DEPARTMENT OF JUSTICE
Antitrust Division

JOEL I. KLEIN
Assistant Attorney General

Main Justice Building
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530-0001
(202) 514-2401 / (202) 616-2645 (f)

antitrust@justice.usdoj.gov (internet)
http://www.usdoj.gov (World Wide Web)

October 2, 2000

Barbara Greenspan, Esq.
Associate General Counsel
Electric Power Research Institute, Inc.
3412 Hillview Avenue
Palo Alta, California 94304-1395

Dear Ms. Greenspan:

This is in response to your request on behalf of the Electric Power Research Institute, Inc. ("EPRI") and its members for the issuance of a business review letter pursuant to the Department of Justice's Business Review Procedure, 28 C.F.R. § 50.6. You have requested a statement of the Department of Justice's antitrust enforcement intentions with respect to a proposed information exchange designed to reduce security risks in the energy industries presented by the increasing interconnection, interdependence and computerization of those industries, and their suppliers.

EPRI is a nonprofit organization committed to providing and disseminating science and technology-based solutions to energy industry problems. Membership is open to all individuals and entities, public and private, interested in the issues relevant to the electric power industry.

EPRI's request notes that our nation's "critical infrastructure industries" -- electric power, oil and natural gas, information and communications, transportation, emergency services, banking and finance, water supply, and the public health services -- have historically been vulnerable to physical attacks on their various physical facilities. You suggest, however, that as firms in the energy industries have become increasingly computer dependent and interconnected to suppliers, customers and rivals, a wide-spread concern has emerged about the vulnerability of these industries to cyber-threats and attacks, i.e., those conducted by electronic, radio frequency or computer-based means.

Indeed, that concern was reflected in a 1997 Presidential Commission Report that concluded that industry cooperation and information sharing is the quickest and most efficient way of protecting our critical infrastructure industries against cyber-threats. Presidential Decision Directive 63, issued in 1998, directed the Department of Energy to coordinate the efforts of the energy industries to enhance their security against cyber-threats. EPRI has developed an Enterprise Infrastructure Security ("EIS") program to assist the various energy industries to efficiently address security risks raised by the increased interconnection, interdependence and computerization of the industry, its suppliers and customers.

You have assured us that the proposed information exchanges will not disadvantage any firm or segment of the various energy markets. Thus, participation in the EIS program will be opened on a nondiscriminatory basis to all firms directly involved in the generation, production, transmission and distribution of energy. It is also contemplated that "Associate" membership will be made available to indirect participants in the production and supply system, and that "Affiliate" membership will be made available to vendors of operating equipment, information systems and security services to the energy industry.

It is contemplated that two principal types of information will be exchanged. The first will involve energy industry specific "best practices" for cyber security programs. You indicate that 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.

According to your request, the second principal type of information that will be exchanged by participants will relate 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. 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.

You note that "it also 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 program participants . . . "

Finally, you indicate that:

> 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.

Your request asserts that EPRI has adopted a number of measurers to lessen the possibility that its proposed information exchange will have any anticompetitive effects. The information to be exchanged will be strictly limited in nature; all information exchanged will relate directly to physical and cyber-security. There will not be any discussion of specific prices for equipment, electronic information or communications systems. No company-specific competitively sensitive information, i.e., prices, capacity or future plans, will be exchanged through the EIS program. The program will not serve as a conduit for discussions or negotiations between or amongst vendors, manufacturers or security service providers with respect to any participant or group of participants. Neither the EPRI nor any participant will recommend in favor of or against any product or systems of particular manufacturers or vendors. On the contrary, it will be left to each participant to determine the effect of the exchanged information on its individual purchasing and related decisions.

On the basis of the information and assurances that EPRI has provided to us, it does not appear that the proposed information exchange will restrict competition in any of the energy-related markets in which the participants do business. As long as the information exchanged is limited, in the manner discussed above, to physical and cyber-security issues, the proposed interdictions on price, purchasing and future product innovation discussions should be sufficient

to avoid any threats to competition. Indeed, to the extent that the proposed information exchanges result in more efficient means of reducing cyber-security costs, and such savings redound to the benefit of consumers, the information exchanges could be procompetitive in effect.

For these reasons, the Department is not presently inclined to initiate antitrust enforcement action against the EPRI's proposed information exchange. This letter, however, expresses the Department's current enforcement intention. In accordance with our normal practices, the Department reserves the right, in appropriate circumstances, to bring any enforcement action in the future if the actual operation of the proposed agreement proves to be anticompetitive in any purpose or effect.

This statement is made in accordance with the Department's Business Review Procedure, 28 C.F.R. § 50.6. Pursuant to its terms, your business review request and this letter will be made publicly available immediately, and any supporting data will be made publicly available within 30 days of the date of this letter, unless you request that part of the material be withheld in accordance with Paragraph 10(c) of the Business Review Procedure.

Sincerely,

\S\

Joel I. Klein