

EDO Principal Correspondence Control

FROM: DUE: 09/04/03 EDO CONTROL: G20030501
DOC DT: 08/22/03
FINAL REPLY:

Rep. Edward J. Markey

TO:

Chairman Diaz

FOR SIGNATURE OF : ** PRI ** CRC NO: 03-0548

Chairman

DESC:

ROUTING:

Concerns Press Report that in January a Computer
Virus Penetrated a Private Computer Network at
First Energy's Davis Besse Nuclear Power Plant

Travers
Paperiello
Kane
Norry
Collins
Dean
Burns/Cyr
Caldwell, RIII
Borchardt, NRR
Merschhoff, CIO

DATE: 08/22/03

ASSIGNED TO: CONTACT:
NSIR Zimmerman

SPECIAL INSTRUCTIONS OR REMARKS:

Coordinate with RIII and NRR.

Template: SECy-017

SECY
ERids: 2003-01

OFFICE OF THE SECRETARY
CORRESPONDENCE CONTROL TICKET

Date Printed: Aug 22, 2003 13:13

PAPER NUMBER: LTR-03-0548 **LOGGING DATE:** 08/22/2003
ACTION OFFICE: EDO

AUTHOR: Edward Markey
AFFILIATION: REP
ADDRESSEE: Nils Diaz
SUBJECT: Concerns press reports that in January a computer virus was able to penetrate a private computer network at First Energy's Davis Besse nuclear power plant

ACTION: Signature of Chairman
DISTRIBUTION: Chairman, Comrs, RF, OCA to Ack

LETTER DATE: 08/22/2003
ACKNOWLEDGED: No
SPECIAL HANDLING:

NOTES: Commission Correspondence
FILE LOCATION: Adams

DATE DUE: 09/08/2003 **DATE SIGNED:**

EDO --G20030501

EDWARD J. MARKEY

7TH DISTRICT, MASSACHUSETTS

ENERGY AND COMMERCE COMMITTEE

RANKING MEMBER
SUBCOMMITTEE ON
TELECOMMUNICATIONS AND
THE INTERNET

SELECT COMMITTEE ON
HOMELAND SECURITY

RESOURCES COMMITTEE

2108 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-2107
(202) 225-2836

DISTRICT OFFICES:

5 HIGH STREET, SUITE 101
MEDFORD, MA 02155
(781) 398-2900

188 CONCORD STREET, SUITE 102
FRAMINGHAM, MA 01702
(508) 875-2900
www.house.gov/markey

Congress of the United States
House of Representatives
Washington, DC 20515-2107

August 22, 2003

The Honorable Nils J. Diaz
Chairman
Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Mr. Chairman:

I am writing to request more information regarding press reports that in January 2003, a computer virus was able to penetrate a private computer network at First Energy's Davis-Besse nuclear power plant in Ohio. The reports indicate that the virus -- known as the "Slammer" Worm -- disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall. Several other press reports have speculated that First Energy's power plants and/or related transmission and distribution infrastructure may be somehow implicated in the events that led to last week's blackout. I am concerned that cyber-security flaws at Davis-Besse, along with other potential such flaws at other nuclear power plants in Ohio, may have rendered the system vulnerable to more recent viruses such as the "Blaster" worm, which was at its peak activity levels at precisely the same time that the blackout occurred.

The August 19, 2003 issue of *Security Focus News*¹ reported that in January, the Slammer worm entered the Davis-Besse plant by penetrating the unsecured network of an unnamed Davis-Besse contractor, and then proceeded through a T1 line that bridged that network and Davis-Besse's corporate network. The T1 line turned out to be one of several that completely bypassed the company's firewall. The Slammer worm was reported to be the fastest spreading computer worm in history, infecting more than 90% of vulnerable hosts within 10 minutes, and causing network outages, cancelled flights, and ATM failures.

According to the *Security Focus News* report, by 9 AM on January 25 (the time Slammer began to infect computers around the world), users noticed slow performance on Davis-Besse's business network. The worm then spread to the plant network, where workers had not installed the Microsoft security patch made available 6 months earlier. By 4 PM, nuclear power plant workers noticed a slowdown on the plant network. At 4:50 PM, the congestion created by the worm crashed the plant's computerized display panel (the Safety Parameter Display System, or SPDS), and at 5:13 PM, the Plant Process

¹ See <http://www.securityfocus.com/news/6767>

² See <http://www.cs.berkeley.edu/~nweaver/sapphire/>

Computer (PPC) crashed. While both systems had redundant analog backups, a March 2003 advisory distributed by the nuclear industry reportedly stated that "the unavailability of SPDS and PPC was burdensome to the operators." It took 4 hours and 50 minutes to restore the SPDS and 6 hours and 9 minutes to restore the PPC.

This press report also drew from other reports from the North American Electric Reliability Council to detail other cyber-security matters that could be relevant to last week's blackout:

- The Slammer worm also cut one utility's critical Supervisory Control and Data Acquisition Network (SCADA, used to monitor substation characteristics, such as kilowatt-hour use and voltage and amperage readings. Utilities can also track electric use in homes and businesses through automated meter reading units placed in strategic parts of the network).
- The Slammer worm also blocked another company's SCADA traffic because it relied on bandwidth leased from a telecommunications company that was affected by the worm.

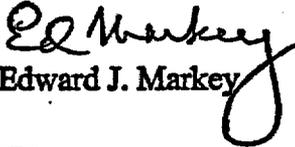
It may be too soon to know whether the Blaster worm was involved in last week's blackout. However, it is clear that cyber-security was deeply flawed at the Davis-Besse nuclear reactor just a few months before the blackout occurred. Consequently, I ask for your prompt assistance in responding to the following questions:

- 1) What proposals has the NRC made to strengthen its cyber-security regulations since September 11, 2001? If no such changes were made, why not?
- 2) Was First Energy in violation of NRC's cyber-security regulations when the Davis-Besse plant was penetrated by the Slammer worm? If so, what penalty did the NRC impose?
- 3) What proposals has the NRC made to strengthen its cyber-security regulations since the Slammer worm penetrated the Davis-Besse plant in January 2003? If no such changes were made, why not, since the incident clearly highlighted a serious and exploitable problem?
- 4) Please provide copies of all cyber-security reviews the NRC has performed on individual reactors or industry-wide since September 11, 2001. If no such reviews have been performed, why not?
- 5) Has the NRC inspected the cyber-security measures taken by other nuclear reactors in order to determine whether they are in compliance with NRC regulations? If so, what was the result? If not, why not?
- 6) Does the NRC ever conduct tests of the adequacy of cyber-security at nuclear power plants? How often? How many plants have been tested, and what were the results? Do these tests consist of NRC attempts to penetrate the plants' networks in order to determine whether hackers, a virus or a cyber-terrorist could do so?
- 7) Is there any evidence that last week's blackout could have been caused by the Blaster worm or some other cyber-security flaw? If so, please provide it?

- 8) Do you believe it is possible that a cyber-attack could successfully penetrate nuclear reactor networks and result in an outage of that reactor and/or a more widespread outage? Why or why not?

Thank you very much for your attention to this important matter. Please provide your response no later than Friday, September 12, 2003. If you have any questions or concerns, please have your staff contact Dr. Michal Freedhoff or Mr. Jeff Duncan of my staff at 202-225-2836.

Sincerely,


Edward J. Markey

cc: The Honorable Spencer Abraham, Secretary
U.S. Department of Energy
cc: The Honorable Tom Ridge, Secretary
U.S. Department of Homeland Security
cc: The Honorable Pat Wood, Chairman
Federal Energy Regulatory Commission
cc: Michehl Gent, President
North American Electricity Reliability Council