TRANSCRIPTION OF POWERPOINT PRESENTATION FROM HOUSE OFFICE OF INSPECTOR GENERAL

Dated September 20, 2016

Complaint background

- On April 25, 2016, CHA requested we review irregular mobile device purchases by a systems administrator shared employee
- The CAO had identified purchase requests for iPads with invoice prices of $499 and with warranties (e.g. Apple Care plan) of $399, totaling approximately $898
- These purchases were irregular because the CDW-G (vendor) pricing schedule for iPads is approximately $750 with warranties costing $88
- There are six known subjects (all shared employees)
- Period of review: October 2015-April 2016
- Identified 20 offices with irregular payments

Equipment Inventory

- The CAO shall maintain an inventory of all Member and Committee office equipment items having an original purchase price of $500 or more.

Sharing Job Duties

- Shared employees shall not share their job duties with other individuals employed by 1) a different Member or Committee offices or 2) individual who are not on the House payroll. (House Ethics Manual and 2 USC S. 101)
- House employees, including shared employees, are prohibited from subletting any portion of their official duties to someone else. (Shared employee manual)

Equipment Inventory

- Six subjects, who are shared employees, requested vendors to split the cost of equipment among multiple items and charged these items as office supplies instead of equipment.
- As of Sept 1 2016 there have been 34 purchases from two vendors (CDW and More Direct) totaling nearly $38,000 where the cost of the item was manipulated to obtain a purchase price of $499.99 or equipment has been purchased in a manner to circumvent the requirement to include equipment exceeding $500 on the House offices inventory.

Purchase Examples

- iPad: Original cost $799; paid $499 for iPad, $350 for Apple Care (costs $88)
- TV: Original cost $640; paid $499 for TV, $263 for TV mount (costs $36)
- Shredder: Original cost $685; paid $499 for shredder, purchased 4 computer keyboards for $69 each (actual cost $25)

Verified that most of the equipment in question was not listed on the House Office's inventory

75 pieces of equipment with a purchase price of $118,416 were recently written off the House inventory for a member because one of the subjects could not produce them

- Shared employee stated that the items were never received, shouldn't have been inventoried, or the staff lost the equipment
- However, equipment could not be on inventory or have asset tag unless it had arrived in office and EIN had been signed
- Missing equipment includes laptops, iPads, TVs, video conferencing equipment, and computers

Identified outstanding invoices that have not been paid

- CDW-G sales rep for the House stated that he has had problems with getting EINs signed and invoices paid by these individuals' offices
- Data from CDW-G has shown that the offices where these shared employee's work owe CDW over $219k
- Five of the offices have invoices over 500 days old

Unauthorized access

- Users shall only access and use information for which they have official authorization
- Shared Employees shall not share their job duties with other shared employees

Identified the 5 shared employee system administrators have collectively logged into 15 member offices and the Democratic Caucus, although they were not employed by the offices they accessed.

- Imran Awan, Abid "Omar" Awan, Hina Alvi, Jamal Awan, and Rao Abbas are the shared employees in question
- Determined that one of the systems administrators logged into a member's office two months after he was terminated from that office
- Based on analysis of Activity Directory data from October 2015 and April 2016

Review of current logon data identified excessive logins to a Democratic Caucus server and three of their workstations over a 7-month period

- All 5 of the shared employee system administrators collectively logged onto the Caucus system 5,735 times, an average of 27 times per day

- Hina Alvi is the shared employee for the Caucus and she logged into the Caucus computers 291 times over the 7-month period
- This is considered unusual since computers in other offices managed by these shared employees were accessed in total less than 60 times.
- The server (dem11ts) was logged onto 1,154 times, or 5.4 times a day

This pattern of login activity suggests steps are being taken to conceal their activity

- Behavior avoids network monitoring
- Use of Active Roles Servers indicates they may be granting access on a temporary basis, which could be done to evade network monitoring
- The Caucus Chief of Staff requested one of the shared employees to not provide IT services or access their computers
- This shared employee continued

The following are risks associated with the unusual logon activity

- Excessive logons are an indication that the server is being used for nefarious purposes and elevated the risk that individuals could be reading and/or removing information
- Computers could be used to store documents taken from other offices or evidence of other illicit activity
- Computers could be used as a launching point to access other systems for which access may be unauthorized.

These risks may be higher since the shared employees have not been vetted (e.g. background check)

SECOND PRESENTATION DATED SEPTEMBER 30, 2016

Updated:

- Network Logon Activity from May - August 2016
- Frequency of access to Democratic Caucus server
- Collectively, the shared administrators accessed the dem11ts server 995 times, or 8.2 times per day.

Server is primarily accessed remotely and the remote sessions for all shared administrators lasted 265.3 days (122 days in the log period)

- Omar's logon sessions 89.1 days (73.1% of log period)
- Imran's sessions: 67.9 days (55.7%)

- Rao's sessions: 65.6 days (53.8%)

Additional results:

Additional computers logged onto frequently:

- Democratic Caucus Conference Room: Computers FL21DC200A and IL02DC143
- Conference Room L1640: CA16JCD010B and CA29DCTC184G

Continuing analysis, including identifying systems used to connect to dem11ts via VPN

- Met with HIR Cybersecurity on 9/20 to discuss assistance and 9/27 to discuss their analysis to date.

Continued Unauthorized Access

During September 2016, shared employee continued to use Democratic Caucus computers in anomalous ways:

- Logged onto laptop as system administrator
- Changed identity and logged onto Democratic Caucus server using 17 other user account credentials
- Some credentials belonged to Members
- The shared employee did not work for 9 of the 17 offices to which these user accounts belonged
- Occurred on the Democratic Caucus computers, even though the employee had never been employed by the Caucus.

Possible storage of sensitive House information outside the House.

- Dropbox is installed on two Caucus computers used by the shared employees
- Two user account had thousands of files in their Dropbox folder on each computer

We have not been permitted to view content of the files on these workstations. However, based on the file names, some of the information is likely sensitive.

While file sharing sites, such as Dropbox, have legitimate business purposes, use of such sites is also a classic method for insiders to exfiltrate data from an organization.