OFFICE OF THE INSPECTOR GENERAL

MEMORANDUM OF LIMITED INVESTIGATION

February 7, 2020

TO: Andrew Kleine
Chief Administrative Officer

FROM: Megan Davey Limarzi
Inspector General

SUBJECT: Department of Permitting Services Security Incident
OIG Publication #20-007

A Memorandum of Limited Investigation (formerly referred to as a "PIM") describes specific issues or complaints received and the outcomes of limited procedures undertaken during a Preliminary Inquiry conducted by the Office of the Inspector General (OIG). Copies of this memorandum along with your response, if any, will be provided to the members of the County Council and the County Executive within 3 business days of this communication and then made public.

Complaints:

Beginning on February 4, 2020, the OIG received several complaints in rapid succession concerning an incident that occurred at the Department of Permitting Services (DPS). All complainants expressed concern that DPS employees felt pressured to provide their computer login user ID and password to their managers so that they could receive new laptops.

Inquiry and Outcome:

Based on emailed documentation obtained by the OIG, we learned that a DPS Information Technology (IT) Specialist sent an email to an email group entitled "DPS Leaders" on January 29, 2020. The email stated:

> "… We can't just give you laptops for your people. We will setup for everyone on their desktops with docking stations. We need you to … [p]rovide your people's account information by COB of this Friday…"

While the email provided an alternate option for "those people who refuse to give out their passwords," the request was nonetheless at odds with recent security training provided to County employees and a violation of County policy. The OIG immediately contacted both the Acting DPS Director and the Department of Technology Services (DTS) Enterprise Information Security Official to discuss the allegations.

Following discussions with the OIG, both DPS and DTS took immediate action:

- The Acting DPS Director sent out an email to all DPS employees instructing them to refrain from sharing passwords, even with the DPS IT Section. Employees who previously shared their passwords were told that they must change their password immediately.
- The DTS Enterprise Security Official emailed the DPS IT Specialist who generated the original request and reminded them that sharing, as well as requesting that others share, ID's/passwords is a violation of the County's information security policy and pointed out it was taught in the County's security awareness training, including the February 2020 training module.

Summary and Conclusion:

Last week, a DPS IT Specialist requested that DPS employees provide their user ID/passwords to their managers so that new laptops could be configured for them. This is a violation of the County's information security policy and placed the County and its employees at increased risk for fraud.[1]

While the DPS IT specialist clearly made an error in judgement when requesting DPS employees provide their password to anyone, it appears that the mandatory, monthly IT Security training provided by the County is having a positive effect. The timely complaints received by the OIG suggest that employees are reaching out when they identify security vulnerabilities, and one of the complainants even mentioned the training specifically.

DPS and DTS took immediate action to stop the sharing of passwords, counsel the employee who requested that passwords be shared, and ensure that DPS employees who shared their passwords took action to protect their data and systems. The DPS Acting Director and DTS Enterprise Security Official used the incident as an opportunity to reiterate that employees should never share their passwords nor request other to do so as well.

cc: Fariba Kassiri, Deputy Chief Administrative Officer

[1] In November 2018, a County employee was convicted of fraud a multimillion-dollar fraud scheme. That employee was able to commit the fraud, in part, because the employee's Department Director shared his user ID and password with him. See https://www.washingtonpost.com/local/md-politics/fake-invoices-and-gambling-debts-how-a-county-bureaucrat-stole-67-million/2019/02/21/7c35e6a6-2641-11e9-90cd-dedb0c92dc17_story.html.

Administration's Response to this Memorandum of Limited Investigation:

On February 12, 2020, the Office of the Chief Administrative Officer responded via email:

"We thank the Office of the Inspector General for the notification and the thorough report.

This incident was caused by a single employee who failed to follow security policy/training, but further damage was prevented by employees rapidly reporting the security incident. An Information Security Alert was sent to all County users (employees, contractors, volunteers) on 2/11/2020 reiterating the policy on userid/password security and reminding users how to create strong passwords."