EPRI

REQUEST LETTER

June 2, 2000

Mr. Joel I. Klein
Assistant Attorney General
Antitrust Division
Main Justice Building
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001

Dear Mr. Klein:

The Electric Power Research Institute, Inc. ("EPRI") hereby requests the issuance of a business review letter pursuant to the business review procedure of the U.S. Department of Justice, Antitrust Division ("Department"), 28 C.F.R. § 50.6 (1997). We would very much appreciate a statement of the Department's current antitrust enforcement intentions regarding the following proposed information exchange. The proposed information exchange is a component of the Enterprise Infrastructure Security program ("EIS Program") being developed by EPRI to facilitate the energy industry's ability to efficiently address security risks presented by the increasing interconnection, interdependence and computerization of the industry, its suppliers and business partners.

Based on EPRI's experience with its collaborative Year 2000 Embedded Systems Program ("Year 2000 Program")[1], we believe that energy companies will be hesitant to exchange information regarding security risks absent an indication from the Department that such information exchanges, when conducted as proposed herein, will not result in enforcement actions against the participants. We note that during operation of the Year 2000 Program there was a noticeable increase in the information actually exchanged by program participants after the Department issued favorable business review letters with respect to the Year 2000 information

[1] The EPRI Year 2000 Embedded Systems Program facilitated the exchange of technical information about year 2000 problems in embedded systems in equipment, process instrumentation and control systems commonly used in the energy operations. Over 100 domestic and international energy companies (electricity, oil and natural gas) participated in this program during the three years it was in operation.

CORPORATE HEADQUARTERS
3412 Hillview Avenue | Palo Alto CA 94304-1395 USA | 650.855.2000 | Customer Service 800.313.3774 | www.epri.com

exchanges proposed by the Securities Industry Association and the National Association of Manufacturers.[2]

We request that the Department's business review be conducted on an expedited basis due to the urgency of the proposed activity, as explained below.

I. The Electric Power Research Institute

The Electric Power Research Institute, Inc is a nonprofit, tax-exempt organization committed to providing science and technology based solutions to all segments of the global energy industry for the benefit of the public. EPRI was incorporated in 1972 as a District of Columbia non-profit, membership corporation funded by voluntary contributions from the electric utility industry. The Internal Revenue Service has granted EPRI tax-exempt status as a scientific organization under Section 501(c)(3) of the Internal Revenue Code.

To carry out its mission, EPRI manages a broad program of collaborative scientific research, technology development and technology transfer. EPRI publishes the results of its research and makes those results available to the interested public on a non-discriminatory basis. Those persons, firms, government agencies, corporations or other entities, public or private, that are committed to, and have evidenced an intention to support, a national or international program for research and development in the production, transmission, distribution and utilization of electric power are eligible for EPRI membership and may participate in EPRI's traditional, collaborative research program. Membership is open to all qualifying entities on a nondiscriminatory basis. Current EPRI members are active in all phases of electricity generation, transmission, distribution, sales, and related services.[3]

II. The Importance of Electronic Security to the Energy Industry

The organizations that comprise the US energy infrastructure are overwhelmingly in the private sector. These organizations are involved in the generation, production, transmission, and/or distribution of electricity, oil and natural gas. The infrastructure for the electricity industry is characterized by generation facilities, transmission networks and distribution networks that create and supply electricity to end-users. The gas and oil industry infrastructure is characterized by production and holding facilities for natural gas, crude and refined petroleum and petroleum derived fuels; the refining and processing facilities for these fuels; and the transportation networks that deliver these commodities to end-users. Historically, these energy infrastructures have been vulnerable to physical security threats and attacks on substations, generation facilities and transmission lines, oil and gas pipelines, interconnects, stand-alone valves, pumps and compressors. Typically these threats have been managed locally by restricting and limiting unauthorized access to the facilities and by the use of physical weapons.

---

[2] Business Review Letter issued July 1, 1998 to Mr. Robert Bell, Esq., on behalf of the Securities Industry Association, and Business Review Letter issued August 14, 1998 to Mr. Jerry J. Jasinowski, President, National Association of Manufacturers.

[3] EPRI's traditional collaborative research program is described at http://www.epri.com/corporate/discover_epri/epri_facts/intro_epri.html

However, over the past few years, the President, Congress and the private sector have realized that the country's critical infrastructure industries[4] are increasingly exposed and vulnerable to cyber-threat and attack[5]. In fact, many now believe electronic information or "cyber" security risks are overshadowing physical security risks for many critical infrastructure industries. For the energy industry, this results from the increasing globalization of all energy segments, deregulation of domestic utilities and the rapid increase in the deployment and integration of real time operating systems in power plants, refineries and other processes vital to energy operations[6]. Exponentially increasing vulnerability to cyber-attack is the industry trend toward increasing connections between operating systems with communication, business and administrative systems which, in turn, may be connected to strategic third parties. Unlike physical vulnerabilities, cyber-vulnerabilities are global, rather than local, and can be easily launched from anywhere in the world. As the lifeblood of the economy of every nation and every major business, assurance of the energy infrastructure is a global issue that crosses the boundaries of business and nations alike.

In 1996, in response to growing concerns, the President established the President's Commission on Critical Infrastructure Protection ("PCCIP"), a joint government and private sector commission whose mission was to study cyber-security threats to the Nation's critical infrastructure industries. In October of 1997, the PCCIP issued a report[7] that identified industry cooperation and sharing of information relating to cyber-threats, vulnerabilities and interdependencies as the quickest and most effective way to achieve much higher levels of protection. In fact, the PCCIP identified information sharing among owners and operators of critical infrastructure assets as the "most immediate need"[8] and "an indispensable step"[9] to such protection. This study ultimately led to the issuance of Presidential Decision Directive 63 ("PDD 63") in May of 1998.

PDD 63 established a national critical infrastructure protection policy and a framework for developing and implementing infrastructure protection measures[10]. PDD 63 calls for taking immediate steps to protect the nation's critical infrastructure from cyber-attack. Under this Directive, the U.S. Department of Energy ("DOE") has been tasked with coordinating the energy sector effort. DOE has named the North American Electric Reliability Council ("NERC") as the Sector Coordinator for the electricity industry, the National Petroleum Council ("NPC") as the

---

[4] The critical infrastructure industries include electric power, oil and natural gas, information and communications, transportation, emergency services, banking and finance, water supply, and public health services.
[5] Cyber-threats and attacks are those conducted by electronic, radio frequency or computer-based means.
[6] For example, supervisory control and data acquisition systems, energy management systems, communications systems and digital control systems.
[7] Critical Foundations, Protecting America's Infrastructures (October, 1997), http://www.pccip.ncr.gov/report_index.html.
[8] Id. at 21.
[9] Id. at 27.
[10] PDD 63 is a classified "white paper". An explanation of its key elements can be found at http://ciao.ncr.gov/pccip/report_index.html.

Sector Coordinator for the oil industry and the American Gas Institute ("AGA") on behalf of the natural gas industry.[11]

III. The Proposed EPRI Enterprise Infrastructure Security Program

As discussed above, the federal government has recognized that a new and collaborative approach is required to manage the increasingly cyber-based risks to the reliability of our energy supply. The increasing interdependence among industry players and the use of common operating equipment, information systems and communication systems throughout the energy industry makes a collaborative effort to address the problem especially appropriate.

EPRI is developing the EIS Program to provide the energy industry with a forum for such a collaborative effort. The EIS Program will focus on the technical cyber-security problems presented by operating equipment, electronic information systems and communications systems. The EIS Program will be coordinated with the three Sector Coordinators (NERC, NPC and AGA) and representatives from these organizations will be invited to attend EIS Program workshops and other meetings as appropriate.

Participation in the EIS Program is open to all companies directly involved in the generation, production, transmission and distribution of energy on a nondiscriminatory basis and fair and reasonable terms. Eligibility for participation in the EIS Program is not conditioned on membership in EPRI's traditional collaborative research program. There will be no competitively significant restrictions on access to the Program, as the entry costs represent a very small component of any likely participant's system administration costs. In addition, for the smallest of the eligible organizations, EPRI will offer an aggregate membership opportunity so that the cost of participation will not be a barrier even for the smallest eligible organization.

In addition to "Members" (*i.e.*, domestic, international and multinational electric power companies, natural gas companies and petrochemical companies directly involved in energy production and distribution), EPRI eventually may create two other classes of participation in the EIS Program. The two additional classes of participation being contemplated are "Associates" - indirect participants in the chain of production and supply of energy and "Affiliates" - vendors of operating equipment and information systems used in the energy industry and providers of security services to the industry. Although the specific information available to each class may be different, each class of participant will have equal access to the information available to that class.

IV. The Proposed Information Exchange

EPRI contemplates information exchange by and between participants will be a primary component of the EIS Program. The exchange of several types of technical and security program management information is proposed. This information would be both experiential and technical and would be exchanged at EIS Program workshops and through an access controlled, interactive

[11] The role of Sector Coordinators as stated in PDD 63 is to provide the focus for industry cooperation and information sharing and to represent the sector in matters of national cooperation and policy.

Internet site. The information would be gathered, analyzed and disseminated with the goal of providing participant a cost-effective way to enhance their overall cyber-security posture. The EIS Program intends to address both the existing security issues and, to the maximum extent possible, anticipate and address future security issues that may be created by new products, evolving technology, and the growing sophistication of malfeasors.

The first type of information proposed to be exchanged in the EIS Program is energy industry-specific "best practices" for cyber-security programs. This information would be gathered from participant and third party experts invited to make presentations at EIS Program workshops. It is likely that this information exchange would include topics such as methodologies for conducting vulnerability assessments; development of plans to identify, alert, rebuff and prevent cyber-security breaches; plans for reconstitution of essential capabilities should an attack succeed; methods for "stress-testing" the cyber-security of the energy infrastructure; and activities designed to raise the level of awareness of directors, officers, employees, independent consultants and others in the energy industry with respect to managing cyber-security risks. The goal of this information exchange is the cost-effective compilation of information specific to the energy industry that can be used by participants to develop effective programs to reduce their cyber-security risk to a level each participant individually determines to be acceptable.

It is also proposed that participants will exchange information with respect to cyber-security vulnerabilities that they have identified in their operating equipment, electronic information and communications systems on a product by product basis. This information would be shared with the corresponding manufacturers, vendors or security services providers who would be invited to participate in the exchange to address their own equipment or systems. Such information is likely to include (1) the status of security technology in existing operating equipment and systems; (2) the results of security testing on specific operating equipment or electronic information or communications systems; (3) solutions to security problems with existing equipment or systems that have been identified or proposed; and (4) concerns that have been identified with such purported solutions. Under most circumstances, the information provided by manufacturers, vendors and security service providers will be shared with all participants who are Members of the EIS Program.[12] It is also anticipated that the EIS program would facilitate the development of "user group" discussions and information exchanges among participants. The goal of this information exchange is to more efficiently disseminate information about vulnerabilities and solutions participants have identified in operating equipment, electronic information and communications systems owned or operated by those in the user group.

It is possible that these product specific information exchanges could lead to the identification of electronic security requirements and features desired by the energy industry in the form of commonly accepted functional security specifications for future equipment and systems. Once compiled, this information would be made available to all affected manufacturers, vendors, security services providers and other interested parties, as well as be exchanged among EIS

[12] In operating its Year 2000 Embedded Systems Program, it was EPRI's experience that some equipment manufacturers and system vendors may be willing to disclose detailed technical information about their products only under a non-disclosure agreement that limits dissemination of the information to owners of such equipment and systems.

Program participants. The goal of this information exchange is to create greater efficiency in communicating security requirements and features between those in the energy industry and manufacturers, vendors and others can, on an individual basis, take this information into consideration with respect to the design of future equipment and systems and services.

Finally, the Program eventually may include the collaborative reporting, discussion and analysis of actual real time cyber-threat and attack information from a variety of sources, including participants, federal and state governments, other infrastructure industries, cyber-security experts and others, in order to more quickly identify and address in real time any actual cyber-security threats and attacks on the reliability of the nation's energy supply.

V. The Proposed EPRI EIS Program Will Not Be Anti-competitive

All participants in the EIS Program will be required to limit the information exchanged through the Program. Both at EIS workshops and on the EIS website, participants will be required to provide only information that they reasonably believe to be factually correct and all information will be exchanged in an objective and non-judgmental manner. Each participant will determine individually how to respond to any information exchanged and how the information will affect its individual purchasing and other related business decisions.

There will be no discussions of any specific prices of any particular operating equipment, electronic information and communications systems or cyber-security systems or services through the EIS Program, although it is likely that there will be some general discussion of cost impacts of various security-related activities and program models. No participant's specific, competitively sensitive information about prices, capacity or future plans will be exchanged directly or indirectly among participants through the EIS Program.

Manufacturers and vendors will be provided with information generated by the participants about their own products and services and will be invited to provide their own comments with respect this information. However, manufacturers and vendors will not be allowed access to confidential or non-public information exchanged about their competitors' products and services. Neither the participants nor EPRI intend to recommend in favor of, or against, the products or systems of particular manufacturers or vendors.

All information exchanged in the EIS Program will relate directly to technical and program management issues regarding physical and cyber-security. Since the costs of developing and operating any individual participant's security program typically would be a very small increment of its ongoing electronic and information systems costs, it is very unlikely that the Program would provide competitors with a meaningful or competitively significant degree of cost information. Nor would such limited information exchange be likely to have any bearing on other primary non-price components of competition such as quality and service values.

Finally, the proposed limited information exchange is not expected to affect innovation rivalry or lessen competition in the procurement of operating equipment, electronic information systems, or security-related services nor facilitate other ancillary or independent agreements that could

subvert competition among manufacturers, vendors, security services providers and others providing, products and services to the energy industry. The EIS Program will not be a conduit for any specific discussions or negotiations between, or on behalf of, vendors, manufacturers, or security services providers regarding any individual participant or group of participants.

VI. The Proposed EPRI EIS Program Will Be Pro-competitive

We believe the proposed information exchange has the potential to become a unique source of useful information about security risks and solutions specific to the energy industry. This, in turn, will make companies in the energy industry better able to withstand potential adverse consequences of security breaches. Companies will be able to focus on their core businesses, rather than on unrelated technical vulnerabilities. The ultimate goal of the EIS Program is the assurance of the business continuity of participating energy infrastructure companies, thereby assuring that the energy industry is better able to reliably generate, produce and distribute energy to the nation. EPRI firmly believes that potentially anti-competitive information exchanges are not necessary to any "good faith" effort to identify or remedy the physical and cyber-security problems facing the energy industry.

The proposed information exchange should have a pro-competitive effect to the extent participants will be able to identify and address their security risks more efficiently. More efficiently identifying cyber-vulnerabilities and the means to rebuff cyber-attacks potentially could increase output by reducing redundant security-related costs and thereby allowing for more productive deployment of resources both by the energy industry and by the operating equipment manufacturers and electronic information and communication systems vendors.[13]

Manufacturers and vendors will benefit, because they will not need to answer inquiries from, and respond to, many customers and potential customers repetitively. Vendors, manufacturers and security services providers will also benefit from having a source of generally accepted industry-based information regarding cyber-security risks and issues that affect the products and services that they market to the energy industry. In fact, the information derived from the EIS Program has the potential to identify a market for new products and services.

VI. Conclusion

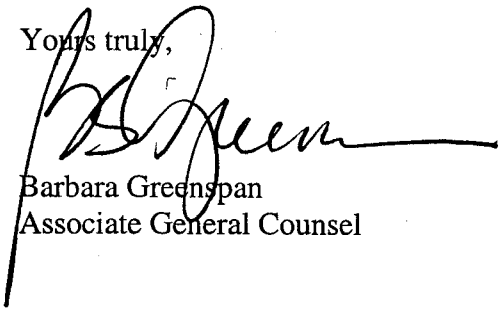
It is very important for the participants and potential participants in this Program to be secure in knowing that the Government of the United States supports these efforts and that the information exchange proposed for the EIS Program, as outlined above, generally does not raise antitrust concerns. We believe a program aimed at assuring the cyber-security of the energy infrastructure is essential, and we are very interested in working with the Department to develop a program that properly recognizes the limits imposed by the antitrust laws with respect to information exchange. If there are specific types of information that the Department believes to be particularly sensitive in this context, we would like to work with you to address them in the

[13] Internet analysts at Aberdeen Group, Boston, MA. Report that corporations spent $7.1 billion on corporate security to protect themselves against cyber-attacks in 1999 and that the bill could reach $17 billion by 2003. "Valley Cool to Reno Cybercrime Plan", Martha Mendoza, Associated Press, April 6, 2000.

program design and to make sure that all EIS Program participants are aware of them.

EPRI would be pleased to provide further information to the Department at your request. I appreciate your assistance and look forward to your response.

Yours truly,



Barbara Greenspan
Associate General Counsel

cc: Barry Grossman, Antitrust Division, US Department of Justice
Jane Kumin, Chief Legal Officer, EPRI
Ric Rudman, Chief Operating Officer, EPRI
Dr. Charles Siebenthal, EIS Program Manager, EPRI