STATE OF NEW YORK DEPARTMENT OF PUBLIC SERVICE
THREE EMPIRE STATE PLAZA, ALBANY, NY 12223-1350
www.dps.ny.gov

September 20, 2012

Chief Operating Officer:

Re: 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

As utility customer transactions and service delivery become steadily more dependent on electronic communications and data storage, the need to maintain the security of customer privacy grows.

The Department of Public Service recently investigated events at one New York utility involving the unauthorized sharing of data systems access credentials by a company contractor that resulted in unauthorized access to the Personally Identifiable Information (PII) of some company customers. The Commission directed that the Department's review and audit be expanded to New York's other regulated utilities.

The Department's review will serve to ensure that sufficient steps are being taken to better prevent a possible compromise of utility-held customer information. In furtherance of such review, each utility receiving this letter is directed to identify and, in accordance with the procedures below, disclose to Department staff the full range of protections the company employs to safeguard customer information.

The areas pertinent to PII protection we would include in our review include:

- Policies, procedures and guidelines
- Credentialing and screening of employees, contractors and vendors.
- Identification of appropriate security technologies and other security features that have been or are planned to be deployed for the better protection of customer information

- Corporate accountability
- Evaluation of the adequacy and frequency of internal audit of IT systems operations and programs
- Internal training re customer privacy protection
- Physical security of data systems and data systems space
- Practices in furtherance of customer advocacy and transparency

Enclosed for your reference and use is a “Personally Identifiable Information Security Standards Review Worksheet” prepared by Department Staff for the conduct of these reviews. This worksheet elaborates more specifically on the general subject areas listed above. The best practices for the protection of PII, compiled by Department Staff, are fully encompassed in the worksheet questions. To best protect potentially sensitive or confidential information we are directing that your company retain the completed worksheet, and to make it available for the Department’s on-site review.

The completed worksheet should be available for discussion when Department Staff visits your offices. Alternatively, for utilities that have an office, agent, or associate in the Albany area, please provide such with a copy of the worksheet so that Department Staff may inspect it there to determine if any further on-site follow-up is necessary.

Finally, as you complete the worksheets, please identify any recent specific goals and measures your company has formulated for improved PII protection prior to your receipt of this letter, as well an expected timeline for implementing any such measures.

Please have the appropriate person in your organization contact John J. Sennett, the Department’s Chief of Utility Security, (518) 427-1431, by Wednesday, October 31, 2012 for follow-up on this inquiry and to schedule an on-site staff review and evaluation of your documentation prepared in response to this letter.

By the Commission,

/s/

JACLYN A. BRILLING
Secretary

New York State Department of Public Service
Utility Security

COMPANY NAME

____

Personally Identifiable Information Security Standards Review Worksheet

DATE______________________________

Compliance Finding Summary

The information contained within this transmittal should be treated as CONFIDENTIAL and PROTECTED from public disclosure under applicable laws. Any unauthorized disclosure or dissemination of this information is strictly prohibited.

Supporting Material/Documentation

Security Expert – Name, Title, Organization, Phone, Email
1.
2.
3.
4.

* Add additional rows as necessary

	Applicable Document(s), Page and Section	Date and/or Version
R1.	1.	
R2.	2.	
R3.	3.	
R4.	4.	
R5	5.	
R6	6.	
R7	7.	

The information contained within this transmittal should be treated as CONFIDENTIAL and PROTECTED from public disclosure under applicable laws. Any unauthorized disclosure or dissemination of this information is strictly prohibited.

R8	8.	

Note: This documentation section is completed by the reviewed entity prior to the Review. All documentation listed in this table must be available the day of the Review. Organization responses may reference documents by their Item number. Add additional rows as necessary.

R1 - Corporate Accountability

1. Does the organization have an office or function dedicated to privacy compliance?

2. Does the organization have persons or committees at various levels of the organization that set, direct and implement information security and privacy strategy, policy and initiatives?

4. Does the organization have senior leaders who are accountable for administrative, technical and physical privacy and information security safeguards?

5. Does the organization have a person or committee responsible for creating privacy and information security policies?

6. Does the organization have policies that document accountability for each of the persons/committees/working groups?

7. Does the organization have assigned representatives within each of its business functions to assist with the implementation of privacy, information security and compliance policies and procedures (information owners)?

R1 Organization Response

Note: Organizational response is completed by the reviewed entity prior to the Review.

R1 Review Team Notes

R2 – Policies and Procedures and Guidelines

1. Does the organization have published privacy principles or a published privacy policy?

2. Does the organization have policies, procedures and guidelines that address compliance with privacy and information security laws and/or regulations?

3. Does the organization have Web site privacy policies for its Web sites?

4. Does the organization have policies that govern data access?

5. Does the organization have policies that govern data protection?

6. Does the organization have policies that govern data transfer?

7. Does the organization have policies that govern data transport?

8. Does the organization have policies that govern data restriction?

9. Does the organization have policies that govern data retention?

10. Does the organization have policies that govern data deletion and destruction?

11. Does the organization have policies that govern data classification?

12. Does the organization have policies that govern breach response and notification?

13. Does the organization have a policy on incident response?

R2 Organization Response

Note: Organizational response is completed by the reviewed entity prior to the Review.

The information contained within this transmittal should be treated as CONFIDENTIAL and PROTECTED from public disclosure under applicable laws. Any unauthorized disclosure or dissemination of this information is strictly prohibited.

R2 Review Team Notes

R3 – Training, Education and Outreach

1. Does the organization have a program for internal and external outreach and communication regarding privacy and information security?

2. Does the organization require annual mandatory training for all employees and vendors/contractors on privacy? If not annually, how often?

3. Does the organization require annual mandatory training for all employees and vendors/contractors on information security? If not annually, how often?

4. Does the organization require annual mandatory training for all employees and vendors/contractors on code of conduct? If not annually, how often?

5. Does the organization require annual mandatory training for record retention and deletion? If not annually, how often?

6. Does the organization require its employees and vendors/contractors to adhere to a code of conduct?

7. Are employees and vendors required to pass each training program with a certain percentage of questions answered correctly?

8. Are there consequences for not successfully completing training?

9. Are privacy and information security policies communicated to employees and vendors/contractors on a regular basis? How?

10. Does the organization send out regular privacy reminders to its employees and vendors/contractors?

11. Does the organization have a program to notify stakeholders on key privacy and information security programs and enhancements?

12. Does the organization have hotlines for employees, vendors/contractors, customers and consumers to report suspicious behavior? What are they?

12. Does the organization have liaisons with regulators? Law enforcement? Privacy advocates?

R3 Organization Response

Note: Organizational response is completed by the reviewed entity prior to the Review.

R3 Review Team Notes

R4 – Credentialing (Background Screening)

Employees

1. Does the organization credential its employees?

2. Does the credentialing process require criminal, and credit checks?

3. Does the organization have a re-credentialing program for employees that include a criminal background check? How frequently?

Customers

1. Does the organization credential its customers?

2. Does the organization centralize its credentialing of customers to ensure consistency and security of the process?

3. Does the organization follow a credentialing checklist or process that verifies each customer's legitimacy and permissible purpose?

4. Does the organization require that each customer pass its credentialing process?

5. Does the organization require that each customer pass its site visit process?

7. Does the organization re-credential its customers?

The information contained within this transmittal should be treated as CONFIDENTIAL and PROTECTED from public disclosure under applicable laws. Any unauthorized disclosure or dissemination of this information is strictly prohibited.

Vendors/Contractors

1. Does the organization assess/credential its vendors/contractors?

2. Does the organization re-credential its vendors/contractors? How frequently?

3. Does the credentialing process for vendors/contractors who will have access to sensitive information require criminal, and credit checks?

R4 Organization Response

Note: Organizational response is completed by the reviewed entity prior to the Review.

R4 Review Team Notes

R5 – PII Confidentiality Safeguards

1. Does the organization categorize its PII based on impact to PII confidentiality?

2. Does the organization minimize the use, collection, and retention of PII?

3. Does the organization consider the total amount of PII?

4. Does the organization properly segregate high impact PII, such as SSNs, on separate systems, as well as obfuscate the data?

5. Does the organization employ separate systems for development, testing, Q&A, and production purposes?

5. Does the organization use 'dummy data' (not actual customer PII), or other techniques to protect PII, on its development, test and Q&A systems?

The information contained within this transmittal should be treated as CONFIDENTIAL and PROTECTED from public disclosure under applicable laws. Any unauthorized disclosure or dissemination of this information is strictly prohibited.

5. Does the organization regularly review its holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting the organization's business purpose and mission?

6. If PII is no longer relevant and necessary, then is the PII properly destroyed? How?

R5 Organization Response

Note: Organizational response is completed by the reviewed entity prior to the Review.

R5 Review Team Notes

R6 – Network Security

1. Does the organization utilize technology enhancements to aid in network security?

2. Does the organization monitor access to sensitive information?

3. Does the organization utilize technologies such as encryption and data classification to protect sensitive information?

4. Are all databases and other data repositories containing sensitive information, including all organizational servers, secured behind firewalls?

5. Does the organization employ anti-virus software and malware protection?

6. Does the organization run periodic vulnerability scans of its critical infrastructure and have strict requirements on addressing issues found? How often?

7. Does the organization have an independent network security assessment performed at least annually?

8. Does the organization maintain a patch management program that is designed to address desktop and server patches within a reasonable time of their release? How soon?

9. Does the organization maintain technical standards for system setup and configuration and assess a sample of systems on a regular basis? How often?

10. Is the organization compliant with the Payment Card Industry standards for credit card data protection? Note: The PCI Security Standards Council is an independent body formed to develop, enhance, disseminate and assist with implementation of security standards for payment account security.

11. Does the organization require employee passwords to be changed least quarterly and require complex passwords? What are the password requirements?

12. Does the organization implement intrusion detection/prevention systems at its Internet perimeter, and monitor these devices 24/7 for malicious activity?

13. Does the organization have an established Web vulnerability assessment program that focuses on finding and eliminating risks with Web-based applications?

15. Does the organization have tools and processes that help automate the user identity management lifecycle (e.g., removing access immediately on employee termination)?

16. Does the organization ask employees a secret security question in the event they are locked out of their computers?

R6 Organization Response

Note: Organizational response is completed by the reviewed entity prior to the Review.

R6 Review Team Notes

R7 – Physical Security

1. Does the organization have appropriate physical security controls to safeguard data?
2. Does the organization monitor employee access to buildings?
3. Does the organization require escorting of visitors?
4. Does the organization have physical security policies that require employees and contractors maintain a “clean desk” to protect exposure of sensitive data?
5. Does the organization have policies and procedures designed to help protect property and assets from unauthorized acquisition, loss or damage?
6. Does the organization restrict access to removable and mobile media for employees?
7. Does the organization require all laptops to be encrypted?

R7 Organization Response

Note: Organizational response is completed by the reviewed entity prior to the Review.

R7 Review Team Notes

R8 – Incident Response for PII Breaches

1. Does the organization have PII breaches included in their incident response plans?
2. Has the organization established clear roles and responsibilities to ensure effective management when an incident occurs? Management of incidents involving PII often

requires close coordination among personnel from across the organization, such as the CIO, CPO, system owner, data owner, legal counsel, and public relations officer.

3. Does the organization have a PII breach notification plan? The plan should include notifications to law enforcement, financial institutions, affected individuals, and appropriate government agencies (local, state, and federal). Depending on the severity of the breach, some or all may require notification.
4. Has the organization established a committee or person responsible for using the breach notification policy to coordinate the organizations response?
5. Are the PII breach response plan policies and procedures communicated to applicable staff via training and awareness programs?
6. Does the organization conduct test exercises on a periodic basis to simulate an incident to assess their response plans? How often? May include tabletop exercises.
7. Does the organization conduct a post-mortem evaluation of the test exercise, and update policies and procedures from lessons learned?
8. Is information learned through detection, analysis, containment, and recovery collected for sharing within the organization, and with relevant entities, to help protect against future incidents?

R8 Organization Response

Note: Organizational response is completed by the reviewed entity prior to the Review.

R8 Review Team Notes

The information contained within this transmittal should be treated as CONFIDENTIAL and PROTECTED from public disclosure under applicable laws. Any unauthorized disclosure or dissemination of this information is strictly prohibited.