NEW YORK RETAIL CHOICE COALITION AND SUPPORTING ESCOS
Case No. 18-M-0376

Questions for DSA Technical Call scheduled for August 1, 2018

Opening

We are technology professional and glad to have the opportunity to provide feedback and questions. While we wish we had started a collaborative dialogue at an earlier point, we want to reiterate that we truly value customer security, data protection and industry resiliency. We believe that a collaborative process, much like NAESB and GISB before it undertook to take a cross company approach at security and standardization, is required as part of ensuring a robust and long surviving set of standards that will create an environment that ensures NY has strong security and resiliency in their distribution grid and power operations. Given the quick timeframe to develop these questions, we reserve the right to come back with further questions or clarifications based on Utility responses.

Questions

1. In order to better ensure that we are focused on the right risks, was the robust risk assessment performed by the utilities internal team or a third party and what are the results of that assessment? What are the types of risks identified by that assessment that are being mitigated as part of the DSA and Self Attestations?

2. Hearing from DPS Staff that a primary goal is grid security and resiliency, what threats do ESEs currently present to grid security (i.e. how can an ESE data breach result in a blackout or other systemic failure)?

3. Given that the EDI providers only interact with the utilities through ANSI X12 EDI (text files) being transmitted via GISB approved encrypted mechanisms, and considering the controls the Joint Utilities have in place to parse the X12 data, how can malware traverse the utility systems or propagate through UNIX/DOS level text files (with no markup language or other code) to comprise grid, billing or other utility systems?

4. Given that the other method of interaction between ESEs and Utilities are systems like RAIS and TCIS:
    a. Are these reporting systems segmented and in separate security zones from the primary operational systems at the utility?
    b. What are the risks to these systems and how are they mitigated by the security attestations?
    c. Do ESE credentials for JU portals grant anything more than limited read-only access to JU systems?

5. Using the published NY EDI specification document. Please categorize the impact of breach for each data point transmitted from Utilities to ESEs as:
    a. Potential impact to the grid;
    b. Potential financial loss to customer;

c. Warrant credit-monitoring or similarly costly mitigation efforts;
d. Specify other potential damages

6. Given the nature of the ESG Incident, being a ransomware attack which caused ESG to not be able to communicate EDI files, that caused a material portion of the NY Market to not transmit data and prevented NY customers to be invoiced accurately; How has the risk of a similar event occurring been mitigated by the proposed DSA and Self Attestations?

7. Internally, when there is a 'single point of failure' in a business process or infrastructure, the solution is to mitigate that with redundancy. Given that a ESE can only have one registered inbox / EDI location, has the NY Utilities considered allowing ESEs to have more than one connection to their systems to allow for continued operation if one part of the process fails? (in this case the EDI provider).

8. Regarding the requirement for notification of security incidents:
    a. What classifications/level of security breach would warrant triggering this notification? For example, Do the utilities want to be notified of every attempted phishing email received by ESEs?
    b. Due to the monetary impact potential to ESEs in the event the incident is on the Utility side of the connection, what is the reason this clause does not also require the Utility to inform the interconnected ESEs of security breaches or incidents?

9. In the interest of information sharing and dialog, what is your security / risk based assessment process for enterprise cloud environments, such as Microsoft Azure, Amazon Webservices, and Google Cloud, for data hosting environments? What criteria are the utilities applying for the selection of storage facilities?
    a. How are global LDCs (i.e., utilities) doing business in NY planning to meet the proposed storage USA only storage limitation?
    b. Do the utilities distinguish between primary and long term backup location security requirements?

10. What Third Party Monitors and alerts for anomalous cyber activity are currently utilized by the Utility?

11. Are any Utility systems currently certified SOC II compliant? Are any Utility systems not currently SOC compliant currently in the process of becoming so? Are the ESE facing systems included in the scope of the SOC II Audit?

12. Explain how a Third Party of the ESE, with no direct access to the Utility systems, presents grid level (and therefore monetary risk equivalent) to an ESE or EDI Provider?

13. Will the Utilities commit to using opportunistic TLS encrypted connections, and both enforce client connections via TLS?

Isn’t it sufficient for non-secure/encrypted e-mails received from a customer/potential customer or from some other third party (like the PSC) containing sensitive/potentially confidential

information such as a customer utility account number to be considered "secure" if an ESCO's employee happens to read such e-mail on his/her phone that is password protected? ConEd representatives mentioned some new language in the DSA that would prohibit receipt/reading of such e-mails containing such sensitive information on a mobile device such as a phone or laptop if is not "encrypted", but is that simply not impractical considering that many ESCO customers and even the PSC currently do not have e-mail encryption capabilities?