EXHIBIT 1

STAFF OF THE DEPARTMENT OF PUBLIC SERVICE
RESPONSE TO INTERROGATORY/DOCUMENT REQUEST

Orange & Rockland Utilities, Inc.
Cases 18-E-0067 & 18-G-0068

Requesting Party: Deborah Kopald
Set No.: 1
Request No.: Kopald-14
Responding Witness: Staff Policy Panel
Date of Response: August 21, 2018

Question:
Please explain the DPS' understanding of how the smart meter data works to "evaluate the impact of electric vehicles"?

Response:

Staff objects to this interrogatory on the grounds that it seeks information that is beyond the scope and not reasonably calculated to lead to admissible evidence in the instant proceedings.

EXHIBIT 2

STAFF OF THE DEPARTMENT OF PUBLIC SERVICE
RESPONSE TO INTERROGATORY/DOCUMENT REQUEST

Orange & Rockland Utilities, Inc.
Cases 18-E-0067 & 18-G-0068

Requesting Party: Deborah Kopald
Set No.: 1
Request No.: Kopald-15
Responding Witness: Staff Policy Panel
Date of Response: August 21, 2018

Question:
Please explain the DPS' understanding of how the smart meter data works to "reduce electric and gas system losses" and pleas estimate the monetary value of that.

Response:

Staff objects to this interrogatory on the grounds that it seeks information that is beyond the scope and not reasonably calculated to lead to admissible evidence in the instant proceedings.

EXHIBIT 3

STAFF OF THE DEPARTMENT OF PUBLIC SERVICE
RESPONSE TO INTERROGATORY/DOCUMENT REQUEST

Orange & Rockland Utilities, Inc.
Cases 18-E-0067 & 18-G-0068

Requesting Party: Deborah Kopald
Set No.: 1
Request No.: Kopald-16
Responding Witness: Staff Policy Panel
Date of Response: August 21, 2018

Question:
O&R is in the process of retiring AMR meters that have only been in service a few years. Can the actual AMI meters slated to be rolled out be retrofitted with software or other add-ons to do the potential future applications identified by O&R Time-of-Use (TOU) rates, Critical Peak Pricing (CPP) and Critical Peak Rebates (CPR) and how much will these retrofits cost?

b) Can the AMI meters slated to be rolled out be retrofitted with software to connect so smart home systems and DSM (demand side management programs)?

(c) Please provide any hard data in support of O&R's contention that "Sacramento Municipal Utility District's "smart home" time-of-use rates . . . helped reduce customer bills by 10-13%" and that in "Oklahoma Gas & Electric's demand response program . . . 99% of participating customers saved an average of $150 annually."

Response:

Staff objects to this interrogatory on the grounds that it is duplicative as an identical interrogatory has been served on Orange and Rockland Utilities, Inc. (O&R or the Company). The interrogatory seeks information belonging to O&R and information related to statements made by O&R and thus is more appropriately directed at the Company.

EXHIBIT 4

STAFF OF THE DEPARTMENT OF PUBLIC SERVICE
RESPONSE TO INTERROGATORY/DOCUMENT REQUEST

Orange & Rockland Utilities, Inc.
Cases 18-E-0067 & 18-G-0068

Requesting Party: Deborah Kopald
Set No.: 1
Request No.: Kopald-17
Responding Witness: Staff Policy Panel
Date of Response: August 21, 2018

Question:
Please explain the DPS' view of how smart meter data collected is safe from any hacking intrusion as disclosed by the Department of Homeland Security (please see the July 23, 2018 Wall Street Journal article by Rebecca Smith, "Russian Hackers Reach Utility Control Rooms, Homeland Security Officials Say").
https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110 (article will be attached to email as well).
(In response to a previous interrogatory, 43, O&R only indicated that they thought their systems were robust, stating:
The Smart Meter solution selected by the Company has an extremely strong cyber security methodology. The Company also has significant experience in this area and not only thoroughly vetted the vendor and the Smart Meter solution, but also performed internal and third-party tests to validate security.)

Please explain how the system is robust enough to withstand the hacking described in the Wall Street Journal Article.

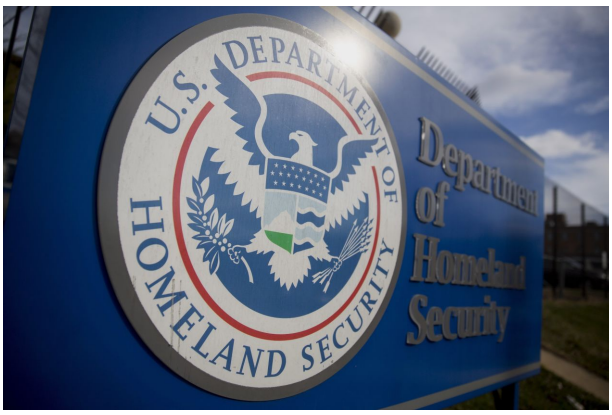
Response:

Staff objects to this interrogatory on the grounds that it seeks information that is beyond the scope and not reasonably calculated to lead to admissible evidence in the instant proceedings.

POLITICS

Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say

Blackouts could have been caused after the networks of trusted vendors were easily penetrated



Officials of the Department of Homeland Security said hackers have reached the control rooms of U.S. electric utilities. PHOTO: ANDREW HARRER/BLOOMBERG NEWS

By Rebecca Smith

July 23, 2018 7:21 p.m. ET

Hackers working for Russia claimed "hundreds of victims" last year in a giant and long-running campaign that put them inside the control rooms of U.S. electric utilities where they could have caused blackouts, federal officials said. They said the campaign likely is continuing.

The Russian hackers, who worked for a shadowy state-sponsored group previously identified as Dragonfly or Energetic Bear, broke into supposedly secure, "air-gapped" or isolated networks owned by utilities with relative ease by first penetrating the networks of key vendors who had trusted relationships with the power companies, said officials at the Department of Homeland Security.

"They got to the point where they could have thrown switches" and disrupted power flows, said Jonathan Homer, chief of industrial-control-system analysis for DHS.

DHS has been warning utility executives with security clearances about the Russian group's threat to critical infrastructure since 2014. But the briefing on Monday was the first time that DHS has given out information in an unclassified setting with as much detail. It continues to withhold the names of victims but now says there were hundreds of victims, not a few dozen as had been said previously.

It also said some companies still may not know they have been compromised, because the attacks used credentials of actual employees to get inside utility networks, potentially making the intrusions more difficult to detect.

Experts have been warning about the Russian threat for some time.

"They've been intruding into our networks and are positioning themselves for a limited or widespread attack," said Michael Carpenter, former deputy assistant secretary of defense, who now is a senior director at the Penn Biden Center at the University of Pennsylvania. "They are waging a covert war on the West."

Russia has denied targeting critical infrastructure.

Mr. Homer said the cyberattack, which surfaced in the U.S. in the spring of 2016 and continued throughout 2017, exploited relationships that utilities have with vendors who have special access to update software, run diagnostics on equipment and perform other services that are needed to keep millions of pieces of gear in working order.

The attackers began by using conventional tools—spear-phishing emails and watering-hole attacks, which trick victims into entering their passwords on spoofed websites—to compromise the corporate networks of suppliers, many of whom were smaller companies without big budgets for cybersecurity.

Once inside the vendor networks, they pivoted to their real focus: the utilities. It was a relatively easy process, in many cases, for them to steal credentials from vendors and gain direct access to utility networks.

Then they began stealing confidential information. For example, the hackers vacuumed up information showing how utility networks were configured, what equipment was in use and how it was controlled. They also familiarized themselves with how the facilities were supposed to work, because attackers "have to learn how to take the normal and make it abnormal" to cause disruptions, said Mr. Homer.

Their goal, he said: to disguise themselves as "the people who touch these systems on a daily basis."

DHS is conducting the briefings—four are planned—hoping for more industry cooperation. One thing the agency is trying to learn is whether there are new infections, and whether the Russians have figured out ways to defeat security enhancements like multifactor authentication.

In addition, DHS is looking for evidence that the Russians are automating their attacks, which investigators worry could presage a large increase in hacking efforts. "To scale, they're eventually going to have to automate," Mr. Homer said.

"You're seeing an uptick in the way government is sharing threats and vulnerabilities," said Scott Aaronson, a cybersecurity expert for Edison Electric Institute, the utility industry trade group. He said information sharing and penetration detection have gotten much better since the Dragonfly attacks began.

It isn't yet clear whether the hackers used their access to prepare the battlefield for some future, devastating blow, investigators said. For example, many experts fear that a skilled technician could use unfettered access to change some equipment's settings. That could make them unreliable in unexpected ways, causing utility engineers to do things that would result in extensive damage and potentially lengthy blackouts.

Write to Rebecca Smith at rebecca.smith@wsj.com

Appeared in the July 24, 2018, print edition as 'Russia Hacks Its Way Into U.S. Utilities.'

EXHIBIT 5

STAFF OF THE DEPARTMENT OF PUBLIC SERVICE
RESPONSE TO INTERROGATORY/DOCUMENT REQUEST

Orange & Rockland Utilities, Inc.
Cases 18-E-0067 & 18-G-0068

Requesting Party: Deborah Kopald
Set No.: 1
Request No.: Kopald-18
Responding Witness: Staff Policy Panel
Date of Response: August 21, 2018

Question:
Please provide any evidence the DPS has that AMI systems of the type O&R is slated to continue to rollout have reduced consumer's bills.

Response:

Staff objects to this interrogatory on the grounds that it seeks information that is beyond the scope and not reasonably calculated to lead to admissible evidence in the instant proceedings.

EXHIBIT 6

STAFF OF THE DEPARTMENT OF PUBLIC SERVICE
RESPONSE TO INTERROGATORY/DOCUMENT REQUEST

Orange & Rockland Utilities, Inc.
Cases 18-E-0067 & 18-G-0068

Requesting Party: Deborah Kopald
Set No.: 1
Request No.: Kopald-19
Responding Witness: Staff Policy Panel
Date of Response: August 21, 2018

Question:
Please provide any evidence the DPS has that AMI systems of the type O&R is slated to continue to rollout have measurably reduced use of electricity.

Response:

Staff objects to this interrogatory on the grounds that it seeks information that is beyond the scope and not reasonably calculated to lead to admissible evidence in the instant proceedings.

EXHIBIT 7

STAFF OF THE DEPARTMENT OF PUBLIC SERVICE
RESPONSE TO INTERROGATORY/DOCUMENT REQUEST

Orange & Rockland Utilities, Inc.
Cases 18-E-0067 & 18-G-0068

Requesting Party: Deborah Kopald
Set No.: 1
Request No.: Kopald-20
Responding Witness: Staff Policy Panel
Date of Response: August 21, 2018

Question:
Please provide any evidence the DPS has that AMI systems of the type O&R is slated to continue to rollout have resulted in peak loaders being turned off/ not needing to otherwise be turned on.

Response:

Staff objects to this interrogatory on the grounds that it seeks information that is beyond the scope and not reasonably calculated to lead to admissible evidence in the instant proceedings.