Transit Auth. v. Victor

OATH Index No. 799/11 (Mar. 3, 2011), *aff'd*, NYC Civ. Serv. Comm'n Item No. CD-11-52-A (Aug. 9, 2011), **appended**

Respondent found guilty of misconduct for shouting at her supervisor, and failing to comply with her supervisors' requests to handle a specific voice message and update the Standard Operating Procedures, but not for failing to timely submit reports for which she was not trained and to which she had no technical access. Petitioner failed to establish that respondent is incapable of performing tasks appropriate for her title of Computer Specialist I. The credible evidence established that respondent made some careless errors which were not so pervasive as to constitute negligence. For respondent's multiple instances of insubordination, ALJ recommends suspension without pay for 25 days.

NEW YORK CITY OFFICE OF ADMINISTRATIVE TRIALS AND HEARINGS

In the Matter of
TRANSIT AUTHORITY
Petitioner
- against -
ALEXANDRIA VICTOR
Respondent

REPORT AND RECOMMENDATION

INGRID M. ADDISON, *Administrative Law Judge*

This is a disciplinary proceeding referred by petitioner, the Transit Authority (TA), pursuant to section 75 of the Civil Service Law. Petitioner alleges that respondent, Alexandria Victor, a Computer Specialist I, is not competent in the tasks commensurate with her position and title, and that she was insubordinate towards her immediate supervisor, failed to submit a report to petitioner's Assistant Chief Officer, and failed to comply with the Director's instructions to update the Cyber Security Center's (CSC) Standard Operating Procedures (SOP)[1] in spite of her representations to the contrary, in violation of rules 2(a), (b), (d), 4(a), (b), 5(a),

[1] Petitioner withdrew with prejudice specification 14, which alleged that respondent improperly created a Novell and internet account for a General Superintendent which subsequently resulted in the loss of internet access.

and 10(a) of the rules and regulations governing employees of the MTA New York City Transit. (ALJ Ex. 1).

At a two-day hearing on January 6 and 28, 2011, both parties submitted documentary evidence. In addition, petitioner presented testimony from respondent's supervisors, and respondent testified on her own behalf.

Based on that evidence, petitioner established that respondent was insubordinate when she: yelled at her supervisor on January 21, 2010; failed to respond to a specific voice message on February 19, 2010, after being asked to do so by her supervisor; and failed to update the SOPs during the period June 23 through July 14, 2010, while assuring the director that she had done so. I did not find respondent guilty of misconduct for failing to produce certain reports to the Assistant Chief Officer of her unit by their due date. Petitioner also failed to prove that respondent is unable to perform the duties associated with her job title. Rather, the credible evidence established that respondent committed some errors due to carelessness. I also find that some errors, as discussed below, were attributable to imprecision in the SOP. For respondent's misconduct, I recommend that she be suspended without pay for 25 days.

ANALYSIS

Respondent was hired by the TA in 1982, and became a Computer Specialist Level I in April 2008. In October 2008, she joined its CSC, whose Assistant Chief Officer (ACO) for the past three years has been David Papismedov[1] (Tr. 10). Respondent's direct supervisor is Vinnie Campbell, a Computer Specialist Level IV, who has been with the TA for 28 years (Tr. 209-11). Mr. Campbell reports to director Ed Cheng, who is directly accountable to Mr. Papis. The CSC is responsible for the information security technology of the TA and all MTA agencies. That includes protecting data from intrusion and fraudulent activities, and perimeter and virus protection. CSC workers monitor screens and look for signs of unusual activity. They also monitor help desk tickets and respond to telephone calls which are logged, to indicate the time of the call, the person who assisted, and the response resolution time. Difficult problems are "escalated" in that they are referred to the immediate supervisor or, in his absence, the director (Papis: Tr. 17; Campbell: Tr. 213-14). An extensive SOP manual is available in printed and electronic format. It was initially compiled by respondent who was assigned the task of

[1] Mr. Papismedov testified that he uses and is known by the abbreviated form of his name, Mr. Papis.

assembling and sorting procedures by subject matter, testing them for clarity, and collating them in a comprehensive manner, soon after she joined the unit. (Tr. 46-48, 52-53; Pet. Ex. 18).

Respondent's work schedule is 8:00 a.m. to 4:00 p.m. Her typical shift on CSC matters is four to six hours long. Her CSC responsibilities include: assisting users with "My Access;" creating user IDs; and responding to telephones and voicemail security inquiries. Otherwise, she updates the SOP and procurement information (Papis: Tr. 13; Campbell: Tr. 211-13).

Petitioner charged respondent with 16 instances of incompetence and/or misconduct. While it cited to rules that respondent allegedly violated, petitioner neglected to reconcile the individual allegations to a specific rule or rules, and at trial, identified the allegations under Specifications 1, 16 and 17 as related to misconduct. Respondent's counsel did not assert lack of notice or that he was prevented from adequately defending against the charges.

Therefore, my discussion below is broken down into two categories: misconduct and incompetence.

Misconduct Allegations

Screaming and Shouting at Supervisor (Specification 1)

Under the TA's Rules and Regulations, employees are required to conduct themselves in such a manner as to merit the confidence and respect of their supervisors. MTA NYC Transit Auth., Rules and Regs., Chp. 1, Rule 10(a) (Nov. 2003). Petitioner alleged that on January 21, 2010, respondent screamed and shouted at her supervisor (ALJ Ex. 1, Spec. 1).

Mr. Campbell testified that some time on January 21, 2010, respondent followed him to his desk after he had instructed her to check on voice mails. She yelled that she could not multitask and was busy. Mr. Campbell found respondent's behavior to be "degrading" because it was overheard by other CSC employees. He was also particularly perturbed because he is careful not to raise his voice or speak to others in a demeaning tone (Tr. 214-17). Mr. Campbell took no action because "people get upset" and none of his bosses suggested that the incident be written up. Ms. Papis testified that he was alerted by e-mail from Nina Fransisco, another computer specialist in the CSC unit, that "Sandra was just screaming and shouting at Vinnie….yikes" (Tr. 27-28; Pet. Ex. 1B).

Respondent objected to the admission of Ms. Fransisco's e-mail on grounds that Mr. Papis was not a witness to respondent's behavior and the e-mail therefore constituted hearsay.

Over respondent's objections, I admitted the e-mail into evidence. Hearsay is admissible in administrative proceedings and may form the sole basis of a finding of fact. *See Transit Auth. v. Wong*, OATH Index No. 1866/08 at 18-19 (Aug. 28, 2008); *Dep't of Correction v. Jackson*, OATH Index No. 134/04 (May 5, 2004), *aff'd*, NYC Civ Serv. Comm'n Item No. CD 05-67-SA (Sept. 14, 2005). The hearsay evidence must be "sufficiently probative of a material issue and must have some objective circumstances demonstrating its reliability." *Police Dep't v. Mazzoli*, OATH Index No. 1610/07, mem. dec. at 4 (Apr. 6, 2007). Even though it is unclear why Ms. Fransisco, and not Mr. Campbell, reported respondent's behavior to Mr. Papis, her e-mail was, nevertheless, a contemporaneous communication of what was occurring in the office. This tribunal has found that contemporaneous statements evince reliability. *See Human Resources Admin. v. Ali*, OATH Index No 2380/09 at 16 (July 20, 2009); *Dep't of Sanitation v. Sanders*, OATH Index No. 558/09 at 4 (Jan 5, 2009); *Dep't of Correction v. Boyce*, OATH Index No. 789/97 at 14 (July 9, 1997), *aff'd*, NYC Civ. Serv. Comm'n Item No. CD 99-75-SA (July 19, 1999). Thus, I found Ms. Fransisco's e-mail to be reliable hearsay that supported Mr. Campbell's testimony.

Respondent could not recall the incident but testified that she is not in the habit of shouting or screaming. At the same time, she left open the possibility that she was upset and may have spoken in an elevated tone.

I found Mr. Campbell's testimony to be sincere. He recalled the incident with clarity and conveyed genuine embarrassment that his subordinates had overheard respondent's vociferous interaction with him.

Not every disagreement with a supervisor or expression of dissatisfaction has been deemed misconduct by this tribunal, even when voices are raised and emotions are vented. *Health & Hospital Corp. (Woodhill Medical & Mental Health Ctr.) v. Freeman*, OATH Index No. 1399/06 at 9 (July 20, 2006); *Transit Auth. v. Nixon*, OATH Index No. 2131/96 at 15-16 (Mar. 31, 1997), *modified on penalty*, Auth. Dec. (May 16, 1997); *Human Resources Admin. v. Bichai*, OATH Index No. 211/90 (Nov. 21, 1989), *aff'd*, NYC Civ. Serv. Comm'n Item No. CD 90-54 (June 15, 1990) (employee has a "right to express his views, even vehemently"). Indeed, it is permissible for an employee to disagree with a supervisor as long as the disagreement remains within the bounds of decorum and discretion. *Health & Hospital Corp. (Lincoln Medical & Mental Health Ctr.) v. Thomas*, OATH Index No. 531/04 at 5 (May 4, 2004). Factors

to consider in determining whether a disagreement rises to the level of misconduct include: the use of threats, insolence, or profanity; office disruption caused by the argument; and whether it was in front of co-workers and/or the public. *Dep't of Citywide Admin. Services v. Phillip*, OATH Index No. 114/10 at 7 (Sep. 10, 2009); *Health & Hospitals Corp. (Queens Health Network) v. Smith*, OATH Index No. 2019/08 at 2 (Oct. 17, 2008); *Dep't of Homeless Services v. Aigbedion*, OATH Index No. 2340/07 at 4 (Nov. 2, 2007).

Here, even though there was no accusation that respondent used profanity, I found pursuit of her supervisor after he instructed her to check on voice mails, and yelling at him within earshot of other employees were insolent. Such conduct is disrespectful and inappropriate in the workplace. Accordingly, Specification 1 is sustained.

Failing to Respond to Voice Messages (Specification 6)

Petitioner alleged that on or about February 19, 2010, respondent failed to respond to calls from customers, which was her primary responsibility.

On February 18, 2010, Mr. Campbell e-mailed respondent, inquiring whether she had responded to a particular voicemail that he had earlier asked her to handle (Pet. Ex. 6 at 3). Respondent replied that she was busy "answering the phones and doing LAN id and internet" and that there were other people who could handle the voicemail (Pet. Ex. 6 at 3). The following day, Mr. Cheng, who had been copied on the e-mails, sought to establish whether respondent's reply to her supervisor was justified. He asked respondent for a detailed summary of the number of local area network (LAN) IDs and internet access requests she had handled the previous day, as well as the number of trouble tickets she had updated and closed.

Respondent replied that she handled 10 LAN IDs, 2 internet access requests, and 20 calls for password resets. Respondent further indicated that she was unable to review the number of trouble tickets but estimated that she had closed about two or three. She expressed that it took 15 to 30 minutes to resolve the problems of some callers.

Mr. Cheng notified respondent that the actual phone records did not support her reply because they revealed that she had only processed four calls as opposed to the twenty that she had claimed. Moreover, her claim that she had created ten LAN IDs was not supported by the Unisys Peregrine ticket system which showed that only five LAN IDs had been created on the day in question. Mr. Cheng requested the paperwork to corroborate her numbers, and respondent provided work for seven LAN IDs, not ten as she had declared in her e-mail to him. He could

not be certain of the number of calls that were logged into the system that day but posited that they numbered far less than the 20 that respondent had asserted. Mr. Cheng acknowledged that each call can range from 15 to 25 minutes but maintained that based on his review, respondent had sufficient time to comply with Mr. Campbell's request (Tr. 299-302).

Respondent neither disputed the charge nor defended against it.

As an initial matter, petitioner presented evidence of only one call which respondent failed to handle, as opposed to the multiple "calls" reflected in the allegation. Mr. Campbell was not questioned about the circumstances surrounding the charge and the documentary evidence was unclear as to when he first asked respondent to attend to a specific voicemail. In any event, it was apparent that respondent failed to comply with Mr. Campbell's second request. The discrepancy in respondent's accounting of her activities and Mr. Cheng's statistics suggest that respondent exaggerated her figures to rationalize her response to Mr. Campbell.

At trial, petitioner did not specifically identify respondent's behavior on February 19, 2010, as misconduct. But I find it more appropriate to classify it as such.

Petitioner's rules provide that employees must obey the orders of their supervisors and perform such duties as directed by their supervisors. MTA NYC Transit Auth., Rules and Regs., Chp. 1, Rule 4(b) (Nov. 2003). This tribunal has held that in order to establish insubordination, the petitioner must prove by a preponderance of the credible evidence that a clear and unambiguous order was issued and the respondent willfully refused to obey it. *Transit Auth. v. Wong*, OATH Index No. 1866/08 at 16-17 (Aug. 28, 2008); *Dep't of Sanitation v. Nieves*, OATH Index No. 1683/07 at 10 (Sept. 19, 2007) (citing *Dep't of Environmental Protection v. Schnell*, OATH Index No. 2262/00 at 6 (Oct. 25, 2000)). The directive need not be in the form of a command, as long as the request was clear and unambiguous. *Wong*, OATH 1866/08 at 16; *Dep't of Sanitation v. David*, OATH Index No. 766/07 at 5 (Jan. 25, 2007), *modified on penalty*, NYC Civ. Serv. Comm'n Item No. CD 07-101-M (Oct. 25, 2007).

Here, Mr. Campbell made a specific request with which respondent made no attempt to comply. The onus was not on respondent to determine which of her activities took priority. That was her supervisor's responsibility. Otherwise, respondent was obligated to comply with Mr. Campbell's request. I found her reply to his second request, that there were others who could handle it, to be obnoxious, and her failure to comply with it, insubordinate.

Accordingly, Specification 6 is sustained.

Failing to Submit a Status Report by Its Due Date (Specification 16)

Petitioner alleged that respondent failed to submit a status report to Mr. Papis by its due date of July 1, 2010.

Monthly, Mr. Papis submits unit performance reviews to CSC's executive level managers. They comprise a collation of reports "for particular systems or particular subjects" from the individuals responsible for the respective areas. On Monday, June 28, Mr. Papis e-mailed a request for status reports to be submitted to him by the close of business on July 1. His e-mail identified the requested reports and the persons charged with submitting them. Respondent was responsible for the following four reports: 1) Users of Internet Access (broken down by FTP and HTTP); 2) Internet Proxy Servers; 3) Total Number of Tickets Closed during January; and 4) CSC Phone Call Log (Tr. 114-15; Pet. Ex. 16A). Mr. Papis testified that respondent was assigned the Internet Proxy Servers report because the person who was normally accountable for it was due to go on vacation. On the due date, Mr. Papis sent reminders at around 8:13 a.m. (Tr. 114; Pet. Ex. 16A). Respondent replied at around 9:13 a.m., that she could not produce the Users of Internet Access report because she did not have access to the binder application which provides it. She further advised Mr. Papis that on the previous day, she had spoken with Mr. Campbell about the Internet Proxy Server report, and he was unsure how to access the application to produce it. Accordingly, respondent notified Mr. Papis that when Ms. Francisco returned to the office, she would seek her assistance (Tr. 120; Pet. Ex. 16B).

While acknowledging that respondent timely produced the reports for which she was regularly responsible (Tr. 187-88), Mr. Papis rejected her explanation for failing to produce two reports for which someone else was normally accountable. In a July 1 e-mail which appeared to ignore respondent's notification that she had communicated with "Vinnie," Mr. Papis admonished that the absence of one team member should not halt operations and that "Vinnie is equipped with Blackberry and has remote access from home; so if you needed his involvement you should have escalated it before the due date" (Tr. 120; Pet. Ex. 16B). Respondent replied on July 2, and reiterated that Nina was the only one who could generate the report and that Vinnie was unsure how Nina accessed the application (Resp. Ex. A).

At trial, Mr. Papis disavowed knowledge of respondent's communication with "Vinnie." He contended that, notwithstanding, he requested the reports in sufficient time "before Nina went on her vacation" for respondent to prepare them (Tr. 120, 189). He could not recall with specificity when either "Nina" or "Vinnie" had started their vacation. As a result of respondent's inability to produce the Users of Internet Access and Internet Proxy Servers reports by the due date, Mr. Papis was unable to provide a complete report to the Vice President of Technology Information Services (VP). Neither Mr. Papis nor the VP received the reports until the following week (Tr. 121-24). He chastised Mr. Campbell by e-mail on July 2, and denounced as "unacceptable" the fact that "only one person in [the] team [knew] a specific system enough to produce a statistics report crucial for upper management." He also decried the practice as "poor team management," which Mr. Campbell needed to fix (Tr. 204-05; Resp. Ex. A).

Respondent, whose overall testimony was cursory, did not testify about this charge. In spite of that, I find that petitioner failed to prove misconduct here.

A finding of misconduct under Section 75 of the Civil Service Law is predicated upon a finding of fault, in that the employee acted either willfully or intentionally, *see Reisig v. Kirby*, 62 Misc. 2d 632, 635 (Sup. Ct. Suffolk Co. 1968), *aff'd*, 31 A.D.2d 1008 (2d Dep't 1969), or carelessly or negligently, *McGinigle v. Town of Greenburgh*, 48 N.Y.2d 949, 951 (1979). Conduct that is lacking in willful intent or is not so unreasonable as to be considered negligence, is not a basis for finding misconduct. *See Berardi v. City of New York*, 12 N.Y.2d 1061, 1064 (1963); *Ryan v. NYS Liquor Auth.*, 273 A.D. 576 (3d Dep't 1948); *Dep't of Correction v. Callabrass*, OATH Index No. 1981/10 at 6-7 (July 23, 2010), *adopted in part, rejected in part*, Comm'r Dec. (Dec. 1, 2010).

There was no dispute that respondent produced the reports for which she is normally accountable. However, it was clear that she did not have the technical capability to produce the Users of Internet Access and the Internet Proxy Server reports that she is accused of failing to timely produce. It was equally clear that even Mr. Campbell, the supervisor of the unit, did not have the capability to do so, and that only Ms. Francisco could access the application to produce the reports. There was no suggestion that respondent was recalcitrant. In fact, respondent directed the problem to Mr. Campbell, as she was required to do under such circumstances, but that was to no avail. Mr. Papis' displeasure at Mr. Campbell for poor team management was evident in his July 2 e-mail. Thus, it was unclear to me how the supervisor's failure to ensure

that others were trained as back-ups to produce the requested reports could be attributed to respondent.

Accordingly, I find that specification 16 is not sustained.

Failure to Update CSC's Standard Operating Procedures between June 23 and July 14, 2010 (Specification 17)

Respondent is charged with failing to update the SOPs during the period June 23 through July 14, 2010, while falsely claiming that the SOP update was complete.

When respondent joined the CSC unit, she was assigned, among others, the task of assembling and editing the SOPs. According to Mr. Cheng, respondent was required keep the SOPs current and accurate by first reviewing all documents submitted to her before compiling and indexing them. New procedures and updates of existing ones are sent to respondent by the source owners, that is, the persons issuing them, for inclusion into both the electronic and manual versions. Mr. Cheng testified that between late June and early July 2010, he made several e-mail requests of respondent to update the SOPs with various procedure, but none were added or compiled correctly, or indexed (Tr. 315-19).

For instance, on July 14, 2010, he asked respondent to update the SOP with the "revised version of the AS400 password reset procedure" (Pet. Ex. 17 at 3). Respondent replied that the procedure had been added to the SOP, but Mr. Cheng claimed that it was not. On July 2, Mr. Cheng asked respondent to make sure that the procedure for the AS400 Midrange Systems was placed in the SOP. On July 6, respondent assured him that "Midrange Access Request Form-CSC and the AS400 Security Menu Reset Password has (sic) been added to SOP under the ICSS-Share" (Pet. Ex. 17 at 7). Mr. Cheng conceded that they were added to the ICSS share but claimed that that was not his request. He distinguished the SOP, which is a manual document, from the ICSS share drive, the server in which the document resides (Tr. 319-20).

Mr. Cheng also referenced a July 8, 2010 e-mail from respondent to the entire unit and Mr. Papis, notifying them that "[t]he Monthly Report for users of Internet Access Breakdown by FTP and HTTP" had been added to the SOP. There was no testimony as to the status of that report.

On July 1 at 12:33 p.m., Mr. Cheng e-mailed respondent as follows: "Attached is the Sentinel Oracle Procedure to check the status along with how to start and stop the Sentinel Oracle database." Later that day, he sent another e-mail to respondent which read: "Attached is

the procedure to stop and start Sentinel. Please make sure it is put in our SOP." The next morning, respondent replied that the "Sentinel Oracle database has been added to our SOP." On July 6 at 8:33 a.m., in an e-mail captioned "RE: Sentinel Oracle Status Check with Start and Stop Procedure" to Mr. Cheng and the CSC group, respondent wrote "Done." Mr. Cheng responded at 8:45 a.m., that he had asked her about the Sentinel procedure not the Sentinel Oracle procedure (Pet. Ex. 17). At 8:49 a.m., respondent e-mailed Mr. Cheng with a "Sentinel Stop and Start Procedure.pdf" attachment, and informed him that "[t]his is the only [procedure] I received from you."

On June 23, Mr. Cheng sent respondent a procedure to be followed by all shifts if it became necessary to reboot PMF servers. He asked her to "copy and paste the procedure to a document, name it Backup of userapp.log and add it to the SOPs" (Pet. Ex. 17). Mr. Papis also e-mailed respondent that it needed to be part of the published SOP book. Respondent's reply to Mr. Cheng indicated that it had been added to the electronic version of the SOP.

In an e-mail on September 16, 2010, Mr. Cheng notified respondent that he had checked the shared drive and found that the SOP book, version and revision dates had not been updated since November 2009, in spite of the directives he had sent to her with new procedures and updates dating back to at least June 23. Instead, respondent had only copied the new procedures and/or updates into folders on the shared drive, which did not equate to putting them in the SOP book and making the appropriate changes to the version number and revision dates (Pet. Ex. 17). He demanded an explanation as to why she had confirmed that the additions and/or updates had been made to the SOP in light of his discovery that they had not. Mr. Cheng testified that the SOPs are required to be kept current and accurate because the unit is audited annually (Tr. 321). Further, a computer specialist should be capable of maintaining the SOP because a person in that title should be able to function without supervision or with limited supervision (Tr. 345).

Respondent's testimony regarding updates to the SOP was odd. She initially claimed that when she received e-mail updates to the SOP, she would "put them in" and then send an e-mail response "with a picture saying that it has been added to the SOP" (Tr. 362-63, 381-82). She later testified that she is usually prompt in responding to e-mails "so when you send me an e-mail, I'm going to send it back to you and say it's been done." It did not make sense that she would confirm that a task had been accomplished simply for the purpose of being prompt in her reply. There was no urgency indicated in Mr. Cheng's e-mail, and it was not apparent that he

expected her to cease what she was doing to update the SOP. But even if true, it was her responsibility to make sure that she later complied with his requests. Her testimony that she did not respond to Mr. Cheng's September 16 e-mail, because she had already responded to him on June 23, three months prior also lacked logic and credibility (Tr. 385-86).

Accordingly, I find that respondent failed to fully comply with multiple requests by Mr. Cheng to update the SOP, and sustain Specification 17.

Incompetence Allegations

Petitioner asserted that respondent's work is so fraught with errors that she is unable to perform competently at her title of computer specialist Level 1, and further, that her incompetence often resulted in the delayed resolution of customer service requests.

According to Mr. Papis, a new CSC employee is typically given some time to become familiar with the procedures of the unit. No formal, structured training is provided because of the unit's workload (Tr. 187). Instead, a new worker is placed with an experienced CSC worker and receives on-the-job training on how to manage firewalls, intrusion detection, protection systems, and the forensics evidence of a network. Mr. Cheng testified that Nina Francisco was the designated instructor (Tr. 338). Short class sessions are conducted in the conference room. Afterwards, the new employee operates independently. The on-the-job training is characterized as "boot camp" training. Mr. Papis evaluated it as "effective," and discounted the need for formal training (Papis: Tr. 198-99; Cheng: Tr. 281). Training may take anywhere from one to a few months depending on the aptitude of the employee, but respondent, who was the newest member of the unit during the period covered by the charges, was given almost one year to become familiar with the systems because there was no operational need to accelerate her learning process (Papis: Tr. 110; Cheng: Tr. 282).

Mr. Papis testified that respondent made errors throughout 2009, but he "didn't pay to them a big attention" because, until the CSC went into full production mode in November 2009 (at which point, all systems began to heavily rely on it for monitoring security activities), any mistakes that respondent made did not really affect operations. As a result, during her first year with the unit, respondent was given no written feedback on her performance (Tr. 109-111, 139, 144-45, 191-92). To the best of Mr. Papis' knowledge, respondent received her first evaluation in January 2010 (Tr. 139-42). However, he asserted that computer specialists are high-level

technicians who should be able to independently assume certain projects or tasks (Tr. 112). He described respondent as "unusual" because sometimes she performed certain tasks on par with her colleagues and at other times she completely failed at tasks that she had previously completed successfully (Tr. 200).

Even though she initially denied it, respondent conceded that she had received some training from Mr. Campbell, but he sometimes directed her to Ms. Francisco who was often dismissive of her when approached for assistance. She contended that Ms. Francisco repeatedly replied that she was not hired to train respondent and would direct her to seek assistance from Mr. Campbell who would redirect her back to Ms. Francisco (Tr. 355-56, 364-66). Respondent further testified that "boot camp" training commenced in September 2010, only after the unit hired seven new employees (Tr. 357). At that time, an e-mail was sent to the unit, advising them that Ms. Francisco was the appointed instructor (Tr. 358, 365). Notably, petitioner did not call Ms. Francisco as a witness.

The allegations against respondent which are discussed below are grouped as closely as possible by the nature of the activity.

Creation of Duplicate IDs

The TA has an electronic identity system called I-Vault (Tr. 34). According to Mr. Campbell, the duplication of accounts in I-Vault is problematic for the I-Vault drivers that manage each user account. It usually takes unnecessary "man hours" to untangle duplications (Tr. 223, 250-51). Because of the prevalence of duplication problems in the past, Mr. Campbell had issued a warning notice on January 15, 2009, advising staff that the creation of duplicate IDs profoundly affects I-Vault's ability to process user objects correctly, and cautioned that staff who created duplicates would be disabled from creating user accounts for six months (Tr. 227-28; Pet. Ex. 21). Each staff member, including respondent, had signed for receipt of the warning. Petitioner also submitted the transit-wide LAN procedures that were initially issued on January 21, 2001, and re-issued on December 7, 2009, which prohibit the duplication of IDs (Pet. Ex. 19 at 5, No. 7(j)).[2] Mr. Papis testified that the procedures comprise a free-standing document that

[2] Petitioner initially submitted a version of the transit-wide policy with an effective date of May 7, 2010, but later submitted the version to was applicable to the period covering January to May, 2010, the majority period covered by the charges.

was incorporated into the CSC's SOP. The transit-wide procedures are available to staff electronically on the Transit Employee News System (Tr. 86-88).

Petitioner alleged that on January 27, 2010, respondent failed to follow the TA's policy for determining Active Directory IDs, and on April 7 and 12, 2010, she created duplicate Novell accounts for the same users (ALJ Ex. 1, Spec. Nos. 2, 11, 12).

January 27, 2010

Unisys is an outside contractor for the creation of accounts. Unisys forwards the requests for account creation in the form of tickets to the CSC unit. On January 22, 2010, Meredith Luning, Director of Systems Support for the NYC Transit Department of Buses, requested that accounts be created for two contractors with MTA bus passes, including one Frank Vitti (Pet. Ex. 2C). Her request was forwarded to the CSC unit and on January 25, respondent replied that a Novell ID had been created for Mr. Vitti. On January 27, a Unisys representative responded that the user was unable to log in with the new password, and had received an error message that the account was disabled or expired (Pet. Ex. 2C at 2). Mr. Campbell contended that in response to Ms. Luning's request, respondent created an ID without first checking for a pre-existing ID in the same name, and as a result, duplicated an ID that was created two years prior. He asserted that, had respondent conducted a search of "i-manager," the directory services tool, she would have discovered that another account existed in the same name. He stated that the SOPs with which respondent is familiar prescribe the steps that she should have taken. In addition, when she first joined the CSC unit, she received on-the-job training from Nina Francisco and Choi Chan as to duplicate e-directory IDs, and he and others had explained to her multiple times that duplicates were impermissible. Mr. Campbell stated that respondent had previously worked with subways where she created accounts, and was therefore familiar with "directory services" and the "i-manager" tool (Tr. 221-25; Pet. Ex. 2C).

Ms. Francisco resolved the problem and afterwards notified George Schlosser, manager of the "My Access" system, Mr. Papis, Mr. Campbell and Mr. Cheng. Mr. Schlosser revoked respondent's rights "because of her persistent failure to follow procedures," but they were restored within "one week or so" because the unit was short-staffed (Tr. 222; Pet. Ex. 2C).

April 7, 2010

On April 7, 2010, Ms. Francisco e-mailed Mr. Campbell and others that respondent had created duplicate accounts. Ms. Francisco's e-mail contained screen shots of accounts created on

April 28 and December 11, 2009, with duplicate user IDs (Pet. Ex. 11). Respondent objected to the document's admission because the dates of the activity predated the date range (January to July, 2010) in petitioner's overarching allegation of incompetence and/or misconduct. Petitioner explained that the date on the e-mail was the date on which the errors were discovered and moved to conform the specification to the proof.

"No person may lose substantial rights because of wrongdoing shown by the evidence, but not charged." *Murray v. Murphy*, 24 N.Y.2d 150, 157 (1969). However, where a respondent has been put on notice of new charges and had an adequate opportunity to respond, courts have found their addition to be acceptable. *Heck v. Lackawanna*, 44 A.D.2d 763, 763 (4th Dep't 1974). Thus, this tribunal has freely granted motions to amend charges absent prejudice to the respondent. *See, e.g., Law Dep't v. Lawrence*, OATH Index No. 1312/10 at 10 (Mar. 20, 2010); *Dep't of Correction v. Patterson*, OATH Index No. 1884/02 at 11 (Feb. 25, 2003), *adopted in part, rev'd in part*, Comm'n Dec. (May 3, 2003), *modified on penalty*, NYC Civ. Serv. Comm'n Item No. CD 05-09-M (Mar. 10, 2005).

It is undisputed that respondent was timely served with discovery and therefore had an opportunity to review the documents that petitioner intended to submit in support of its allegations. However, at trial, Mr. Papis testified that respondent was not given a performance evaluation prior to January 2010, and indicated that any errors which she might have made in 2009, especially prior to the CSC unit becoming fully operational, were not addressed because they did not affect operations. Hence, I found evidence of respondent's performance in 2009 to be unduly prejudicial, and denied petitioner's motion.

April 12, 2010

On April 12, 2010, Mr. Campbell received an e-mail from Ms. Francisco alerting him to a duplicate Novell account in the name of "SANAIR1" (Pet. Ex. 12). The e-mail displayed what Mr. Campbell referred to as the "creator tool" (Tr. 250), demonstrating that the first user ID for SANAIR1 was created in 2006, and a duplicate was created by respondent on March 18, 2010. At trial, I granted petitioner's motion to amend the specification (No. 12), which erroneously alleged that the duplicate id was created on April 12.

Respondent did not refute petitioner's proof that she created duplicate IDs. She acknowledged that she might have made errors in creating them, but stated that had they been brought to her attention, she would have corrected them. She also contended that when an

account is created, the system does not alert the specialist that one already exists in the same name. Nor does it block the creation of a duplicate account. She maintained that it was only in April 2010 that she was taught how to identify if there was a pre-existing ID/account (Tr. 370-73). Respondent disclaimed knowledge of the transit-wide LAN procedures and their incorporation into the SOP, and noted that there was no reference to them on the SOP index.

I did not credit respondent's testimony. Her rights were initially revoked in January 2010, after she had created the duplicate account for Mr. Vitti. It made no sense that after they had been restored, she would attempt to create accounts without knowing how to avoid duplications. While it is true that there was no reference to the transit-wide procedures on the SOP index, I found it unlikely that the numerous TA policies at the rear of the SOP were assembled solely for trial. In any event, respondent may not avail herself of a defense that she lacked knowledge of a procedure where that procedure was properly published. *Dep't of Finance v. Hatcher*, OATH Index No. 1381/03 at 11 (Jan. 15, 2004), *aff'd*, NYC Civ. Serv. Comm'n Item No. CD 05-20-SA (Apr. 25, 2005). Here, there was no reason for me to doubt Mr. Papis' testimony that the transit-wide procedure was electronically available to staff. Respondent is therefore deemed to have knowledge of them.

Accordingly, the credible evidence established that respondent created duplicate user IDs on March 18, 2010, and I sustain specification 12, and that part of specification 2 that alleged that she failed to follow the policy for determining active directory IDs on or about January 27, 2010. Specification 11 is dismissed because it involved 2009 conduct for which respondent had not received instructions or counseling.

Inadequate Customer Service Responses

Mishandling a Request from a Car Inspector (Specification 1)

Petitioner charged that on January 21, 2010, respondent's handling of a request from a car inspector was unacceptable and she had to be retrained (ALJ Ex. 1, Spec. 1).

"My Access" is a feature that provides employees with a self-service portal through which they may view benefits information. A LAN ID and cubicle number are required for users who have internet access, but not for field employees because they are not assigned cubicles and do not have internet access. According to Mr. Campbell, when an employee seeks assistance with "My Access," the responding CSC worker must first review the help desk tool to determine

if the user has a LAN account or if one needs to be created. None is required if the worker only uses My Access to view benefits (Tr. 220).

On January 21, 2010, a TA car inspector, Larry Thomas, called the CSC help desk seeking assistance with "My Access," and was told that he needed a LAN ID and a cubicle number. Mr. Thomas e-mailed the CSC seeking further assistance (Tr. 213, 217-221). Ms. Francisco responded to Mr. Thomas and resolved the problem (Pet. Ex. 1A at 3). It was unclear from his testimony how Mr. Papis learned of the incident, but he e-mailed Ms. Francisco and Mr. Campbell soon after the matter was resolved, inquiring after whom the inspector had originally contacted (Pet. Ex. 1A at 2). By e-mail, Ms. Francisco identified respondent as the worker who had not only provided inaccurate information, but created a LAN ID for Mr. Thomas. Embodied in the e-mail was a screenshot of Mr. Thomas's demographics which showed "EBENEFITS" under his entitlement information and revealed that he was a car inspector. Mr. Papis instructed Mr. Campbell to re-train respondent and provide her with copies of "applicable resolving flowcharts" to avoid such occurrences in the future (Pet. Ex. 1A). The flowcharts are contained in the SOP under "MYACCESS Login Troubleshooting" (Pet. Ex. 18 at 197).

Respondent could not recall the service to Mr. Thomas, and did not deny knowing the appropriate steps she should have taken in response to his request. Rather, she suggested that she might have been overwhelmed with work. Even if respondent was busy, Mr. Thomas' demographic information, which respondent appears to have overlooked, was a clear indicator that he did not need internet access and therefore, no LAN ID was required.

Thus, that portion of specification 1 that alleges that respondent handled the request of a car inspector in an unacceptable manner is sustained.

Failing to Provide Internet Access & Failing to Follow Proper Format for Novell Account (Specification 2)

On January 27, 2010, Mr. Cheng received an e-mail from a college intern, Ms. Yao, advising him that she had received a call from a user, Douglas Connett, who had been unable to access the internet. Ms. Yao had checked the user's Novell account and discovered that Mr. Connett had not been assigned a group membership ID. Embodied in Ms. Yao's e-mail was a screen shot of respondent's confirmation to Mr. Connett on December 23, 2009, that an internet account had been created (Pet. Ex. 2A). According to Mr. Cheng, providing internet access is a two-step process. In addition to creating an internet account for the user, a group membership ID

must also be assigned. Because respondent overlooked the latter step, the user was unable to access the internet (Tr. 287).

Respondent objected to the document's admission because her action occurred on December 23, 2009, and not January 27, 2010, as alleged. While noting that petitioner repeatedly misidentified the actual dates of respondent's action that it charged as misconduct or incompetence, I admitted the document into evidence over respondent's objection. *See Dep't of Correction v. Patterson*, OATH Index No. 1884/02 at 11 (Feb. 25, 2003), *aff'd in part, rev'd in part*, Comm'r Dec. (May 9, 2003), *modified on penalty*, NYC Civ. Serv. Comm'n Item No. CD 05-09-M (Mar. 10, 2005) (specification conformed to the credible evidence at trial); *Dep't of Correction v. Sostre-Valentin*, OATH Index No. 1923/99 at 8 (Sept. 22, 1999), *aff'd*, NYC Civ. Serv. Comm'n Item No. CD 00-94-SA (Nov. 14, 2000) (appropriate to conform charge to correspond to the proof since respondent and all other witnesses were well aware of the incident charged).

Also on January 27, 2010, Mr. Cheng received an e-mail from Ms. Francisco notifying him that in response to an Internet Access request from one Sandra Arellano, respondent had renamed the Novell account for that user, assigning only the first name of the user as the login ID, which was contrary to the TA policy (Tr. 295-97; Pet. Exs. 2B, 19 at 5). Attached to the e-mail was a screen shot of the demographics, contact information, and account information and status, which showed respondent as the person modifying the user's ID. Mr. Cheng testified that as a result of respondent's actions, internet access could not be assigned to the user (Tr. 297).

Respondent addressed neither allegation. In any event, because it involved 2009 conduct for which respondent had not received instructions or counseling, that portion of specification 2 alleging that respondent failed to complete the two-step process required to provide internet access to Mr. Connett is dismissed. However, I also find that respondent failed to follow the format prescribed in the TA policy for assigning a Novell account ID. Therefore, that portion of the allegation is sustained.

Failing to Update Tickets (Specification 5)

Mr. Papis testified that everyone on duty in the CSC must review open tickets at least three times per shift. On February 18, respondent's shift was 8:00 a.m. to 12:00 p.m. That morning, "Peregrine" tickets were opened at 7:44 a.m. and 8:15 a.m. respectively, for one employee who could not logon and another who had an I-Vault password issue. "Peregrine" is

the name of the system through which tickets are opened in the TA system and Unisys manages the tickets (Tr. 64-65). Unisys usually handles ID-related problems for the MTA but complicated problems are forwarded to the CSC unit. The CSC specialist must attempt to resolve the matter, or if too complex, refer it to one of the supervisors.

Petitioner submitted an e-mail from Nina Francisco to Mr. Campbell, Mr. Papis and Mr. Cheng, at 11:11 a.m. on February 18, informing them that two tickets had been opened earlier that morning during respondent's shift, and had not been updated (Pet. Ex. 5). Embodied in the e-mail was a screenshot of the tickets displaying, among others, two columns with dates and times. The first column reflected the time that the tickets were received by Unisys and the second, the time when Unisys forwarded the tickets to the CSC. Mr. Papis claimed that respondent's failure to address the tickets precluded two employees from being able to access their e-mail account for hours. He acknowledged that respondent was the sole employee in the command center and that one of the tickets came in 15 minutes before her shift started, but asserted that within a reasonable time, she should have checked the inbox and tried to resolve the problems on any tickets therein (Tr. 169-70). By e-mail, he directed Mr. Campbell to instruct respondent on her duties and responsibilities and have her sign a statement acknowledging them. He testified that he understood that mistakes can be made, but when they become repetitive, some form of disciplinary action must be considered.

Respondent challenged petitioner's proof that she had not yet addressed the tickets reflected in the screenshot at the time that Ms. Francisco's e-mail was generated. Mr. Papis countered that the Peregrine system could have verified the time but he had not checked it. He accepted Ms. Francisco's e-mail as true because, otherwise, he would "have to presume that [Ms. Francisco] is fabricating this document for some reason, you know" (Tr. 167-69).

Respondent also maintained that she had not been made aware that those tickets had not been updated. If they were, a possible reason for such an oversight was if she was handling 20 to 30 tickets. Indeed, Mr. Campbell testified that besides e-mails and voicemails, the CSC workers, who typically work in teams, might receive 15 to 30 calls on a light day and 50 to 60 calls on a busy day (Tr. 263). Thus, I find reasonable, respondent's position that, as the sole employee in the command unit that morning, she was possibly consumed with work.

On the other hand, petitioner's evidence was insufficient to establish that at 11:11 a.m., the tickets forwarded by Unisys approximately three hours earlier, had not yet been processed.

Ms. Francisco did not testify, and petitioner did not provide verification of the time from the Peregrine system.

Accordingly, specification 5 is not sustained.

Failing to Follow Protocol (Specifications 7, 8)

Petitioner alleged that respondent failed to follow protocol on February 23 and March 5, 2010, causing the delay of a service request, and delay in restoring access for expired accounts.

February 23, 2010

Petitioner submitted a stream of e-mails spanning January 25 through February 23, 2010 (Pet. Ex. 7). They reveal that on January 25, a ticket was opened by Unisys' Kumar Suresh, requesting that Novell and Active Directory (AD) accounts for user Michael Ramdass be created. A Novell account permits users access to files and printers, and an AD account permits users to access applications and use e-mail. The user must complete and fax a form to Unisys for the accounts to be created. On February 5, 2010, Unisys forwarded Mr. Ramdass' form to the CSC unit. Respondent accepted the ticket on the same day and referred it back to Unisys with an update that a Novell account had been created.

Mr. Papis contended that even though the CSC does not create AD accounts, after completing her part, respondent should have forwarded the request for the AD account to the appropriate unit and followed up on it, but she failed to do so. The e-mails demonstrate that a few hours after receiving respondent's referral, Neelmani Singh of Unisys informed the CSC that the AD account had not been created. On February 17, Mohamed Barry from Unisys advised the CSC that Mr. Ramdass had an I-Vault account but the AD account had not been automatically created. Mr. Papis testified that the matter was ultimately resolved by Nina Francisco on February 22. The e-mails reveal that on February 19 and 22, Ms. Francisco contacted Unisys to notify them that she had been unable to reach Mr. Ramdass, but he needed to activate his I-Vault account and contact Peter Giang of the AD unit (Pet. Ex. 7 at 2). On February 23, Ms. Francisco e-mailed Mr. Campbell, Mr. Cheng and Mr. Papis with her overview of what should have been done (Pet. Ex. 7). Mr. Papis claimed that by returning the ticket to Unisys instead of forwarding it to AD, respondent mishandled the matter (Tr. 172). He reacted to Ms. Francisco's e-mail by directing Mr. Campbell to instruct respondent on how to handle "the 'in-scope' and 'out-of-

scope' for I-Vault user account requests." He further asked Mr. Campbell to "verify that the appropriate procedure recorded in [the CSC] SOP is adequate and correctly reflects all steps."

Mr. Papis maintained that the procedure is clearly outlined on pages 43 and 44 of the SOP (Pet. Ex. 18). Page 43 was headed "Using I-Vault Help Desk Tool." It provided a series of steps that the CSC operator needed to use to access a user's account information and status. Page 44 displayed a screenshot of the Account Information and Status. The first line provided a field to indicate whether the user's I-Vault status was active. The line for Active Directory ID reflected a user name. Mr. Papis asserted that there would be no data in that field if the user had no AD. Nothing in the text below the screenshot instructed what steps should be taken if data was absent in that field.

Respondent contended that the length of time that elapsed between her response and the eventual resolution of the ticket was not entirely attributable to her. According to her, Unisys was aware since February 5 that an AD needed to be created. Mr. Papis contended that the person who accepts a ticket is responsible for ensuring its successful resolution (Tr. 195). Once the ticket reappeared in CSC's ticket bucket, respondent should have recognized the number and opened it again, to determine why it had been returned. He conceded, however, that once Unisys was made aware on February 17 that the user should contact AD, they bore some culpability from then until full resolution (Tr. 175-79, 195-96).

Here again, the allegation that respondent failed to follow protocol should have reflected February 5, and not February 23, the date that the ticket was fully resolved. Accordingly, I *sua sponte* conformed the allegation to the proof.

While it made sense that the person accepting the ticket should ensure that all necessary steps are taken towards its resolution, the only document suggesting that respondent bore the burden of forwarding the ticket to the AD unit for an account to be created was Ms. Francisco's e-mail. Certainly, the SOP was not instructive as to the steps respondent should have taken when the text box contiguous to the active directory box was blank. Moreover, Mr. Papis even asked Mr. Campbell to verify that the procedure in the SOP was adequate, thereby signaling doubts as to its clarity and guidance.

Because I found the SOP to be non-instructive as to the steps that respondent needed to follow with respect to Mr. Ramdass' request, I could not fault respondent for failing to forward the ticket to the AD unit. Accordingly, Specification 7 is not sustained.

March 5, 2010

On March 5, 2010, Ms. Francisco notified Mr. Campbell, Mr. Papis and Mr. Cheng that for a second time that week, tickets on which respondent had worked had been returned to the unit because respondent, after addressing the Novell side of the respective user accounts, had failed to forward them to the AD group. Attached to Ms. Francisco's e-mail were screen shots of Peregrine tickets which displayed requests for extensions of expiration dates for users Bojean Boucka-ezeh and Susan Vazquez. In both cases, after setting new expiration dates, respondent returned the tickets to Unisys on March 1 and 2, respectively, notifying them of the new dates (Pet. Ex. 8). In her e-mail, Ms. Francisco asserted that "it is common sense that if the request is for both system (Novell and AD) that we need to refer the ticket to the sec-messaging group so that the account on the AD side will get extended as well." According to her, the same procedure for the opening of Novell and AD accounts (discussed above) should have been emulated.

At trial, Mr. Cheng referred to page 90 of the SOP, which instructed how a ticket should be forwarded to another group (Pet. Ex. 18). It provided that, using the drop-down menu, the "Primary Assignment Group" should be changed to the group to which the ticket was being forwarded. However, it was lacking in direction as to the conditions under which tickets should be forwarded to another group. Both Mr. Papis and Mr. Cheng expected a certain level of expertise because of respondent's title. While that was not unreasonable, I found an absence of clear direction as to when tickets should be forwarded to another group. Moreover, even though there was a previous instance of respondent failing to forward a ticket to the AD group, there was no evidence that it was brought to her attention, or that Mr. Campbell had ever retrained her in accordance with Mr. Papis' e-mail of February 23 (Tr. 304-05).

In sum, while there is no dispute that respondent failed to forward the tickets to the AD group, I did not find that failure indicative of incompetence. Therefore, Specification 8 is not sustained.

Referring Customer to Another Group (Specification 13)

Respondent is accused of failing to provide customer service on April 14, 2010, when she referred a customer to another group instead of resetting the customer's password. The documentary evidence, which was undisputed, established that the underlying incident that gave

rise to the allegation occurred on April 13th, not the 14th. Again, I *sua sponte* conformed the specification to the evidence.

On April 13, 2010, Choi Chan, a TA employee from the Information Technology Unit, but not part of the CSC unit, e-mailed respondent, under copy to Ms. Francisco, a request for assistance for an MTA Bus Company employee who had been unable to logon to the internet (Pet. Ex. 13A). Respondent replied that trouble or call tickets must be sent to CSC Notification Group, which, Mr. Papis explained, included the entire unit. Ms. Chan re-sent her e-mail to the entire unit and the matter was resolved by one of the TA's college interns. Mr. Papis claimed that the CSC Notification Group should only be implicated in the resolution of a complex problem that has to be escalated and needs widespread input. In this case, the problem was relatively trivial and would have taken approximately five to twenty minutes to resolve. He maintained that "common sense" dictated that the customer should have been assisted because the unit operates by the motto of "customer first." Thus, once the CSC's help is sought, providing service should be primary (Pet. Ex. 13A at 1). Mr. Papis admitted that there was no written policy governing "these types of requests from users" but alluded to memos that Mr. Cheng had issued delineating the responsibilities of the unit, as guidance.

Petitioner submitted e-mails dated March 1 and 8, 2010, from Mr. Cheng to the CSC Notification Group and other individuals, with a four-page attachment of amendments to the SOP (Pet. Ex. 13B). Even though Mr. Cheng's e-mails purported to address procedures for the CSC personnel, they lacked any discussion regarding how to deal with trouble tickets. What they did address was vague. For instance, in his March 1, 2010 e-mail, referring to SOPs that he had sent to CSC personnel in December 2008 and April 2009, Mr. Cheng acknowledged that it was difficult to identify the problems that may arise on a daily basis. He further noted that "due to the nature of Security Operations, priorities change on a regular basis and will be communicated to all shifts as necessary." In his March 8, 2010 e-mail, Mr. Cheng indicated that he had attached an amended version of the SOP for CSC personnel and instructed in bold print that it was to be used as a "high level guideline of procedures for CSC personnel." He also expressed that he did not wish to provide guidance on every single procedure or to "have to tell everyone what is expected of [them]." Mr. Papis opined that Mr. Cheng's e-mail was borne out of his dissatisfaction with the performance of the CSC notification group (Tr. 184-85). Mr. Papis emphasized that the CSC's employees' duties, as delineated, included "Answering of CSC

phones and the retrieval of CSC voicemails . . .” as well as initial troubleshooting on all alert notifications (Tr. 99-101; Pet. Ex. 13B). In spite of that, it was apparent from his previous testimony that tickets and e-mail requests for assistance were appropriately directed to a bucket where they were retrieved by the next available CSC agent (Tr. 195).

Respondent was not asked why she responded to Mr. Chan’s request as she did, and she offered no explanation. But it was also unclear why Mr. Chan directed his request to respondent instead of sending it to the bucket where any one of the CSC agents could have retrieved it and worked on it. In any event, I found respondent’s reply was more pragmatic than disrespectful. While customer service was undeniably a priority, Mr. Papis’ testimony that there was no written policy governing “these types of requests from users” was significant and persuasive. Moreover, the absence of specificity in Mr. Cheng’s e-mails created more uncertainty as to what was expected of workers when requests are forwarded to them directly. Thus, because I did not find respondent’s reply to be inappropriate, it was unclear to me that she had violated any rules.

Accordingly, specification 13 is dismissed.

Security Violations

Erroneously Granting Access to I-Vault (Specification 3)

In or around February 2010, the MTA Bus Company was a newly-created state agency and part of the MTA family. Approximately 60 percent of the MTA bus employees were previously employees of private bus companies and therefore not part of the TA system. The remaining 40 percent consisted of employees who transferred to the bus company from the TA. I-Vault manages the IDs of employees who were originally part of the TA system. The IDs for all others are managed manually (Tr. 34). Thus, the status of the MTA employees determines how accounts are created. The CSC unit has a special tool called “I-Vault Helpdesk” which all specialists must review prior to creating an account, to determine whether or not an employee has an ID that is managed by I-Vault. Such a review is part of established procedure (Tr. 39-40).

Petitioner alleges that on February 9, 2010, respondent granted an individual access to I-Vault when none should have been granted.

On January 28, 2010, pursuant to a request from Ms. Luning, a Unisys operator opened a ticket for an account to be created for employee Francis Johnson. On February 1, 2010, Kerry Donovan from Unisys, requested that the CSC unit open tickets for three new bus employee

users, including Mr. Johnson. Ms. Donovan advised that the users "have an MTA Bus BO pass # so they will not be part of the password management system and should be considered a contractor" (Pet. Ex. 3 at 2). On the same day, respondent replied that a Novell account had been created for Mr. Johnson (Pet. Ex. 3 at 2). On February 5, Ms. Luning requested an update from Unisys on the status of the tickets. Her e-mail emphasized that the users were not part of I-Vault and there was no need for I-Vault to be activated for the accounts to be created. On February 5, respondent replied that a LAN ID had already been created for Mr. Johnson and that "USER NEED TO LOGIN NOVELL W/PW." The ticket was referred back to CSC on February 8 by Unisys operator Nazia Nazeer, who advised that she tried to assist the user to activate the I-Vault, but they were unable to, and the user confirmed that he had never done so.

On February 9, 2010, Ms. Francisco noticed the ticket in CSC's inbox, realized that the user was not an I-Vault user, and reported respondent's error to Mr. Campbell, Mr. Papis and Mr. Cheng (Pet. Ex. 3 at 1). Ms. Francisco's e-mail reflected her concern that respondent's "conflicting updates confuses Unisys and makes us look like we do not know what we are doing or at least not reading and investigating before updating the tickets." Mr. Papis insisted that as a result of respondent's error, the user was unable to use his account for eight days from the time that the request was first made. He therefore instructed Mr. Campbell to re-train respondent and find out if there were reasons that prevented her from following established procedures (Pet. Ex. 3 at 1). Mr. Papis expressed that he was more concerned about respondent's failure to follow established procedures than her mistake itself. He added that because his unit was responsible for information security, he could not permit deviation from procedures (Tr. 157-59).

Respondent did not specifically address this allegation but noted that it was entirely possible for her to make errors when preoccupied with tickets, phone calls and e-mails.

Petitioner's allegation that respondent granted I-Vault access to a user in spite of clear notification that the user was not part of the I-Vault system is sustained.

Revealing a Password in an Unencrypted E-mail (Specification 4)

Specification 4 alleges that on February 10, 2010, respondent violated security protocol by revealing the password of a general superintendent in an e-mail.

On February 9, 2010, Ramesh Ballie, a general superintendent in the Bronx, e-mailed CSC for internet access (Pet. Ex. 4). The following day, respondent informed Mr. Ballie by e-mail that he already had internet access. In the meantime, Mr. Campbell e-mailed respondent

with instructions for her to determine whether Mr. Ballie was a consultant or an employee. Respondent was unable to determine Mr. Ballie's status because his pass number did not show up on the "I-Vault Help Desk Tool" (Pet. Ex. 4 at 2). She informed Mr. Campbell that she would set Mr. Ballie's password and e-mail him. When respondent had done so, she notified Mr. Campbell and Mr. Papis that she had contacted Mr. Ballie. The e-mail included Mr. Ballie's password. Mr. Papis stated that in the field of information security, common sense dictates that passwords "should never, ever be sent period by open text," which could be read by anyone. Such a prohibition was basic and fundamental even though there was no written policy, but it was part of common practice that had not changed in his nine years of supervising the unit. He explained that because Mr. Ballie held a relatively senior position, a security breach could have had dire consequences. By e-mail, Mr. Papis admonished respondent that "No password should be sent by email, EVER!" (Pet. Ex. 4 at 1).

Respondent neither disputed the allegation nor defended against it. However, while there was uncontroverted proof that she exposed Mr. Ballie's password in an e-mail, I was not convinced that in the absence of a written policy, or proof that staff was instructed that remitting passwords by e-mail was prohibited, respondent should have known that to do so was strictly impermissible. Her e-mail to Mr. Papis and Mr. Campbell gave me the sense that she wanted to assure them that she was being responsive to the superintendent in a timely manner. Thus, there was insufficient support for petitioner's allegation that remitting a password by e-mail constituted a violation of security policy.

Accordingly, specification 4 is dismissed.

Creating Accounts for Contractors with No Expiration Dates (Specifications 9, 10)

Accounts that are created for contractors must have, at the maximum, a six-month expiration date because of the temporary nature of a contractual relationship. Otherwise, if the account remains active after a contractor's relationship with the TA expires, it may be accessed by anyone who obtains the identity of the previous user (Cheng: Tr. 314).

On March 19, 2010, Ms. Francisco e-mailed Mr. Campbell and Mr. Papis on two separate occasions, notifying them that respondent had created Novell accounts for two contractors, Odetta Sauls and Oneca Mims, with no expiration date (Pet. Ex. 9A). The e-mail contained screenshots of the "modify object" pages for both contractors. The boxes beside the "Account has expiration date" and "Expiration date" were unchecked. Other than Ms. Francisco's

accusations, there was nothing on the screen shots to identify that respondent was responsible for the creation of the accounts. Mr. Campbell explained that "Directory Services" could reveal who opened the account, and speculated that "Nina obviously went into where they can find out the account and look into who created the account via directory services" (Tr. 230-31). Likewise, on March 22, 2010, Ms. Francisco alerted Mr. Papis, Mr. Campbell and Mr. Cheng that respondent had created two additional accounts for contractors without inserting an expiration date. This time, her e-mail contained screenshots of the Novell iManager, as proof that the accounts were indeed created by respondent.

Mr. Campbell testified that not only do the SOPs provide guidance on how a contractor's ID should be set for LAN, remote and internet access, but "My Access" provides similar guidance (Tr. 232). Likewise, Mr. Cheng was adamant that the SOP provided guidance. Petitioner submitted the TA's "User Account Workflow System" (Pet. Ex. 9B), applicable to contractors (Tr. 233). The document informed that the TA's paperless system was being abolished, and delineated instructions for requesting a LAN ID and e-mail account for contractors. The second page of the document contained the following description "This workflow allows you to request a LAN and e-mail account for an NYCT contractor." It was followed by a series of instructions and form details for the contractor. Instruction number 7 read:

> Specify the Expiration Date for this contractor's access. To do this, click on the calendar icon to the right of this field. The expiration date can be no great [sic] than six months from today. When the contractor's access expires, you can request additional access time.

(Tr. 233; Pet. Ex. 9B at 2).

Respondent testified that the "User Account Workflow System" was introduced in February 2010, approximately one month prior to her creation of the accounts for the contractors. She did not dispute that she had created the accounts in question, but argued that she was never trained about setting a six-month expiration date for contractors, there was no procedure or memo, and the SOP did not address the issue (Tr. 359-60, 372). She insisted that Unisys was required to insert an expiration date on its electronic form submission for the contractors for whom IDs and accounts were being requested. Otherwise, she would create the account but not insert one. Indeed, it appeared that the document was intended to provide guidance to the personnel who generated requests for the creation of contractor accounts. This supported

respondent's contention that someone other than the CSC computer specialist was required to insert the expiration date. Besides, it did not make sense that the CSC specialists should be the ones vested with the discretion to set expiration dates for contractors.

In fact, after receiving Ms. Francisco's notification, Mr. Papis e-mailed Mr. Campbell to verify that the SOP procedure for contractors specified how to set the expiration date. If not, it needed to be corrected and re-issued to staff. Mr. Campbell replied that:

> The OLD SOP is not sufficient as it has no mention of LAN/EAMIL (sic) for contractors. The only reference is to Unisys, but they use templates and they do not expire according to the template. We will have to re-do the SOPs in the future, as I am burdened with BSC sftp's at this time.

(Resp. Ex. B).

I find that Mr. Campbell's e-mail fully corroborated respondent's testimony that the SOP did not address the issue, and exonerated her for creating contractor accounts without expiration dates.

Given this evidence presented by respondent, I find no reason to sustain specifications 9 and 10, that respondent created accounts for contractors with no expiration dates.

Failing to Follow Additional Protocol

Accepting a Paper Form Request (Specification 15)

Respondent is charged with providing a LAN ID on or about July 1, 2010, based on a paper form request despite the abolition of paper forms four months prior.

On March 3, 2010, Mr. Schlosser issued a memo to CSC staff, that effective immediately, the paper-based process had been replaced by an electronic workflow system and therefore, paper requests for remote and internet access were no longer to be accepted. On the same day, Mr. Papis issued a clarification that the abolition of the paper form requests was applicable to I-Vault users (Tr. 104; Pet. Ex. 15 at 5). He explained that permitting the parallel operation of the paper process and the electronic process would result in duplication of IDs, where one person would have two IDs at the same time (Tr. 105-06). On June 30, 2010, respondent admitted to Mr. Cheng that she had given LAN entitlement to an employee. Mr. Cheng informed her that the employee should have been instructed to submit a workflow request because he was an I-Vault user, but respondent replied that she could not comprehend how security procedures had been violated because the request had been signed off on by the

employee's manager (Pet. Ex. 15 at 2). As far as she was concerned, she had complied with a manager's request (Tr. 107-09; Pet. Ex. 15 at 1, 2). On July 1, Mr. Papis e-mailed respondent that in spite of what is requested on a ticket, strict adherence to CSC's internal policies is required to prevent security breaches. He opined that she had been provided with sufficient training and re-instructions from him, Mr. Campbell and Mr. Cheng. Moreover, he noted that she should have been very familiar with the CSC procedures because she was the person who had compiled the SOP for the unit.

Respondent did not deny the allegation and offered no testimony in support of her reason for creating a LAN ID based on a paper form request.

The "User Account Workflow System" which, according to respondent, was issued in February 2010, clearly indicated that the paper forms were being discontinued (Pet. Ex. 9B). That, plus Mr. Schlosser's e-mail, as corrected by Mr. Papis on March 3, 2010, was sufficient for me to find that respondent should have known that paper forms for I-Vault users were unauthorized.

Accordingly, Specification 15 is sustained.

INCOMPETENCE

Petitioner's rules provide that employees must be familiar with and obey the rules that govern their particular duties and special instructions issued by their supervisors, and must perform their duties in accordance with those rules, policy instructions and their division's instructions. MTA NYC Transit Auth., Rules and Regs., Chp. 1, Rules 2(d), 4(a), 4(b) (Nov. 2003).

Here, the credible evidence established that respondent: created duplicate IDs on January 25 and March 18, 2010 (Specs. 2, 12); provided inaccurate information to a field inspector seeking assistance in accessing his benefits online (Spec. 1); failed to follow the proper format for assigning a Novell account ID on January 27, 2010 (Spec. 2); erroneously granted I-Vault access to an employee who was not part of the I-Vault system (Spec. 3); and created a LAN ID based on a paper request when such format had been abolished and replaced with electronic forms (Spec. 15). Petitioner contends that these failures demonstrate that respondent is incompetent in that she is unfamiliar with the tasks necessary to successfully accomplish her job.

Incompetence is defined as either the inability to perform one's job or the persistent unwillingness or failure to do the work. *Law Dep't v. Stanley*, OATH Index No. 1540/05 at 4 (June 15, 2005), *aff'd*, NYC Civ. Serv. Comm'n Item No. CD 06-08-SA (Jan. 9, 2006). As distinct from misconduct, fault on the part of the employee is not necessarily required to establish incompetence. Petitioner need only prove that respondent is unable to meet the minimally acceptable threshold requirements of the duties of her title. *Employers Retirement System v. Myrick*, OATH Index No. 505/95 at 20 (Apr. 11, 1995).

In considering charges of incompetence, this tribunal has distinguished between making errors, which all employees make on occasion, and making "constant and repetitive errors." *Transit Auth. v. Ondeje*, OATH Index No. 1339/04 at 13 (Dec. 30, 2004); *compare Dep't of Housing Preservation & Development v. Hand*, OATH Index No. 2594/10 (Sept. 2, 2010) (incompetence found where respondent improperly processed 125 appointments), *with Fire Dep't v. Hodge*, OATH Index No. 574/06 (May 18, 2006) (no incompetence found where respondent made five isolated errors). Several factors are considered when distinguishing minor errors from incompetence, including: the frequency of the errors in comparison to those made by other employees and the consequences of the errors, in terms of time spent by respondent's supervisor to monitor respondent. *Hodge*, OATH 574/06 at 7; *Human Resources Admin. v. Green*, OATH Index No. 1794/02 at 19 (Dec. 6, 2002), *aff'd*, Civ. Serv. Comm'n Item No. CD 06-78-SA (Aug. 23, 2006); *Financial Information Services Agency v. Boritz*, OATH Index No. 744/91 at 18 (Apr. 16, 1991), aff'd, NYC Civ Serv. Comm'n Item No. CD 91-147 (Dec. 10, 1991). Notice to respondent that his performance is viewed as inadequate "is a necessary part of an incompetence case." *Ondeje*, OATH 1339/04 at 12.

Petitioner asserts that respondent's performance parallels the respondent's in *Transit Authority v. Wong*, OATH Index No. 1866/08 (Aug. 28, 2008). Undeniably, respondent made mistakes, but I disagree with petitioner's contention. In *Wong*, the record overwhelmingly supported a finding of incompetence. The evidence established Mr. Wong had trouble performing tasks that someone in his position should be able to do; his frequent errors were based on a lack of knowledge and understanding of various computer systems which were necessary to perform his job. Supervisors spent hours trying to explain his tasks to him to no avail and informed him that he was not performing at the requisite level. This monopolization of his supervisors' time had an adverse effect on the workplace. That was not the case here.

Respondent made six errors over six months. There was no evidence that these errors were repetitive. On the contrary, Mr. Papis affirmed that when brought to her attention, they were not repeated. Nor was there any evidence that respondent's work performance required supervisors to spend inordinate time monitoring her. Further, I was not persuaded that she was unable to process what was requested of her or perform simple tasks. Indeed, while Mr. Papis expressed frustration at respondent's errors, some of her mistakes dismayed him because she had previously performed similar tasks without a hitch. That belies any suggestion that respondent is unfamiliar with the rules and particular duties that govern her job. In fact, I found it more likely than not that respondent's errors were caused by isolated judgment errors. In any event, there was nothing to establish that respondent was ever told that her work was inadequate.

In short, petitioner failed to prove by a preponderance of the credible evidence that respondent's errors were willful, or that there was such a proliferation of them so as to deem her incompetent.

As a corollary, it appears that other factors contributed to respondent's performance. The issue of her training was of some concern to me. Petitioner's witnesses testified that she was trained by Ms. Francisco, but Ms. Francisco was not made available for trial to testify as to the time that she devoted to respondent's training, the nature of the training, and her evaluation of respondent from an instructor's perspective. Notably, as teacher/instructor, she never appeared to notify respondent of her errors, or address their resolution with respondent. Rather, she seemed focused on uncovering and reporting them to the supervisors. I found that to be uncharacteristically odd behavior for an instructor. Moreover, none of the e-mails from Mr. Papis, Mr. Cheng, nor Mr. Campbell ever directed Ms. Francisco, as instructor, to re-train respondent. Mr. Campbell was the only who received those directions, leaving me to credit respondent's testimony that she was not trained by Ms. Francisco, but received some training from Mr. Campbell.

FINDINGS AND CONCLUSIONS

1. Petitioner established that respondent committed misconduct when she shouted and yelled at her supervisor on January 21, 2010 (Specification 1).

2. Respondent is guilty of misconduct for failing to comply with her supervisor's request to handle a specific voice message on February 18, 2010 (Specification 6).

3. Petitioner failed to establish that respondent deliberately failed to provide a report by the due date of July 1, 2010 (Specification 16).

4. Petitioner established that respondent is guilty of misconduct for failing to comply with the director's request to update the Standard Operating Procedures when she had confirmed that she had done so (Specification 17).

5. Petitioner established that respondent failed to follow policy and created duplicate user IDs on March 18, 2010 (Specification 12). Specification 11, which alleged that respondent created duplicate user IDs in 2009 is dismissed.

6. Petitioner established that on January 21, 2010, respondent mishandled a car inspector's request for assistance in accessing "My Access." (Specification 1).

7. Petitioner established that on or about January 27, 2010, respondent failed to follow the policy for determining Active Directory IDs, and failed to follow the TA policy for assigning a Novell account ID. That portion of the allegation that on or about the same date, respondent failed to provide a Superintendent access to the internet is dismissed. (Specification 2).

8. Petitioner failed to prove that respondent neglected to update tickets on February 18, 2010 (Specification 5).

9. Petitioner failed to establish that respondent was at fault for failing to forward tickets to the Active Directory unit on February 23 and March 5, 2010. (Specifications 7, 8).

10. Petitioner failed to establish that respondent violated any rules or policy when, on April 13, 2010, she referred a ticket elsewhere instead of resetting a password. (Specification 13).

11. Petitioner established that on January 28, 2010, respondent granted I-Vault access to a user, in spite of clear notification that the user was not part of the I-Vault system (Specification 3).

12. Petitioner failed to establish that there was any clear policy that respondent violated when, on February 9, 2010, she revealed a user's password in an unencrypted e-mail. Accordingly, Specification 4 is dismissed.

13. Petitioner failed to establish that respondent was at fault for creating contractors' accounts without expiration dates on March 19, 2010. (Specifications 9, 10).

14. Petitioner established that on July 1, 2010, respondent provided a LAN ID in response to a request by paper form, which had been abolished four months prior. (Specification 15).

RECOMMENDATION

Upon making the above findings and conclusions, I requested and reviewed a copy of respondent's personnel file in order to make an appropriate penalty recommendation. Respondent has worked for the City of New York since 1980 and has been employed by petitioner since 1982. During her almost 30 years with the Authority, respondent has held the following positions: Manhole Inspector, Office Aide Level I, Office Aide Level III, Office Associate, Associate Word Processor, Technical Aide Level II, and her current title of Computer Specialist Level I. In January 2009, respondent was charged with being absent without leave authorization (AWOL) on one occasion. There is no indication that that charge was sustained. Otherwise, respondent appears to have no disciplinary history.

In her last three performance reviews for the periods ending December 2007, 2008 and 2009, respondent received an overall rating of "fully satisfactory." The 2009 review, signed by respondent and her supervisor on January 19, 2010, was particularly significant because it covered a period during which respondent was alleged to have made errors that were overlooked because the CSC was not yet in full production. Respondent received "SP" or "superior performance" for her relationship with customers and co-workers, for her attendance record, and for the condition in which she maintains her work area. For all other areas, she received "FS" or "fully satisfactory." Her technical skills were deemed adequate, and it was noted that she always asks questions, documents the answers, and increases her technical knowledge base. For quality and quantity of work, the review reflected that respondent "consistently delivers good quality, and quantity of work." For creativity and initiative, it indicated that she "has demonstrated

creativity in many tasks assigned to her, it is seen in her work on the SOP project and the LAN/Email/Internet task that she performs every day."

At trial, petitioner sought respondent's demotion. Because the record does not demonstrate that respondent is incompetent, I find demotion to be inappropriate. However, respondent was found guilty of shouting at her supervisor and failing to comply with her supervisors' requests to handle a specific voice message and update the SOP. Therefore, some penalty is warranted.

In cases where employees were found to have disobeyed their supervisor's order and/or engaged in cursing or threatening a supervisor, this tribunal has imposed penalties ranging from five to thirty-three days' suspension without pay, and in extreme circumstances, termination. *See Transit Auth. v. Felix*, OATH Index No. 1206/09 (June 16, 2009) (eight days suspension for multiple instances of rude and discourteous behavior and insubordination); *Transit Auth. v. Bernard*, OATH Index No. 1805/02 (Dec. 3, 2002) (15-day suspension for insubordination, penalty mitigated by long tenure and unblemished record); *Transit Auth. v. Wagh*, OATH Index No. 517/02 (July 11, 2002), *modified on penalty*, Comm'r Dec. (Aug. 8, 2002) (30-day suspension for what the Authority characterized as gross insubordination, involving repeated refusals to perform assigned work over a five to six week period); *Bd. of Education v. Fuccio*, OATH Index No. 924/01 (June 21, 2001), *aff'd*, NYC Civ. Serv. Comm'n Item No. CD 03-37-SA (Apr. 11, 2003) (termination recommended for respondent's refusal to follow a lawful order, threatening one supervisor, and screaming at and punching another); *Transit Auth. v. Walker*, OATH Index No. 864/98 (Dec. 24, 1997) (10-day suspension for respondent guilty of insubordination for failure to maintain orderly work area; late arrivals to work; and failure to register end of lunch period in computerized timekeeping system); *Transit Auth. v. Smallwood*, OATH Index No. 442/96 (Aug. 8, 1997) (33-day suspension for engaging in a loud, angry tirade toward supervisor; excessive absence; neglect of duties; willful failure on several occasions to perform productive work; failure on one occasion to report to another supervisor for work assignments; and 16 time and leave violations); *Transit Auth. v. Flowers*, OATH Index No. 562/91 (Feb. 18, 1991), *modified on penalty*, NYC Civ. Serv. Comm'n Item No. CD 92-52 (May 8, 1992) (where office associate was guilty of three instances of discourtesy/disrespect, yelling at her supervisor, and other misconduct, penalty reduced to five-day suspension taking into account 20-year tenure and limited prior discipline).

As previously discussed, while I found respondent guilty of insubordination for shouting at her supervisor, her behavior was not so outrageous as to warrant a harsh penalty. Rather, respondent's misconduct must be balanced by her long tenure and lack of disciplinary history. *See Dep't of Transportation v. Jackson*, OATH Index No. 299/90 at 13 (Feb. 6, 1990) ("employees should have the benefit of progressive discipline wherever appropriate, to ensure that they have the opportunity to be apprised of the seriousness with which their employer views their misconduct and to give them a chance to correct it"). Accordingly, for this instance of insubordination, I recommend that respondent be suspended without pay for five days.

For respondent's failure to comply with Mr. Campbell's request to handle a voice message, I find a five-day suspension without pay to be appropriate.

I found respondent's failure to fully comply with Mr. Cheng's requests to update the SOP, to be more serious because the procedures affect the entire unit and are required to be kept current. Accordingly, for this instance of misconduct, I find a 15-day suspension without pay to be appropriate.

In sum, for the charges sustained, I recommend that respondent be suspended without pay for 25 days.

Ingrid M. Addison
Administrative Law Judge

March 3, 2011

SUBMITTED TO:

ANITA MILLER
Vice President for Labor Relations

APPEARANCES:

CRAIG COSTA, ESQ.
JUDITH BUCKLEY, ESQ.
Attorneys for Petitioner

BROWN & GROPPER, LLP
Attorneys for Respondent
BY: JAMES A. BROWN, ESQ.

NYC Civ. Serv. Comm'n Decision, Item No. CD 11-61-SA (Aug. 30, 2011)

THE CITY OF NEW YORK CIVIL SERVICE COMMISSION

In the Matter of the Appeal of:
ALEXANDRIA VICTOR
Appellant
-against-
NYC TRANSIT AUTHORITY
Respondent

Pursuant to Section 76 of the New York State Civil Service Law

---

PRESENT:

RUDY WASHINGTON, COMMISSIONER
VICE CHAIR

CHARLES D. MCFAUL, COMMISSIONER

ALINA A. GARCIA
DIRECTOR/GENERAL COUNSEL

AMANDA M. WISMANS
ATTORNEY FOR THE COMMISSION

JAMES BROWN, ESQ.
REPRESENTIVE FOR APPELLANT

MARIEL TANNE, ESQ.
REPRESENTATIVE FOR RESPONDENT

APPELLANT PRESENT

STATEMENT

On Thursday, August 18, 2011 the City Civil Service Commission heard oral argument in the appeal of **ALEXANDRIA VICTOR**, Computer Specialist I, NYC Transit Authority (NYCTA), from a determination by the NYCTA, finding her guilty of charges of incompetency or misconduct and imposing a penalty of **25 DAYS SUSPENSION**, following an administrative hearing conducted pursuant to Civil Service Law Section 75.

COMMISSIONERS' FINDINGS

After a careful review of the testimony adduced at the departmental hearing and based on the record in this case, the Civil Service Commission finds no reversible error and affirms the decision and penalty imposed by the New York City Transit Authority.

NANCY G. CHAFFETZ, *Commissioner/Chair*, Civil Service Commission
RUDY WASHINGTON, *Commissioner/Vice Chair*, Civil Service Commission
MATTHEW W. DAUS, *Commissioner*, Civil Service Commission
CHARLES D. McFAUL, *Commissioner*, Civil Service Commission

August 30, 2011