STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

At a session of the Public Service Commission held in the City of Albany on July 12, 2012

COMMISSIONERS PRESENT:

Garry A. Brown, Chairman
Patricia L. Acampora
Maureen F. Harris
James L. Larocca
Gregg C. Sayre

CASE: 12-M-0282 – In the Matter of Staff's Review of a New York State Electric & Gas Corporation/Rochester Gas and Electric Corporation Security Breach.

ORDER DIRECTING A REPORT ON IMPLEMENTATION OF RECOMMENDATIONS

(Issued and Effective July 18, 2012)

BY THE COMMISSION:

BACKGROUND

In January 2012, New York State Electric & Gas Corporation (NYSEG) and Rochester Gas and Electric Corporation (RG&E) advised the Department that unauthorized parties had obtained access to confidential information of their customers, including Social Security Numbers, dates of birth, and in some cases, financial institution account information. The Department immediately commenced a review of actions taken by NYSEG/RG&E to inform and assist their customers, including efforts to provide accurate information about the potential impact of this security breach and to provide tools to assist customers in identifying instances in which their confidential information was misused. The Department also immediately began an investigation to identify deficiencies in NYSEG/RG&E systems and procedures regarding the protection of confidential customer information, including those that may have contributed to the incident, and to develop recommendations for corrective action.

The attached Staff Report provides a summary of the Department's oversight of the Companies' response to the security breach, as well as an overview of the Department's investigation of the event. Based on the information in the Staff Report, we direct the Companies to report within 60 days of this Order on their progress in implementing Staff's recommendations and include in such report a response to the concerns raised by the Department as to the Companies' plans with regard to the treatment of costs incurred by the Companies including, specifically, their plans on how to treat such costs in NYSEG's and RG&E's 2012 earnings sharing filings.

DISCUSSION AND CONCLUSION

The attached Staff Report details the events that culminated in a January 2012 communication from NYSEG/RG&E to the Department that a compromise of confidential customer information had occurred as a result of unauthorized sharing of that information on the part of a company contractor. After being so informed, the Department began its oversight of the responses of NYSEG and RG&E to address the security breach and its impact on their respective customers, as well as an investigation of the NYSEG/RG&E event.

The Report makes the following conclusions: (1) there is no evidence to date that any confidential customer information was misused; (2) after the Companies became aware of the security breach, NYSEG/RG&E generally took reasonable actions to inform their customers of the potential impact of the breach; (3) several deficiencies in the Companies' systems and practices contributed to allowing the security breach to occur; (4) NYSEG/RG&E have taken sufficient steps to prevent a recurrence of a security breach similar to that which was announced in January 2012; and (5) NYSEG/RG&E are planning a major revamp of their information systems and data protection security.

We do appreciate the Report's conclusions, although we remain concerned that all aspects of this event be addressed by NYSEG/RG&E. While the immediate steps taken by both the Companies seem reasonable, we want to insure that the Companies

follow through to minimize any potential harm to their customers to the maximum extent practicable, especially because the absence of evidence of any immediate harm does not necessarily indicate that no future harm will occur.

The Report indicates that there exist established and well-recognized best practices for the collection and handling of personally identifiable information (PII). Staff referred to these best practices as a guide to determine the scope of its investigation. Staff concludes its findings by making five recommendations for the Companies to better protect their customers' information and facilitate communication with the Department in the event of any future compromise.

In summary, the Report's five recommendations are that NYSEG/RG&E should: (1) Further refine their policies, processes and procedures regarding confidentiality safeguards; (2) Minimize access to the most sensitive PII by maintaining a strictly "need to know" standard for contractors and employees alike; (3) Conduct, at least annually, an incident response exercise simulating a breach of PII data; (4) Establish company protocols for notification of the Department of Public Service in the event of any significant cyber incident involving a possible compromise of customer data; and (5) Promptly implement steps to better ensure the security of all data stored on company mobile computers and removable data storage media.

We believe it is essential that NYSEG/RG&E consider all opportunities to increase their protection of customer PII. Staff's recommendations provide the Companies with important input so that they may continue to implement corrective measures designed to reduce the possibility of a compromise of data of the kind that occurred in January.

Through this order, we are directing NYSEG/RG&E to file within 60 days a report detailing the measures being taken or to be taken to respond to the above recommendations and a timetable for the implementation of these measures. If NYSEG/RG&E concludes that one or more of the above recommendations should not be implemented or should be modified before implementation, their report should so indicate and should state how the failure to implement the recommendation as proposed

is consistent with best practices for the protection of their customers. If NYSEG/RG&E contend that one or more of these recommendations should not be implemented because of costs, their report should indicate how and to what extent the cost savings from not implementing the recommendation exceeds the benefits to customers from implementation.

In addition to the foregoing recommendations, Staff raises the issue of costs that both the Companies incur in responding to this security breach. We share Staff's concern about its understanding of the manner in which the Companies plan to handle the costs incurred, specifically as those plans relate to including some or all of these costs in the Companies' respective earnings sharing calculation.

We believe that Staff rightly expresses concern that including such costs in earnings sharing calculations could result in a potential recovery from ratepayers of certain of those costs. Staff recommends that we require the Companies to segregate and report all of the costs associated with addressing the security breach, including the customer care costs identified above as well as any incremental investigation and remediation costs, as part of their respective 2012 earnings sharing filings, and that the Commission closely scrutinize any proposal to incorporate these costs in the earnings sharing calculation. In this way, in Staff's view, the Companies should be put on notice that they will be required to justify fully the inclusion of any such expenses in their earnings sharing calculations.

We agree Staff's approach may be necessary and expect NYSEG/RG&E's status report to fully address the Companies' plans regarding the recovery, if any, of these costs, including the specific concerns with their earnings sharing calculations raised in the Staff Report. In their 60-day report, NYSEG/RG&E should also address the Companies' intentions for such cost recovery, and, in particular, whether ratepayers would pay, either directly or indirectly, any portion of these costs and the manner in which such cost recovery is consistent with the Companies' current rate plans.

Moreover, consistent with Staff's work with some other utilities, we are expanding the audit of the systems and procedures in place for the protection of

confidential customer information to New York's other regulated utilities. Such entities are on notice that we expect them to cooperate with the Department's ongoing effort to conduct reviews of their customer data protection measures.

Finally, to the extent that Staff refines its standard and best practices related to protecting PII as a result of such expanded review and audit, NYSEG/RG&E should be aware that Staff may make further recommendations in addition to those contained in the attached Staff report.

The Commission orders:

1. New York State Electric & Gas Corporation/Rochester Gas & Electric Corporation are directed to file a report, as described more fully in the above Discussion and Conclusion, not more than 60 days after the issuance of this Order informing the Commission of their progress in implementing the Report's recommendations. In such report NYSEG/RG&E should also fully address their plans regarding the costs incurred in investigating and addressing this event, including, but not limited to, addressing the specific concerns with their earnings sharing calculations raised in the Staff Report. Moreover, NYSEG/RG&E should explain how their respective approaches are in conformity with the requirements of earnings sharing with their respective rate plans.

2. This proceeding is continued.

By the Commission,

Jaclyn A. Brilling
Digitally Signed by Secretary
New York Public Service Commission

(SIGNED) JACLYN A. BRILLING
Secretary

STATE OF NEW YORK
DEPARTMENT OF PUBLIC SERVICE

New York State Electric & Gas Corporation and Rochester Gas and Electric Corporation Customer Information Security Breach
Case 12-M-0282

Staff Report

July 2012

SUMMARY

In January 2012, New York State Electric & Gas Corporation (NYSEG) and Rochester Gas and Electric Corporation (RG&E) advised the Department that unauthorized parties had obtained access to confidential information of their customers, including Social Security Numbers, dates of birth, and in some cases, financial institution account information. The Department immediately commenced a review of actions taken by NYSEG/RG&E to inform and assist their customers, including Company efforts to provide accurate information about the potential impact of this security breach and to provide tools to assist customers in identifying instances in which their confidential information was misused. The Department also immediately began an investigation to identify deficiencies in NYSEG/RG&E systems and procedures regarding protection of confidential customer information including those that may have contributed to the incident, and to develop recommendations for corrective action.

This Report provides a summary of the Department's oversight of the Companies' response to that security breach as well as an overview of the Department's investigation of the event. The major conclusions are: (1) there is no evidence to date that any confidential customer information was misused or that the individuals who had unauthorized access to that data had malicious intent; (2) after the Companies became aware of the security breach, NYSEG/RG&E generally took reasonable actions to inform their customers of the potential impact of the breach, and to provide customers with free services to help identify instances in which customer information was misused; (3) several serious deficiencies in NYSEG's and RG&E's systems and practices contributed to the security breach, including the absence of formal procedures applicable to contractors regarding protection of confidential customer information, inadequate limitations on subcontracting by a contractor, and the absence of requirements that systems development and testing be conducted using encrypted or fictitious data; (4) NYSEG/RG&E have taken sufficient steps to prevent a recurrence of a security breach similar to that which was announced in January 2012, and continue to implement Staff's recommendations; and (5) NYSEG/RG&E are planning a major revamp of their information systems and data protection security, for which they expect to issue an RFP

by July 1, 2012, award a bid in the third quarter of 2012 and complete work by the end of 2013.

The Department will continue to review and assess NYSEG's and RG&E's progress in implementing Staff's recommendations and completing their overhaul of their information systems and data protection security, and will report any concerns to the Commission. While NYSEG and RG&E have committed they will not seek recovery of the costs associated with this remedying breach, they will include the costs in their earnings sharing mechanism which could potentially reduce customer's share of future excess earnings. Accordingly, we also recommend that NYSEG and RG&E be required to report the costs associated with this breach and justify their inclusion in any earnings sharing calculations.

BACKGROUND

On or about January 9, 2012, NYSEG and RG&E concluded that there had been unauthorized access to their computer systems containing confidential customer information. On January 23, 2012, NYSEG and RG&E advised the Department that a compromise of confidential customer information had occurred as a result of unauthorized sharing of that information on the part of a third-partycontractor. The Companies' Information Technology (IT) staff had noticed unusual and suspicious network traffic that appeared to be from sources using the contractor's access credentials. NYSEG and RG&E immediately conferred with the contractor and required that the contractor surrender its company access codes.

NYSEG and RG&E further advised that Verizon Business had been retained to conduct an investigation into the cause of the compromise, identify its source, collect evidence, and identify what, if any, broader exposure of sensitive data may have occurred.

Verizon Business found that the contractor had been subcontracting out some of the work it was to perform for NYSEG and RG&E. The contractor gave NYSEG and RGE's access credentials to several persons working for the contractor who were located outside

the United States and accessing NYSEG and RG&E systems from there. Verizon identified the factors that allowed the contractor to give access to others unauthorized to have such access, and how they were able to gain entry to company databases.

Verizon Business did not find any evidence of wrongful intent on the part of the contractor or its subcontractors. There has been no indication to date that the compromised data has been used for malicious or fraudulent purposes.

Following a subsequent briefing by NYSEG and RG&E to Department senior staff, and a sharing of the Verizon Business report, it was determined that the Office of Electric, Gas and Water's Utility Security Section should conduct a review of the full range of NYSEG and RG&E's information systems policies, procedures and technologies that affect or potentially affect the safeguarding of customer data. This review was intended to determine whether any of the cyber security deficiencies that contributed to the compromise in question had been remedied. Further, the review would analyze whether the information system structure of the Companies was sufficiently protected, so as to minimize the possibility of any unauthorized access to sensitive customer information, both from within and outside the Companies.

NYSEG/RG&E ACTION TO INFORM AND PROTECT CUSTOMERS

On January 23, 2012, NYSEG/RG&E began to notify customers of the incident. The Companies mailed more than 1.8 million notification letters to NYSEG and RG&E's residential, commercial and industrial customers to provide information about the breach, how customers may be affected, and the actions that customers should take to determine if their confidential information has been misused. The Companies' also announced that they were offering NYSEG and RG&E customers the option of one year of credit monitoring service from Experian, one of the nation's largest credit reporting entities, at no charge. That service includes a copy of the customer's credit report, a daily monitoring service that provides alerts regarding suspicious activity, and an insurance policy to help cover certain costs in the event that identity theft occurs. The Companies

also augmented its call centers to address an expected increase in call volumes, issued press releases, and provided relevant information on the home pages of its websites.

Shortly after public announcement of the security breach, the Department recognized that the free services that NYSEG/RG&E offered through Experian were provided for residential customers only, and requested that the Companies provide comparable services to non-residential customers. The utilities promptly agreed to do so. Approximately 420 non-residential customers have signed up for those free services.

Staff closely monitored the Companies' activities and customer concerns. We requested and received weekly reports regarding customer inquiries made to the Companies and Experian. More than 65,000 customers have contacted NYSEG/RG&E and more than 600,000 customers have contacted Experian about this issue.

The Department also requested and received weekly reports regarding the number of NYSEG/RG&E customers who enrolled in the free credit monitoring service. Approximately 160,000 residential customers have enrolled in the free credit monitoring service. NYSEG/RG&E had planned to end the ability of customers to enroll in the free credit reporting service as of the end of April 2012. In response to the Department's request, the Companies extended free enrollment in the Experian services through mid-July 2012.

Staff also received reports from Experian regarding the number of new fraud cases that Experian opened for NYSEG/RG&E customers and the disposition of such cases. Experian opens a case when the customer identifies activity regarding his/her accounts that the customer cannot readily explain. Cases are closed when the issue causing the opening has been resolved to the satisfaction of the customer. Through May 31, Experian opened 297 fraud cases for NYSEG/RG&E customers and has closed them all. NYSEG/RG&E reports that they have no information that indicates that there has been any inappropriate use of customer data attributable to this incident.

COSTS INCURRED BY NYSEG/RG&E AND ASSOCIATED RATEMAKING

NYSEG/RG&E reported that they have incurred $3.99 million of incremental costs (through April 2012) to implement the programs described above in order to respond to their customers' situation. According to NYSEG/RG&E, the majority of these costs ($3.2 million) were incurred for customer account monitoring activities. NYSEG/RG&E report that of the customer accounts it monitored, 69% were NYSEG's customers and 31% were RG&E customers, thus it plans to allocate the majority of costs to NYSEG. In its June 22, 2012 response to Staff questions, the Companies indicate that they "will record costs incurred as operating expenses" and "will not be requesting any separate reimbursement or deferral of such costs for future recovery from customers." However, the Companies also state that they will "include such costs in each Company's respective earnings sharing calculation."

Since these costs have been charged to operating expenses, they will reduce the Companies' profits during 2012. Under the terms of the Companies 2010 Rate Order,[1] earnings in excess of a 10.6% return on equity (ROE) are shared equally[2] between customers and shareholders. Since the Companies indicate that they will include such costs in their respective earnings sharing calculations, this may result in a potential recovery of up to 50% (or more) of such costs should the Companies have shared earnings in the rate year ending December 31, 2012. [3]

Given that the Companies intend to include costs attributable to the security breach in their respective earnings sharing calculations, we recommend that the Commission

---

[1] See Cases 09-E-0715 et al., Rochester Gas and Electric Corporation, Order Establishing Rate Plan (issued and effective September 21, 2010).

[2] For 2012, earnings above 11.35% are shared 85% with customers and 15% is retained by the Companies.

[3] For the first rate year 2011, RG&E's electric department reported a return on equity of 10.74% which exceeded its 2011 ROE target of 10.3% by 44 basis points and produced shared earnings of $1.6 million (unaudited). The other operations were between $3 million and $16 million (81 and 131 basis points) below the earnings sharing target of 10.3% return on equity. Pursuant to the terms of the JP, the ROE target for earnings sharing increases to 10.6% for 2012.

require the Companies to segregate and report all of the costs associated with rectifying the security breach, including the customer care costs identified above, as well as any incremental investigation and remediation costs, as part of their 2012 earnings sharing filing. Should those costs affect the level of earnings sharing with customers (including bringing excess earnings to beneath the earnings sharing target of 10.6%) staff recommends that the Companies be put on notice that they will be required to justify the inclusion of any such expenses in their earnings sharing calculations.

SCOPE OF THE DEPARTMENT'S INQUIRY REGARDING PROTECTION OF PERSONALLY IDENTIFIABLE CUSTOMER INFORMATION

Established and well-recognized best practices for the Protection of Personally Identifiable Information (PII) were used to establish the scope of the review conducted by the Department's Utility Security Section.

These best practices were drawn from the National Institute of Standards and Technology (NIST), "Guide to Protecting the Confidentiality of Personally Identifiable Information" (2010). Also referenced for this purpose were the rules for the protection of student information required under the federal Family Educational Rights and Privacy Act (FERPA). Many of the requirements for the protection of student privacy under that act are directly pertinent and readily applicable to the protection of business customer privacy, as well.

From the NIST guidelines and the FERPA rules, staff formed a series of questions grouped into eight subject categories listed below. Staff submitted the questions to NYSEG/RG&E with instructions to supply answers along with documentation to support those answers. Staff later conducted an on-site review of the Companies' responses and documents, and interviewed appropriate NYSEG/RG&E officials and employees for verification and clarification as necessary

The eight subject areas of inquiry were:

Corporate Accountability

In this area of review staff sought to identify the nature and extent of those functional units within NYSEG/RG&E specifically charged with responsibility for protecting customer privacy. Further, staff looked for confirmation that the customer privacy responsibility was fully accepted and shared by senior management and executive level company officials. Written policies were reviewed and documents in support of those policies were examined. NYSEG/RG&E officials were interviewed.

Policies, Procedures and Guidelines

This section of the inquiry examined more specific company policies and procedures, supported by documentation, that govern data access, data transfer, data restriction, data retention, deletion and destruction, and other related matters. Also in this section, policies and documentation were reviewed regarding breach response and notification procedures.

Training, Education and Outreach

Here staff examined the programs in place at the Companies for internal and external outreach and communication regarding privacy and information security. Requirements, or the lack thereof, for mandatory training for all employees and vendors/contractors were examined. Staff reviewed the means by which, and the frequency with which, NYSEG/RG&E ethical standards and codes of conduct are communicated to employees and vendors alike.

Credentialing (Background Screening)

Under this section of review, staff examined the regularly required steps taken by NYSEG/RG&E to be sure of the identity and good integrity of employees, prospective employees, and contractors, and to confirm the identity of customers who interface with NYSEG/RG&E using the Companies online services.

Personally Identifiable Information (PII) Confidentiality Safeguards

In this area of review staff looked at how NYSEG and RG&E handle PII in a variety of important ways -- how NYSEG/RG&E categorize PII, collect it, retain it, segregate it, and periodically review their inventory of PII and destroy that which no longer has any practical business usefulness. Additionally, staff review sought to determine that separate and fully segregated data systems, not containing actual customer data, were used for purposes of systems development and testing.

Network Security

This area of review included an examination of all common network security policies, practices and equipment utilization. Database and electronic traffic monitoring, data encryption, firewalls, antivirus software and malware protection, vulnerability scans, independent third-party assessments, patch management programs, password protocol and discipline, and compartmentalization of employee access rights, etc. were among the specific subjects investigated. NYSEG/RG&E staff was interviewed regarding these practices and measures and produced documentation to confirm their responses.

Physical Security

Staff reviewed physical security measures in place and in force at NYSEG/RG&E as they pertain to the protection of private customer data. The elements of examination in this area mostly concern restrictions on personnel, visitor and contractor access to spaces that house Information systems equipment and terminals.

Incident Response for Possible Compromise of Customer Data

This last area of review concerned the identification and adequacy of plans and protocols in place at NYSEG/RG&E to respond promptly and effectively to a known or suspected instance of unauthorized access to customer data. Also, staff examined the extent to which such plans and protocols were tested through exercises and drills.

SUMMARY OF FINDINGS OF THE DEPARTMENT'S SECURITY REVIEW

While inadequacies in any of the subject areas listed above could result in or contribute to a compromise of sensitive information, the shortcomings that allowed the NYSEG/RG&E problem with its contractor to occur were most concentrated in the area of PII Confidentially Safeguards.

1.) As a matter of policy at NYSEG/RG&E, the use and collection of PII is limited to authorized personnel. However, that policy had not been sufficiently formalized in either company documentation or day-to-day practice. Nor had NYSEG/RG&E followed a practice of carefully communicating to all employees and to all contractors the importance of their ethical and legal obligation to protect customer privacy. NYSEG/RG&E have not been sufficiently explicit in communicating with contractors regarding the obligation they have in protecting confidential information. NYSEG/RG&E are presently developing a program with specific implementing procedures for greater compartmentalizing of employee/contractor access to sensitive customer information. These were serious and aberrational deficiencies.

2.) NYSEG/RG&E have not followed a practice of monitoring the total quantity of PII information that it has collected in its databases and periodically identifying such data that should no longer be retained and therefore destroyed. Their failure in this regard provided a larger amount of PII able to be compromised than should have existed when its systems were breached.

3.) In collecting PII in the normal course of business NYSEG/RG&E have not sufficiently sought to segregate such information into "low-impact" or "high-impact" information (such as Social Security numbers). NYSEG/RG&E advised that they are presently investigating options for this kind of segregation and compartmentalization of more sensitive customer information, most subject to abuse as a result of an unauthorized release or theft

4.) NYSEG/RG&E had been insufficiently attentive to the need to use only "dummy data" or other techniques for protecting against exposure to PII when conducting systems development and testing.

5.) NYSEG/RG&E's inventory of portable (laptop) business computers are vulnerable because of certain security deficiencies. The accidental loss or theft of a NYSEG/RG&E portable computer is an ever present possibility. The result can be a serious compromise of sensitive customer and operational data.

CORRECTIVE MEASURES IMPLEMENTED

To preclude the possibility of a compromise of data of the kind that occurred in January, NYSEG/RG&E have tightened and restricted contractor access to customer data.

1.) Corporate owned portable computers are no longer being utilized by contractors.

2.) Contractors may now only log-in remotely through a secure server, negating the possibility of a contractor sharing log-in credentials with others.

3.) File uploads and downloads to any memory device are administratively disabled and no contractors have the ability to change that configuration.

4.) All contractors are now authenticated when accessing the secure server with multiple layers of validation.

5.) Access to the secure server requires encryption.

6.) All sensitive data, including PII, has been removed from company development and testing systems. All contractors have access only to those systems and do not have access to business and operations systems.

Going beyond the specific vulnerabilities revealed by the January incident, NYSEG/RG&E have assembled a working group within the Companies to comprehensively address data privacy issues and solutions.

The Corporate Security Group of Iberdrola, USA has solicited the assistance of systems security consultants and vendors to evaluate ways to improve the use and collection of PII, and the full range of data and systems security needs. It is expected that an RFP will be issued for the new "Iberdrola Information Security Long Term Framework" by July 1, 2012, with a bid to be awarded in the third quarter of 2012. Work on development and implementation of that new framework will begin in late 2012 and be completed by the close of 2013.

RECOMMENDATIONS

NYSEG/RG&E should:

1.) Further refine policies, processes and procedures regarding confidentiality safeguards. It must fully assess all sensitive information stored on company systems to determine how much has been aggregated, and destroy any data that is not required for business purposes. This will help reduce both the risk and impact of unauthorized exposure by any possible means.

2.) Minimize access to the most sensitive PII, such as Social Security numbers, by maintaining a strictly "need to know" standard for contractors and employees alike.

3.) Conduct, at least annually, an incident response exercise simulating a breach of PII data. This would help to measure the adequacy of the involvement of all stakeholders from across NYSEG/RG&E and the sufficiency of existing plans and procedures.

4.) Establish a NYSEG/RG&E protocol for notification of the Department of Public Service in the event of any significant cyber incident involving a possible compromise of customer data. Following determination (under current company policy) by designated executive and legal officers of the Companies that an IT "critical issue" involving PII has occurred, NYSEG/RG&E should notify the Department within 48 hours of such determination.

5.) Promptly implement steps to better ensure the security of all data stored on company mobile computers and removable data storage media.

Staff has provided these recommendations to NYSEG/RG&E. Some recommendations will be implemented in the near term and the remaining recommendations will be incorporated in the "Information Security Long Term Framework" overhaul project (cited above) currently commencing at NYSEG and RG&E. Staff will continue to monitor their implementation by NYSEG/RG&E and report back to the Commission as needed.

WORK WITH OTHER UTILITIES

Following staff's NYSEG/RG&E review, in order to be sure that the privacy of customer data was being properly assured at the other regulated energy utilities, the Department notified each company that we would be conducting reviews of their customer data protection measures. Each company was instructed to respond to the same set of inquiries as was issued to NYSEG/RG&E and to prepare responses in anticipation of an on-site evaluation of those responses and interviews with appropriate company personnel. The review process focused on best practices and included the issues identified in the NYSEG/RG&E review.

Staff has completed on-site reviews of the policies, practices and procedures for the protection of customer PII at Consolidated Edison and Orange and Rockland, National Grid, and National Fuel Gas. Each company fully cooperated in the conduct of these reviews, making available all documentation and personnel as requested. A comparable

review of Central Hudson Gas and Electric is underway and will be completed shortly. No significant vulnerabilities requiring immediate corrective action were discovered.

Findings to date from these reviews indicate that best practices for the protection of customer information are being generally observed. However, areas for improvement have been identified. For example, some document retention and destruction protocols need to be adhered to more diligently and internal controls on personnel access to data need to be stricter in some instances.

Staff will share its recommendations with the utilities. We expect the utilities to implement these recommendations. Should our follow-up review show utilities are not implementing the recommendations we make, we will report back to the Commission as needed.