractors) in North

America.

b) The interface could act as the central clearinghouse regarding availability of spares, equipment, and journeyman skill requirements.

c) Interface could also manage any Strategic Utility Equipment Inventory (SURE) which is established to support the new levels of electric power system National Security Emergency Preparedness. [This could well be a pool of spares cooperatively owned by 3d party investors or by the KEPS themselves. There has already been discussions about storing the SURE items (when and if established) on military bases near KEPS for safeguarding. Also, these components could, by agreement, be used as construction or maintenance spares.

SUMMARY

The threat to our electric power system is real. Yet, the government does not have the limitless resources to address a total solution for this problem. Our electric power systems are vulnerable targets, yet they must be relied upon more than ever in a national emergency. Industry is already committed to its long standing agenda of energy reliability and it can be of assistance, but cannot meet all of the national security challenges without government participation. Presently, industry does not have the military preparedness knowledge or requisite national security clearances to perform the classified tasks required. However, industry's capital investment and the continued servicing of their customers--big and small--could well depend on the effectiveness of a joint program of National Security Emergency Preparedness. An effective Government-Industry cooperative program could well facilitate such a program.

About Ed Badolato, President, Contingency Management Services, Inc.

Mr. Badolato, is an internationally recognized authority in the field of emergency management for energy infrastructure and the environment, including contingency planning and response measures. He has been involved at every level of emergency activities with both government and private industry. As a former Deputy Assistant Secretary of the U.S. Department of Energy under Presidents Reagan and Bush, he was the principal architect of the U.S. government's readiness and response to emergencies in the oil, coal, gas, and electricity infrastructures--as well as protecting the U.S. nuclear weapon facilities from threats of natural disasters, terrorism, and sabotage. *Mr. Badolato is the president of CMS, Inc., a Washington based security company that provides consultant services to various major corporations and businesses. He is a retired U.S. Marine Corps Colonel*

His first-hand knowledge and top level energy emergency management experiences have included the following highlights:

■ **Managing the largest industrial security program in the United States Government: protecting the 58 DOE nuclear weapons facilities from espionage, terrorism and theft.**

■ **Directing the emergency response and planning for crises in our national energy infrastructure**

■ **Heading the National Response Team's Fact-finding Team that was sent to Valdez, Alaska to gather information for the 30-day report to the President after the Exxon Valdez oil spill;**

■ **Organizing the National Level Task Force that gathered put together the lessons learned from Hurricane Hugo;**

■ **Leading groups of U.S. experts abroad to solve such emergency problems as terrorist bomb attacks on oil facilities in South America and the Middle East and security problems with nuclear facilities in the Far East; and**

■ **Managing the Kuwait mine/EOD clearance operations for the Texaco and Getty Oil Companies after Operation Desert Storm.**

.