



Agenda Date: 3/18/16
Agenda Item: 6A

STATE OF NEW JERSEY
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, New Jersey 08625-0350
www.nj.gov/bpu

RELIABILITY & SECURITY

IN THE MATTER OF UTILITY CYBER SECURITY
PROGRAM REQUIREMENTS

)
)
)
)
)

ORDER

DOCKET NO. AO16030196

(SERVICE LIST ATTACHED)

BY THE BOARD:

The New Jersey Board of Public Utilities ("Board") initiated this matter in order to establish requirements to mitigate cyber risks to critical systems of electric, natural gas, and water/wastewater utilities ("Utilities"). As technology advances, Utilities' computerized systems are increasingly susceptible to cybersecurity attacks, including data breaches, corporate theft, and sabotage perpetrated by actors throughout the world. Due to the critical nature of the Utilities' services, the Board recognizes that action is necessary to mitigate cyber security risks to Utilities' computerized systems. In addition, to the extent information is shared and provided by the Utilities; the Board recognizes that such information is confidential and sensitive and requires appropriate confidentiality protections.

BACKGROUND

The New Jersey Domestic Security Preparedness Act was enacted after the events of September 11, 2001 to establish a domestic security preparedness planning group and task force to enhance and integrate security and preparedness measures throughout the State. N.J.S.A. App. A:9-68. "No record held, maintained or kept on file by the [New Jersey Domestic Security Preparedness Task Force ("Task Force")] or planning group shall be deemed to be a public record under the provisions of [the Open Public Records Act, N.J.S.A.] or the common law concerning the access to public records." N.J.S.A. App. A:9-74a. Pursuant to Executive Order No. 5 (Corzine), the Task Force is now part of the New Jersey Office of Homeland Security and Preparedness ("NJOHSP").

In the wake of the September 11 attacks, it became evident that Utilities could be prime targets for additional attacks. The State of New Jersey has found it necessary to develop standard utility industry security practices. In 2004, the Board ordered all utilities to implement the Best Practices and Recommended Response Protocols to the Homeland Security Advisory Systems ("Security Documents") developed by the Task Force, which superseded the preliminary utility security protocols and best practices initially implemented by the Board on December 11, 2001. See I/M/O Revised Security Best Practices For All Public Utilities and Cable Television Companies, BPU Dkt. No. AO04070733, Order dated August 20, 2004.

Pursuant to N.J.S.A. 48:2-36.1, the Board "may by order in writing require any public utility to ... submit to the Board any data, material and relevant to any inquiry, investigation, or proceeding."

Pursuant to N.J.A.C. 14:3-6.7, utilities are required to report various suspicious activities, including (a)(2) "forced entry to any utility facility, or entry achieved by deception;" and (a)(5) "intentional damage to any utility facility or equipment."

In 2011, the Board directed public utilities to report to Reliability and Security Staff regarding operation and use of their Industrial Control Systems ("ICS"). See I/M/O Cyber Incident Reporting for Utility Industrial Control Systems, BPU Dkt. No. EO11090575, Order dated October 23, 2011. The Board directed utilities under its jurisdiction to identify whether they use ICS, including Supervisory Control and Data Acquisition ("SCADA"), to monitor and/or remotely control utility facilities. It further directed those utilities who responded affirmatively to report cyber incidents involving those systems directly to the Director of Reliability and Security and Reliability and Security Staff designated by the Director of Reliability and Security ("Reliability and Security Division Staff") and to NJOHSP.

In 2013, President Barack Obama identified cyber threats to critical infrastructure as one the most serious security challenges facing our nation. See Executive Order No. 13636, February 19, 2013. To demonstrate his point, the President cited repeated attempts to sabotage the power grid and similar infrastructure by a host of enemies from hackers to nation states. He suggested that more needed to be done. (2013 State of the Union Address).

In 2015, pursuant to Executive Order No. 178 (Christie), the Governor established the New Jersey Cyber Security and Communications Integration Cell ("NJCCIC") under NJOHSP to coordinate cybersecurity information sharing and analysis between and among the government and private sectors. Specifically, NJCCIC was created to "receive relevant cybersecurity threat information from appropriate sources, including public utilities and private industry."

The U.S. Department of Homeland Security reported that attacks against utilities' digital infrastructure doubled in 2014. Moreover, a cyber-attack on the power distribution system in Ukraine in late 2015 underscored the risk for utilities in the U.S. The attack, triggered by unauthorized access to industrial control systems, caused regional disruptions to more than 225,000 people. See Alert (IR-ALERT-H-16-056-01), U.S. ICS-CERT, February 25, 2016.

Staff met with cyber security professionals from electric, natural gas, and water utilities on multiple occasions to discuss the approach to and specific requirements of cyber security for critical utility systems. These Utilities were given opportunities to review and provide comments to Staff on draft requirements. Substantive comments were incorporated into the final recommendations presented for Board consideration. Additionally, Staff consulted with cyber experts from the Federal Bureau of Investigation ("FBI") and NJOHSP.

DISCUSSION AND FINDINGS

As technology evolves, entry into a facility can be accomplished by means other than physical entry. In this case, the Board is concerned that unauthorized persons could be accessing Utilities' critical systems. Such access may be accomplished by forceful hacking or deception, such as social engineering. Pursuant to N.J.A.C. 14:3-6.7, such "entry" or damage to Utilities' computer system would constitute a reportable incident.

As described above, Utilities' systems are increasingly susceptible to cyber-attack, which jeopardizes safety, reliability, and customer privacy. Due to the critical nature of Utilities' services, action beyond information sharing and implementing best practices is necessary to safeguard the Utilities' critical systems.

The goal of cybersecurity is to safeguard the confidentiality, integrity, and availability of an organization's digital information assets. Risks associated with unauthorized access, changes or destruction of these assets must be effectively managed. A comprehensive Cyber Security Program represents both a strategic and tactical approach to risk identification and assessment, mitigation and monitoring, and audit and reporting.

To this end, Reliability and Security Division Staff developed a set of cyber security requirements that apply equally to Utilities to reduce cyber security risks to critical utility systems. For purposes of this Order, these systems include industrial control systems, including SCADA, and systems that contain customer personally identifiable information. Furthermore, the cyber security requirements generally focus activities at the program level rather than prescribe specific and detailed practices and technologies. In this way, Utilities may retain the flexibility necessary to meet the continuously evolving cyber threat landscape while remaining compliant to overarching cyber security program goals.

Reliability and Security Division Staff sought out and included input from cyber security experts at electric, natural gas, and water utilities. Additionally, Reliability and Security Division Staff consulted with FBI and NJOHSP during the development of these requirements.

Reliability and Security Division Staff recommends that the Board direct electric, natural gas, and water/wastewater utilities to meet certain cyber security program requirements to reduce cyber security risks to ICS and computer systems that contain customers' personally identifiable information. Reliability and Security Division Staff further recommends that these issues continue to be reviewed to determine whether these requirements should be extended to other parties subject to the Board's jurisdiction or otherwise broadened in scope by the Board.

The Board **HEREBY FINDS** that the Utilities must safeguard their computerized systems against cyber-attacks. The Board **FURTHER FINDS** that the sharing of information by the Utilities through NJCCIC is useful and vital to cyber security safeguarding. Therefore, pursuant to N.J.S.A. 48:2-36.1 and N.J.A.C. 14:3-6.7, the Board **HEREBY DIRECTS** that electric, natural gas, and water/wastewater utilities implement the following Cyber Security Program requirements, at a minimum, to manage cyber security risks, and that these measures would supersede the 2011 Cyber Security related order:

Scope of Assets

For purposes of this Order, covered assets, hereafter called critical systems, include the following:

- 1) industrial control systems (ICS), defined as a computerized system capable of gathering and processing data from utility facilities or applying operational controls to utility facilities; and
- 2) customer information systems that contain "personal information" as defined at N.J.S.A. 56:8-161.

Cybersecurity Requirements

Utilities must have a Cyber Security Program that defines and implements organizational oversight, accountabilities, and responsibilities for cyber risk management activities, and that establishes policies, plans, processes, and procedures for identifying and mitigating risk to critical systems to acceptable levels.

Additionally, the Cyber Security Program must meet the following minimum requirements:

1. Cyber Risk Management:

- a. Identify – Annually inventory critical systems and document changes.
- b. Analyze – Annually assess and prioritize cyber risks, including physical risks, to identified critical systems. At a minimum, incorporate information from the following as input into the risk analysis: vulnerability assessments; current threat assessment; and, relevant disaster recovery and business continuity requirements. Document risk assessment methodology and criteria used to assess and prioritize risks. A prevalent cyber security framework, such as those promulgated by National Institute of Standards & Technology ("NIST"), Department of Energy ("DOE"), and ISACA, should be considered when selecting a risk methodology.
- c. Control – Implement administrative, technical (logical and physical), and compensating controls, alone or in combination, to mitigate prioritized cyber risks in accordance with the assessment performed in 1b above.
- d. Measure and Monitor – Annually review risk assessment methodology to identify and incorporate revisions as appropriate.

2. Situational Awareness:

Utilities must maintain situational awareness of cyber threats and vulnerabilities so that cyber risks to critical systems are identified, mitigated, and remediated on an ongoing basis. At a minimum, Utilities shall:

- a. Monitor log files of critical systems, in accordance with the risk identified in 1b;
- b. Monitor internal and external sources of threat and vulnerability information, including vendor and industry-appropriate Information Sharing and Analysis Center ("ISAC") or Information Sharing and Analysis Organizations ("ISAO") advisories; and establish a review process to determine applicability and response.
- c. Review vendor security patches in a timely manner, and implement as appropriate.

3. Incident Reporting:

Utilities shall report the following, at a minimum, to designated Reliability and Security Division Staff:

- a. Utilities shall report cyber events relating to ICS, as set forth below:
 - i. A person, including any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity that accessed the ICS without authorization or exceeded authorized access. For purposes of this order, "exceeds authorized access" means a person who accesses the ICS with authorization and uses such access to obtain or alter information in the ICS that the person is not entitled to obtain or alter.
 - ii. Unauthorized programs, information, code or commands discovered on an ICS.
 - iii. A person extorted any money or other thing of value by threatening to cause damage to your industrial control system. For purposes of this order, damage includes any impairment to the integrity or availability of data, a program a system, or information.
 - iv. Reports must be submitted to Reliability and Security Division Staff through the NJ Cybersecurity and Communications Integration Cell ("NJCCIC") and in accordance with the prevailing rules, requirements, and submittal forms and formats designated by the NJCCIC. Pursuant to N.J.A.C. 14:3-6.7, reports shall be made within 6 hours of the detection of an incident.
- b. Utilities shall copy Reliability and Security Division Staff on notifications to law enforcement agencies of the State of New Jersey regarding information breaches involving the personally identifiable information of customers to the extent such notifications are required by the laws of the State of New Jersey, including, but not limited to, N.J.S.A. 56:8-163.
- c. Utilities shall report unusual cyber activity that has the potential to compromise critical systems and for which controls are ineffective. Reports must be submitted to Reliability and Security Division Staff through the NJCCIC and in accordance with the prevailing rules, requirements, and submittal forms and formats designated by the NJCCIC.

4. Response and Recovery:

- a. Establish a Cyber Security Incident Response Plan ("Plan") that addresses the life-cycle of an incident, including identification of, response to, and recovery from a cyber event. The Plan must include protocols for log file retention to support forensic analyses.
- b. Conduct an exercise to test the Plan once every 24 calendar months, at a minimum. The exercise can be a tabletop or a response to an actual cyber incident. Subsequent to the exercise or cyber incident, the utility shall document and incorporate lessons learned into the Plan, as appropriate.

5. Security Awareness and Training:

- a. Develop and implement a cyber security awareness program.
 - i. The cyber security awareness program must include general cybersecurity topics as well as emerging threats.
 - ii. The cyber security awareness program must be reviewed biannually and updated as appropriate.
- b. Cyber security awareness communications must be provided periodically throughout the year.
- c. Develop and implement cyber security training that details cyber security roles and responsibilities, for individuals who have access credentials to industrial control systems and for administrators of customer information systems that contain personal information.
- d. Develop and implement protocols for training new personnel as well as periodic training re-enforcement.

Implementation

1. Utilities must join the NJCCIC and create a cyber security incident reporting process no later than 60 days after the effective date of this order. Utilities must submit written confirmation of compliance with this requirement to Reliability and Security Division Staff no later than June 1, 2016.
2. Utilities must submit a written report to Reliability and Security Division Staff no later than June 1, 2016 that documents the assignment of organizational oversight, accountabilities, and responsibilities for cyber risk management activities.
3. Utilities must comply with all other requirements no later than October 1, 2017. Utilities must submit a written certification of compliance to Reliability and Security Division Staff no later than October 31, 2017. The certification must be signed by appropriate executive-level personnel with authority for the Utilities' Cyber Security Program.
4. Utilities must submit a written report to Reliability and Security Division Staff no later than December 31, 2016 describing progress toward compliance with these requirements and defining potential barriers that may interfere with meeting the defined implementation date.

Accountability and Board Review

1. Utilities shall certify on an annual basis compliance with the minimum requirements set forth above. Such certification must be submitted to Reliability and Security Division Staff no later than December 31 of each year following the implementation period. Further, each certification must be signed by appropriate executive-level personnel with authority for the Utility's Cyber Security Program.
2. In cases where Utilities have critical systems that are also subject to North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") standards, certification of compliance with those standards is sufficient to meet the annual certification requirement under this order for those critical systems. Such certification of compliance must be submitted to Reliability and Security Division Staff in accordance with the timeline noted above.
3. Utilities shall cooperate with Reliability and Security Division Staff in evaluations of the effectiveness of the Utilities' Cyber Security Program.

The Board further **DIRECTS** Reliability and Security Division Staff to review incidents of cyber intrusion into critical systems as defined in this Order. The Board **HEREBY FINDS** that in order to facilitate this review it must gather information from the Utilities. The Board further **DIRECTS** the Utilities to report and certify on the adequacy of the utility security arrangements as set forth in this Order. Reliability and Security Division Staff will continue to monitor the Utilities' performance and compliance with the Cyber Security Program requirements documented in this Order.

The Board further **DIRECTS** Staff to share information with NJCCIC regarding Utilities' cyber intrusions.

The Board further **DIRECTS** Reliability and Security Division Staff to continue to review and determine the appropriateness of a Cyber Security Program for any public utilities and other entities subject to the Board's jurisdiction not subject to this Order.

Reliability and Security Division Staff shall further review the Cyber Security requirements set forth in this order to determine whether additional requirements or program refinements are appropriate.

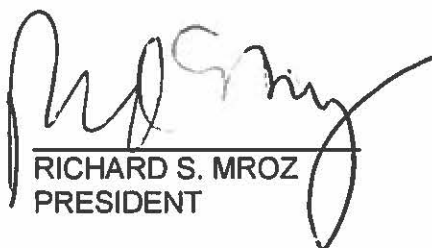
The Board has given consideration to the sensitive security nature of the information and reports required by this order, including the Utilities' Cyber Security Programs and the Utilities' ability to defend against cyber intrusions. The Board **FINDS**, consistent with Executive Order No. 21 (McGreevey), that public disclosure of such information would "substantially interfere with the State's ability to protect and defend its citizens against acts of sabotage or terrorism or would materially increase the risk or consequences of potential acts of sabotage or terrorism". The Board **FURTHER FINDS** that similar Cyber Security information reported to NJCCIC, within NJOHSP, would be deemed confidential. Therefore, the Board **HEREBY ORDERS** that in exercising its authority pursuant to N.J.A.C. 14:1-12.1(e), any reports and other information submitted, collected or exchanged in accordance with this Order shall be deemed confidential and shall not be considered to be a government record consistent with N.J.S.A. 47:1A-1 et seq.. As such, when submitted by Utilities, such information shall be appropriately labeled and protected consistent with the Board's confidentiality rules. The Board directs staff to develop a Memorandum of Understanding, to be negotiated between the BPU and the New Jersey

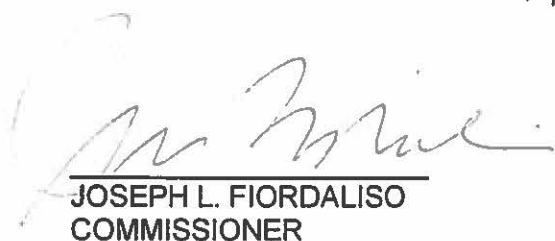
Cybersecurity Communications and Integration Cell ("NJCCIC"), to address how cybersecurity information submitted to NJCCIC will be handled and shared with the BPU. The Board **FURTHER AUTHORIZES** the President to execute such a Memorandum of Understanding on behalf of the BPU.

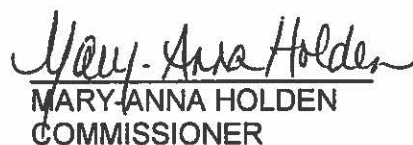
This Order shall be effective on March 28, 2016.

DATED: 3-18-16

BOARD OF PUBLIC UTILITIES
BY:


RICHARD S. MROZ
PRESIDENT

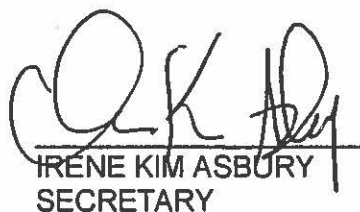

JOSEPH L. FIORDALISO
COMMISSIONER


MARY-ANNA HOLDEN
COMMISSIONER

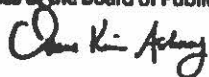

DIANNE SOLOMON
COMMISSIONER


UPENDRA J. CHIVUKULA
COMMISSIONER

ATTEST:


IRENE KIM ASBURY
SECRETARY

I HEREBY CERTIFY that the within
document is a true copy of the original
in the files of the Board of Public Utilities



IN THE MATTER OF UTILITY CYBER SECURITY PROGRAM REQUIREMENTS

Docket No. AO16030196

SERVICE LIST

Irene Kim Asbury, Esq.
Secretary of the Board
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, NJ 08625-0350
Irene.asbury@bpu.state.nj.us

Kenneth Sheehan, Esq.
Chief of Staff
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, NJ 08625-0350
Kenneth.Sheehan@bpu.state.nj.us

Paul Flanagan, Esq.
Executive Director
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, NJ 08625-0350
Paul.Flanagan@bpu.state.nj.us

James Giuliano, Director
Division of Reliability & Security
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, NJ 08625-0350
James.Giuliano@bpu.state.nj.us

Lynn Costantini
Division of Reliability & Security
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, NJ 08625-0350
Lynn.Costantini@bpu.state.nj.us

Tim Davies, President & CEO
Applied Wastewater
2 Clerico Lane
Hillsborough, NJ 08844-1615

William Davis, President
Aqua NJ
10 Black Forest Road
Hamilton, NJ 08691

John Hildabrandt, Manager Operations
Aqua NJ
10 Black Forest Road
Hamilton, NJ 08691

David Watson, Acting Superintendent
Berlin Borough
59 South White Horse Pike
Berlin, NJ 08009

John Walls, Supervisor
Bordentown City
324 Farnsworth Avenue
Bordentown, NJ 08505

Burt Lundbert, President
Cedar Glen Lakes Water
Michigan Avenue
Whiting, NJ 08759

Robert Cutter, Business Admin
Kathy Olsen, CFO
Clinton Town of
43 Leigh Street
PO Box 5194
Clinton, NJ 08809

Jan Kokes, President
Thomas O'Gara, Manager
Crestwood Village Water
55 Schoolhouse Road
Whiting, NJ 08759

Carol Artale, Esq.
Legal Specialist
Counsel's Office
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, NJ 08625-0350
Carol.Artale@bpu.state.nj.us

James Kane, Esq.
Legal Specialist
Counsel's Office
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, NJ 08625-0350
James.Kane@bpu.state.nj.us

Geoffrey Gersten, Esq.
Department of Law and Public Safety
Division of Law
124 Halsey Street
Post Office Box 45029
Newark, NJ 07102-45029
Geoffrey.gersten@dol.lps.state.nj.us

Roger Pederson
Manager, NJ Regulatory Affairs, External
Issues and Compliance
ACE – 63ML38
5100 Harding Highway
Mays Landing, NJ 08333

Philip J. Passanante, Esq.
Associate General Counsel
ACE – 92DC42
500 North Wakefield Drive
Post Office Box 6066
Newark, DE 19714-6066

Alison Regan
Pepco Holdings, Inc. – 79NC59
401 Eagle Run Road
Post Office Box 9239
Newark, DE 19714-9239

Luis Acevedo, Interim Superintendent
Dover Town of
100 Princeton Avenue
Dover, NJ 07801

James Carroll, Manager
John Sanclimenti, President
Jeff Kalajian, Vice President
John Cannie, Treasurer
Fayson Lakes Water
160 Boonton Avenue
Kinneelon, NJ 07405

Dorothy Gorman, Owner
Charles Gartland, Chairman
John McDonough, President
Bob Chozick, VP
Forest Lakes Water
45 Sleepy Hollow Road
PO Box 264
Andover, NJ 07821

Gary Ern, President
David Ern, Vice President
Gordon's Corner Water
475 County Road 520
Marlboro, NJ 07746

Jeffrey Fuller, President
Lake Lenape Water
83 Eagle Chase
Woodbury, NY 11797

Steve Parah, Superintendent
Lawrenceville Water
12 Gordon Avenue
Lawrenceville, NJ 08648

Dennis Doll, President
Middlesex Water
1500 Ronson Road
PO Box 1500
Iselin, NJ 08830-0452

Mario A. Giovannini
Pepco Holdings, Inc. – 79NC22
401 Eagle Run Road
Post Office Box 9239
Newark, DE 19714-9239

John L. Carley, Esq.
Consolidated Edison Co., of NY
Law Department, Room 1815-S
4 Irving Place
New York, NY 10003

Margaret Comes, Sr. Staff Attorney
Consolidated Edison Co., of NY
Law Department, Room 1815-S
4 Irving Place
New York, NY 10003

Brian MacLean
Elizabethtown Gas
52 Green Lane
Union, NJ 07083
bmaclean@aglresources.com

Mary Patricia Keffe, Esq.
Elizabethtown Gas
520 Green Lane
Union, NJ 07083
pkeefe@aglresources.com

Kevin Connelly
First Energy
300 Madison Avenue
Post Office Box 1911
Morristown, NJ 07962-1991

Mark A. Jones
First Energy
300 Madison Avenue
Post Office Box 1911
Morristown, NJ 07962-1991

Jim O'Toole
First Energy
300 Madison Avenue
Post Office Box 1911
Morristown, NJ 07962-1991

John Brunetti, President
John Brunetti Jr., Vice President
Midtown Water
1655 U.S. Highway 9
Red Oak Lane
Old Bridge, NJ 08857

Lawrence Schumacher, President
John Stover, VP & Secretary
Steven Lubertozzi, VP & Treasurer
Montague Water
2335 Sanders Road
Northbrook, Illinois 60062

Henry Schwarz, President
Salvatore Garofalo, VP
Mt. Olive Villages Water
200 Central Avenue
Mountainside, NJ 07092

John Bigelow, President
New Jersey American
131 Woodcrest Road
Cherry Hill, NJ 08034

Bill Beattie, Director Operations
George Mehm, President
John Poulestsos, Vice President
Park Ridge Borough
53 Park Avenue
Park Ridge, NJ 07565

Robert Bebee, Superintendent
Dennis Doll, Chairman
Richard Risoldi, President
Bruce O'Connor, VP & Treasurer
Pinelands Water
1500 Ronson Road
Iselin, NJ 08830-0452

Frank J. Moritz, Director
Ridgewood Village of
13 North Maple Avenue
Ridgewood, NJ 07451

Mark A. Mader
First Energy
300 Madison Avenue
Post Office Box 1911
Morristown, NJ 07962-1991

Lauren Lepkoski
FirstEnergy Corp.
2800 Pottsville Pike
Reading, PA 19612
llepkoski@firstenergycorp.com

Bradley A. Bingaman
FirstEnergy Corp
76 South Main Street
Akron, Ohio 44308
bbingaman@firstenergycorp.com

Andrew Dembia, Esq.
Director, Regulatory Affairs Counsel
New Jersey Natural Gas 1415 Wyckoff Road
Wall, NJ 07719
adembia@NJNG.com

Alexander C. Stern, Esq.
Assistant General Regulatory Counsel
PSEG Services Corporation
80 Park Plaza, T5
Newark, NJ 07102
Alexander.stern@pseg.com

Martin C. Rothfelder, Esq.
Law Department
PSEG Services Corporation
80 Park Plaza, T5G
Newark, NJ 07102-4194

Shawn P. Leyden
PSEG Energy Resources & Trade, LLC
80 Park Plaza, T19
Newark, NJ 07102

Hesser McBride, Esq.
PSE&G Services Corp.
80 Park Plaza, T5
Newark, NJ 07102
Hesser.mcbride@pseg.com

John (Jack) Hosking, President
Roxbury Water
79 Sunset Strip
PO Box 560
Succasunna, NJ 07876

Roger Hall, Vice President
Lawrence Zucker, Controller
Roxiticus Water
1920 Frontage Road
Suite 110
Cherry Hill, NJ 08034

Roger Hall, Vice President
S. B. Water
1920 Frontage Road Suite 110
Cherry Hill, NJ 08034

Daniel T. Stephano, Acting VP
Seaview Water
102 South Manor Avenue
Longport, NJ 08403

Samuel J. Faiello, President
Shore Water
105 23rd Avenue
South Seaside Park, NJ 08752

Michael Walsh, President
Shorelands Water
1709 Union Avenue
Hazlet, NJ 07730

David Simmons, President
Simmons Water
PO Box 900
Branchville, NJ 07826-0900

Frida Salvigsen, President
Tranquility Springs
PO Box 99
West Milford, NJ 07480

Robert Iacullo, President
United Water New Jersey
200 Old Hook Road
Harrington Park, NJ

Stacy A. Mitchell, Esq.
Cozen O'Connor, PC
457 Haddonfield Road, Suite 300
Post Office Box 5459
Cherry Hill, NJ 08002
smitchell@cozen.com

John F. Stanziola
Director, Regulatory Affairs
South Jersey Gas Company
One South Jersey Plaza, Route 54
Folsom, NJ 08037
istanziola@sjindustries.com

Gina Merritt-Epps, Esq.
South Jersey Gas Company
One South Jersey Plaza, Route 54
Folsom, NJ 08037
gmerritt@sjindustries.com

Abbey Greenberg
Public Affairs Specialist- Government &
Regulatory Affairs
South Jersey Gas Company
One South Jersey Plaza, Route 54
Folsom, NJ 08037
agreenberg@sjindustries.com

Nicholas Rizzo, President
Tanya Rovner, Edgewater Assoc
Wallkill Sewer
3331 Rt. 94 South
Hamburg, NJ 07419

Robert Iacullo, President
James Glozzy, VP & Gen Mgr
United Water Arlington Hills
200 Old Hook Road
Harrington Park, NJ 07640

Robert Iacullo, President
James Glozzy, VP & Gen Mgr
United Water Great Gorge
200 Old Hook Road
Harrington Park, NJ 07640

Nadine Leslie, Regional Mgr
James Mastrokalos, Superintendent
United Water Matchaponix
103 Wilson Avenue
Manalapan, NJ 07726

Nadine Leslie, Regional Mgr
United Water Toms River
15 Adafre Avenue
Toms River, NJ 08753

Michael Janel, President
Vernon Water
P.O. Box 376
Pompton Lakes, NJ 07442

Nicholas Rizzo, President
Wallkill Water
3331 Route 94 South
Hamburg, NJ 07419

Tim Davies, President/CEO
Applied Wastewater
2 Clerico Lane
Suite #1
Hillsborough, NJ 08844

William Davis, President
John Hildabrandt, Manager Operations
Aqua NJ
10 Black Forest Road
Hamilton, NJ 08054

Robert Fitzgerald, President
Atlantic City Sewerage
1200 Atlantic Avenue
Suite 300
Atlantic City, NJ 08404

Jan Kokes, President
Crestwood Village Sewer
55 Schoolhouse Road
Whiting, NJ

Thomas Dillon, President
Environmental Disposal
Rt. 202/206
Bedminster, NJ 07978

Robert Iacullo, President
James Glozzy, VP & Gen Mgr
United Water Princeton Meadows
200 Old Hook Road
Harrington Park, NJ 07640

Robert Iacullo, President
James Glozzy, VP & Gen Mgr
United Water Vernon Sewer
200 Old Hook Road
Harrington Park, NJ 07640

Robert Iacullo, President
James Glozzy, VP & Gen Mgr
United Water West Milford
200 Old Hook Road
Harrington Park, NJ 07640

Lawrence N. Schumacher, President
Montague Sewer
2335 Sanders Road
Northbrook, IL 60062

Henry Schwarz, President
Mt. Olive Villages Sewer
200 Central Avenue
Mountainside, NJ 07092

John Bigelow, President
New Jersey American Water
131 Woodcrest Road
Cherry Hill, NJ 08034

Jeffrey Goldstein, VP
Oakwood Village Sewer
308 Vreeland Road
Florham Park, NJ 07932

Robert Risoldi, President
Dennis Doll, Chairman
Bruce O'Connor, VP & Treas
Pinelands Wastewater
1500 Ronson Road
Iselin, NJ 08830-0452

David R. Monie, President – GPM
Roger M. Hall, VP
Larry Zucker, Treasurer
S. B. Sewer
1920 Frontage Road
Suite 110
Cherry Hill, NJ 08034