

HEARING OFFICER, CAREER SERVICE BOARD, CITY AND COUNTY OF DENVER,  
COLORADO

Appeal No. 265-00

---

**FINDINGS AND ORDER**

---

IN THE MATTER OF THE APPEAL OF:

**STEVE M. SMITH**, Appellant

Agency: DEPARTMENT OF AVIATION, DENVER INTERNATIONAL AIRPORT,  
and THE CITY AND COUNTY OF DENVER, a municipal corporation

---

**INTRODUCTION**

This matter comes before the Career Service Board on appeal by Steve M. Smith (hereinafter "Appellant") filed December 18, 2000. Appellant challenges the Department of Aviation, Denver International Airport's (hereinafter "Aviation" or "Agency") decision to suspend his employment for five days without pay after Appellant allegedly used Agency computer equipment to contact inappropriate Internet sites.

A hearing in this matter was held before Personnel Hearing Officer Joanna L. Wilkerson ("hearing officer") on April 23, 2001 at the Career Service Authority Offices. Appellant was present and represented himself. The Agency was represented by Assistant City Attorney Robert D. Nespor, with Aviation Human Resources Assistant Manager, James Thomas, present for the entirety of the proceedings and serving as advisory representative for the Agency.

Witnesses for the Agency included Mr. Thomas, Aviation's Assistant Deputy Manager Edward T. Currier, Engineering Supervisor Mike H. Steffens, and Senior Network Administrator Michael Wright.

Appellant's witnesses included Mr. Wright, DMJM Aviation Contract Employee James T. Adams, and Appellant himself.

The parties stipulated to the admission of Agency's Exhibits 1 through 7 and Appellant's Exhibit A. No additional exhibits were offered or admitted.

For purposes of the Findings and Order, the Rules of the Career Service Authority shall be abbreviated as the "CSR" with a corresponding numerical citation.

## NATURE OF THE CASE

The Agency posits that it had just cause to suspend Appellant for five days as follows. In January of 2000, Aviation management became aware of certain inappropriate access of the Internet by employees using Agency computer equipment. In response, the Agency revised its policy concerning the use of Agency computer equipment, and management held a meeting with all supervisors informing them of the problem. The various department supervisors then instructed their employees during subsequent staff meetings of the policy revisions, and directed them to refrain from any further such inappropriate access in the future in lieu of disciplinary action.

The Agency asserts that despite this mandate from management, Appellant made inappropriate web contacts on five different occasions in April and May of 2000. These contacts were detected by the Management Information Services ("MIS") computer scanning system and the Agency issued Appellant a Verbal Reprimand on June 5, 2000. The Agency attached a copy of the revised Agency policy to the Verbal Reprimand.

The Agency further asserts that despite this Verbal Reprimand, three months later Appellant again engaged in inappropriate web contacts during four different days in September and October of 2000. Again, the Agency's computer detection system generated a report of these contacts. As a result, and taking into consideration Appellant's previous Verbal Reprimand, the Agency issued Appellant a Notice of Contemplation of Disciplinary Action on November 13, 2000. After a meeting was held giving Appellant the opportunity to respond to these charges, and a subsequent investigation of the MIS detection devices and controls, the Agency issued Appellant the five-day suspension without pay, giving rise to this appeal.

Appellant first responds that he was not at the January 2000 meeting where the problem was first discussed, and that he was completely unaware of the edicts and policy revisions concerning inappropriate use of the Internet. Appellant admits, with some degree of embarrassment and contrition, to making the inappropriate contacts in April and May of 2000. Appellant argues in his defense that these contacts were partly out of curiosity, and partly out of concern over the prospect of buying a home computer, where his two young daughters live and might gain such access. He asserts that the Verbal Reprimand and attached Agency policy were his first exposure to the Agency's stance on the issue. At that time, Appellant posits, he ceased all such inappropriate web activity permanently.

Second, in light of his cessation of such activity, Appellant asserts that he was taken completely by surprise when he was issued the November 13, 2000 Notice of Contemplation of Disciplinary Action. Appellant offers the following possibilities in explanation for this second round of activity. Either the web sites were generating additional contacts to his home site without his knowledge, or another individual had gotten access either to his password or to his computer itself. Appellant points to the fact that the Agency admits anyone using Appellant's user name and password could have caused the report from any terminal in the system. In addition, the MIS reports did not reflect which actual computer terminal was used to engage in the contacts. Furthermore, despite the Agency's capability to ascertain which computer terminal was being used, it failed to do so. Finally, Appellant points out that the Agency failed to

## NATURE OF THE CASE

The Agency posits that it had just cause to suspend Appellant for five days as follows. In January of 2000, Aviation management became aware of certain inappropriate access of the Internet by employees using Agency computer equipment. In response, the Agency revised its policy concerning the use of Agency computer equipment, and management held a meeting with all supervisors informing them of the problem. The various department supervisors then instructed their employees during subsequent staff meetings of the policy revisions, and directed them to refrain from any further such inappropriate access in the future in lieu of disciplinary action.

The Agency asserts that despite this mandate from management, Appellant made inappropriate web contacts on five different occasions in April and May of 2000. These contacts were detected by the Management Information Services ("MIS") computer scanning system and the Agency issued Appellant a Verbal Reprimand on June 5, 2000. The Agency attached a copy of the revised Agency policy to the Verbal Reprimand.

The Agency further asserts that despite this Verbal Reprimand, three months later Appellant again engaged in inappropriate web contacts during four different days in September and October of 2000. Again, the Agency's computer detection system generated a report of these contacts. As a result, and taking into consideration Appellant's previous Verbal Reprimand, the Agency issued Appellant a Notice of Contemplation of Disciplinary Action on November 13, 2000. After a meeting was held giving Appellant the opportunity to respond to these charges, and a subsequent investigation of the MIS detection devices and controls, the Agency issued Appellant the five-day suspension without pay, giving rise to this appeal.

Appellant first responds that he was not at the January 2000 meeting where the problem was first discussed, and that he was completely unaware of the edicts and policy revisions concerning inappropriate use of the Internet. Appellant admits, with some degree of embarrassment and contrition, to making the inappropriate contacts in April and May of 2000. Appellant argues in his defense that these contacts were partly out of curiosity, and partly out of concern over the prospect of buying a home computer, where is two young daughters live and might gain such access. He asserts that the Verbal Reprimand and attached Agency policy were his first exposure to the Agency's stance on the issue. At that time, Appellant posits, he ceased all such inappropriate web activity permanently.

Second, in light of his cessation of such activity, Appellant asserts that he was taken completely by surprise when he was issued the November 13, 2000 Notice of Contemplation of Disciplinary Action. Appellant offers the following possibilities in explanation for this second round of activity. Either the web sites were generating additional contacts to his home site without his knowledge, or another individual had gotten access either to his password or to his computer itself. Appellant points to the fact that the Agency admits anyone using Appellant's user name and password could have caused the report from any terminal in the system. In addition, the MIS reports did not reflect which actual computer terminal was used to engage in the contacts. Furthermore, despite the Agency's capability to ascertain which computer terminal was being used, it failed to do so. Finally, Appellant points out that the Agency failed to

investigate the security flaws in his office area, which he asserts are a possible source of tampering for which he was not responsible.

In essence, Appellant argues that the Agency had the burden of establishing where the activity was actually coming from and who was responsible for it before accusing him, but that it failed to satisfy that burden. Appellant therefore posits that the Agency has not proven its case, and strongly maintains that he was not responsible for the contacts in September and October of 2000 giving rise to the suspension in question.

The Agency first replies that the MIS report clearly reflects activity deliberately generated from within the office, not solicitations from other locations. Second, even if Appellant's assertions that the access and illicit usage of the net was done by another using Appellant's password or equipment, this means Appellant has failed to safeguard his password and equipment, resulting in a security breach for which Appellant is nonetheless responsible. These failures are also in violation of the Agency policy governing the use of, and access to, the computer system. The Agency maintains that the safeguard of Appellant's password and equipment is ultimately his responsibility, and that either way, the discipline is appropriate.

### ISSUES

1. Whether the Agency has demonstrated by a preponderance of evidence that Appellant himself used Agency computer equipment for inappropriate purposes.
2. Alternatively, whether the Agency has demonstrated by a preponderance of evidence that Appellant failed to maintain his computer security, whereby permitting access to his equipment or password by another.
3. Whether through the actions described above in either 1 or 2, Appellant engaged in :
  - a) Gross negligence in violation of CSR Rule 16-50 A. 1);
  - b) Refusing to comply with the orders of an authorized supervisor in violation of CSR Rule 16-50 A. 7);
  - c) Failure to observe departmental regulations, specifically Aviation Department Standard Policy and Procedure No. 2005, in violation of CSR Rule 16-51 A. 5);
  - d) Sexual harassment in violation of Aviation Department Standard Policy and Procedure No. 100-15.1 and CSR Rule 16-51 A. 5);
  - e) Unauthorized use of Agency equipment in violation of CSR Rule 16-51 A. 7);
  - f) Failure to comply with the instructions of an authorized supervisor in violation of 16-51 A. 10); and/or
  - g) Conduct not specified in CSR Rule 16-50 and 16-51 which may otherwise be cause for discipline.

4. Whether the Agency demonstrated just cause for disciplining Appellant by a preponderance of the evidence.
5. If so, whether the Agency's five-day suspension of Appellant is reasonably related to the seriousness of the offense given the totality of the evidence.

### FINDINGS OF FACT

1. Appellant is a Project Inspector for the Agency's Department of Aviation at Denver International Airport. Appellant is an "exempt" employee, meaning that there are certain CSR Rules governing overtime pay and other regulations from which he is exempt.
2. Appellant has been in his current position since April of 1998 as the result of a promotion that year. While in this position, Appellant began using the Agency's current computer technology resources when he was first assigned a terminal in April or May of 1999.
3. Prior to his use of this system, Appellant's only computer exposure was to a DOS system at his previous place of employment, and a laptop basic system in his previous HVAC post for the Agency. Neither of these systems had Internet access. Appellant's first experience with the Internet was shortly after the assignment of his terminal in 1999.
4. Appellant supervises Aviation Contract Employee James T. Adams. The two moved into the office they presently jointly occupy around the first of the year in 1999 (*see*, Appellant's Exhibit A). This office has floor-to-ceiling walls and a locking door which Appellant and Mr. Adams usually keep locked when they are away. The area of office space indicated in Exhibit A has card-key access and is in a secure area. However, Appellant's office is on a long corridor accessed by non-city tenants renting space from DIA, and by other city employees and contractors. There is a time clock just outside Appellant's office where individuals punch in and out.
5. Appellant and Mr. Adams both do similar types of work. Mr. Adams described a typical day on the job to include frequent departures from the office itself to do on-site inspections, and perform other city contract-related responsibilities which take both Appellant and Mr. Adams away from the office on a frequent and unpredictable basis. Mr. Adams further indicated that while he and Appellant typically lock the door when they are both gone, there are sometimes other individuals in their office for purposes of consultation and planning, and that in his experience, these individuals might on occasion sit at Appellant's desk in front of his computer if Appellant is not there. However, Mr. Adams testified that in his experience, these individuals are not left alone in the office.
6. Both Appellant and Mr. Adams testified that shortly after they moved into this office, there was a ceiling tile out of place in the ceiling outside the office adjacent to theirs, and there were what appeared to be footprints on the walls under the disturbed ceiling tile. However, Appellant and Mr. Adams did not observe anything out of place or otherwise suspicious of a break-in inside their office. Appellant further testified that he knew of one employee who

breached the inside of his office after locking his keys in by going up through the ceiling and over the wall to gain access.

7. Mr. Adams has never seen any inappropriate material on Appellant's computer screen, which is aimed away from the direction of Mr. Adams' desk. There is no evidence that anyone else has ever witnessed any inappropriate material displayed on Appellant's computer screen.
8. The Agency's MIS System includes a scanning device which monitors Internet use and identifies inappropriate web-site contacts through the use of certain "key terms" which are typically associated with pornographic and other inappropriate web sites. The device retrieves lists of these questionable site contacts, and generates an e-mail report to Aviation management. The report identifies the user name, the date, the time, and the name of the web site in question (*see*, Exhibit 5).
9. In or around December of 1999, the Agency became aware that some employees were apparently accessing pornographic and other inappropriate web sites using their terminals at work.
10. On January 1, 2000, the Agency issued a revised Department of Aviation Standard Policies and Procedures Policy No. 2005 (hereafter "Policy 2005") (Exhibit 6). These revisions presumably addressed inappropriate Internet use (Procedure VI. B), and warned users that their Internet activities are subject to monitoring (Procedure VI. C. 2). Policy 2005 also specifically states that each employee is held responsible for maintaining the security of the computer system by guarding and changing their passwords, and the use of screen savers which require password re-entry (Procedure II. B). It further limits the use of Agency computer equipment to "work-related purposes only" (Procedure V. F).
11. On Thursday, January 20, 2000, Aviation Manager Bruce Baumgartner held a meeting with all supervisory staff, detailing the nature of the inappropriate Internet use problem and laying out the procedures for correcting the problem. Mr. Baumgartner distributed a copy of the revised Policy 2005 at the time of this meeting. Thereafter, the various supervisors held staff meetings where they discussed the Internet problem with their employees, directing them to cease any such activities, and notifying them there would be disciplinary action issued in the future for any such subsequent infractions.
12. Engineering Supervisor Mike Steffens, Appellant's supervisor, was one of the supervisors at the January 20, 2000 meeting. Mr. Steffens testified that he held a staff meeting with his employees either Friday, January 21, 2000 or the following Friday. At that meeting, he informed his employees of the Internet problem, the Agency mandate to stop such activity, and the potential for disciplinary proceedings should the activity continue. Mr. Steffens could not recall whether he handed out a copy of the new Policy 2005 at the meeting. Mr. Steffens testified he could not say for certain whether Appellant was in attendance at that meeting, but thought he was. Mr. Steffens was short-staffed at the time and had no minutes of the meeting to establish whether Appellant was at the meeting or not. The Agency could not provide any information otherwise establishing that Appellant was at this meeting.

13. Mr. Steffens testified that MIS has distributed copies of Policy 2005 to employees in the past, and keeps copies bearing the employee's signature indicating they have received the Policy and are therefor constructively aware of its contents. However, the Agency did not offer such a copy signed by Appellant into evidence, or otherwise definitively establish that Appellant had ever seen Policy 2005 prior to his receipt of it as an attachment to his Verbal Reprimand issued June 5, 2000.
14. In April and May of 2000, the MIS tracking device described in paragraph (8) above generated information that a user employing Appellant's user name had gained access to inappropriate web sites for brief periods on April 7, April 14, April 28, May 12, and May 16, 2000. (See, Exhibit 4) This information was forwarded to the Human Resources Department.
15. The Human Resources Department verified the sites were sexually oriented and inappropriate, and notified Assistant Deputy Manager of Aviation, Ed Currier, of the alleged infraction. Mr. Currier consulted with Aviation management, and they determined to issue Appellant a Verbal Reprimand on June 5, 2000 (Exhibit 4). The Verbal Reprimand set forth that the activity was in violation of Policy 2005, ordered Appellant to stop such contacts, and admonished him that any further such activities could result in more severe discipline.
16. On June 6, 2000, Appellant met with Mr. Currier, who issued the Verbal Reprimand to Appellant (Exhibit 4) with a copy of revised Policy 2005 (Exhibit 6) attached. Appellant acknowledged the inappropriate Internet activity indicated in the Verbal Reprimand (see, Exhibit 4), and the two discussed the activity in question. Appellant signed the document, and indicated the inappropriate activity would cease.
17. In September and October of 2000, the MIS tracking system generated another report indicating inappropriate Internet communications by someone using Appellant's user name and password (Exhibit 5). The contacts in question were made for 11 minutes in the morning and 2 minutes in early afternoon of September 14, 8 minutes during the morning of September 28, 3 minutes in the morning and 8 minutes in the mid-afternoon of October 4, and 2 visits approximately 45 minutes apart on the morning of October 10. The actual time periods during which these contacts occurred were brief. However, according to the testimony of Mr. Wright, apparently the refresher function in the computer system repeatedly recorded each instance of refreshing the connection as another "hit" in the report (some of these hits were recorded to have occurred at the rate of ten per second). Therefore, the hearing officer finds that the report indicates an inordinately large number of "hits" given the actual activity indicated.
18. This report was again forwarded to Human Resources, which again reviewed the activity and verified that it was mostly sexually oriented and inappropriate. After consulting with management, the Agency elected this time to issue a Notice of Contemplation of Disciplinary Action to Appellant ("Contemplation letter") dated November 13, 2000 (Exhibit 3). This Contemplation letter set a predisciplinary meeting for November 21, 2000.
19. Appellant received the Contemplation letter on November 13, 2000. Appellant testified that this letter took him completely by surprise because he had ceased the activity in question as

he had told Mr. Currier he would on June 6, 2000 when they discussed his Verbal Reprimand.

20. In response to the Contemplation Letter, Appellant immediately consulted with Mr. Steffens about what might have happened. During this conversation, Mr. Steffens learned that Appellant's screen saver (which re-secures the computer each time it is turned on, requiring the user to re-enter his password) was set to trigger after thirty minutes. Mr. Steffens testified that his own screen saver is set for four minutes, and that he told Appellant thirty minutes is too long because it allows for unauthorized use for that length of time in the event that Appellant should leave his computer unattended and the office door open. Appellant set his screen saver to four minutes before the end of the day on November 13, 2000.
21. Appellant testified that the following morning on November 14, 2000, he also decided to change his password as an extra precautionary measure. The Agency has no evidence to establish that Appellant changed his password before November 14, 2000.
22. Appellant further discovered several indicators of Internet site contacts, known as "cookies," in his computer data. Appellant testified that he thought these indicators might be triggering unsolicited communications with the inappropriate Internet sites he had admittedly contacted earlier in the year, or similar Internet sites which were soliciting similar communications. Appellant testified he therefore deleted them from his system as well some time around November 13 or 14, in an attempt to terminate and additional solicitations.
23. The Agency's Senior Network Administrator, Michael Wright, testified that a "cookie" is an address indicating the user has initiated contact with the site indicated. He testified that a "cookie" can only be generated through the deliberate activity of a user and does not arise from solicitations coming from outside the office. Therefore, the "cookies" Appellant deleted had to represent communications initiated by someone in the office using Appellant's terminal for them to have turned up in his database.
24. On November 21, 2000, the predisciplinary meeting took place as scheduled. In attendance were Ed Currier who conducted the meeting, Deputy Manager of Aviation Turner West, Mike Steffens, and Human Resources Assistant Manager James Thomas. Appellant appeared and responded to the allegations. The Agency witnesses are unanimous in characterizing Appellant's response as adamantly denying he had initiated the contacts indicated in Exhibit 5. Appellant stated his knowledge of the Internet is limited and there had to be some kind of mistake, possibly arising from an error on his part, but he was not aware that the contacts had been occurring. Appellant raised the possibility of a break-in and use of Appellant's terminal by someone other than himself, perhaps one of the many individuals who have access to the corridor where Appellant's office is located. Appellant also stated he talked to Ed Johnson in MIS on how to make any necessary changes due to his limited knowledge, that he had removed the "cookies" from his database in the event they were the source of the problem, and that he had shortened his screen saver and changed his password as preventative measures.

25. Following the meeting, Mr. Thomas consulted with MIS officials. Mr. Wright reviewed the data and determined that this could not have been an accident as Appellant asserted might be a possibility. The reason Mr. Wright determined that this could not have been a mistake is because of the repeated contacts with several similar inappropriate sites in quick succession, establishing that the user was deliberately "surfing" from one to the next, and the length of time at the sites both individually and cumulatively, indicating that the user was not exiting as one would if he had contacted the site by mistake.
26. The reports generated by the MIS web-use tracking device do not reveal which password the user is using, but Mr. Wright testified that it is possible to trace whether any given user name has more than one password associated with it at one time. Mr. Wright testified that Appellant's user name only had one password at the time. The MIS reports also do not indicate from which terminal the user engaging in the web activities is communicating, only the user name being employed by that individual to gain access to the web. Mr. Wright further testified that while MIS has the capacity to trace the terminal being used, the determination of the user name and password (assuming there is only one in use as was the case here) is a more precise way of ascertaining who is responsible for a given instance of internet activity, than is identification of which terminal is being used to make the contacts. This is precisely because anyone can log in on any given terminal, but must have their own identifying information to do so. Mr. Wright testified that for this reason, MIS did not determine which terminal was used to generate the activity in question.
27. The Agency witnesses testified under cross-examination that they did not do an on-site inspection of Appellant's office as Appellant requested. Mr. Thomas testified that this was because the office security issue was irrelevant. Either Appellant had engaged in the contacts himself, or he had negligently allowed his password to be revealed to someone else, or he had allowed someone to gain unauthorized access directly to his computer. Since each employee is directly responsible for maintaining the security of his computer access, as specifically set forth in Policy 2005 of which Appellant acknowledges receipt in June, Appellant's culpability had been established one way or the other, and the offense was equally egregious either way.
28. After considering a three-day suspension, but then ascertaining that CSR Rule 16-20 3) only allows for suspensions of exempt employees in five-day increments, the Agency determined that a five-day suspension was appropriate discipline. In making this determination, the Agency considered Appellant's previous Verbal Reprimand, as well as his statements in mitigation during the predisciplinary meeting and its subsequent investigation (*see*, Exhibit 2).
29. On December 6, 2000, the Agency issued Appellant a Letter of Suspension (Exhibit 2) which is the letter giving rise to this appeal.
30. On December 18, 2000, Appellant filed his appeal with Career Service Authority (Exhibit 1).

## PRELIMINARY MATTERS

### 1. The Hearing Officer's Jurisdiction

The hearing officer finds she has jurisdiction to hear this case as a suspension case, pursuant to CSR Rule 19-10 b), as follows in relevant part:

#### Section 19-10 Actions Subject to Appeal

An applicant or employee who holds career service status may appeal the following administrative actions relating to personnel.

- ...b) Actions of appointing authority: Any action of an appointing authority resulting in... suspension... which results in alleged violation of the Career Service Charter Provisions, or Ordinances relating to the Career Service, or the Personnel Rules.

Jurisdiction over Appellant's suspension was not disputed by either party to this case.

### 2. Burden of proof

It has been previously established that the Agency responsible for suspending a career service employee bears the burden of establishing, by a preponderance of the evidence, that it had just cause for the suspension action. *See, In the Matter of the Appeal of Vernon Brunzetti*, Appeal No. 160-00 (Hearing Officer Bruce A. Plotkin, 12/8/00). The Agency must also demonstrate that the severity of discipline is reasonably related to the offense in question. *See, In the Matter of Leamon Taplan*, Appeal No. 35-99 (Hearing Officer Michael L. Bieda, 11/22/99). The burden of proof was not disputed by either party to this case.

## DISCUSSION

### 1. The Agency's Case in Support of Appellant's five-day suspension.

#### *a. Rules the Agency alleges Appellant violated.*

The Agency posits Appellant violated the following relevant portions of CSR Rule 16, DISCIPLINE:

#### Section 16-50 Discipline and Termination

##### A. Causes for Dismissal:

The following may be cause for dismissal of a career service employee. A lesser discipline other than dismissal may be imposed where circumstances warrant...

- 1) Gross negligence or willful neglect of duty...

- ...7) Refusing to comply with the orders of an authorized supervisor or refusing to do assigned work, which the employee is capable of performing...
- ...20) Conduct not specifically identified herein may be cause for dismissal.

### Section 16-51 Causes for Progressive Discipline

A. The following unacceptable behavior or performance may be cause for progressive discipline.... Failure to correct behavior or committing additional violations after progressive discipline has been taken may subject the employee to further discipline...

- ...5) Failure to observe departmental regulations...
- ...7) Unauthorized operation or use of any vehicles, machines or equipment of the City and County...
- ...10) Failure to comply with the instructions of an authorized supervisor...

The Agency further cites Policy 2005, governing Aviation employees' responsibilities regarding the use of company computer equipment, as follows in relevant part:

### II. Maintain Security for DIA Data

- ...B. Users will maintain security for DIA data in their possession or to which they have access...by not leaving their terminal or PC signed on when unauthorized people could access it, by changing their password on a regular basis, [and] by protecting files which contain a password.... Use of Windows 95 screen saver with a password is considered sufficient security when leaving a signed-on computer unattended.

### VI. Internet Access Policy

- ...B. The individual user is ultimately responsible for his/her actions when using Internet services.... The fact that a user can perform a particular function does not imply that they should, or are permitted to.
- C. Division Deputy Managers shall authorize Internet e-mail and Internet browsing access. Division Deputy Managers should be aware of the following when granting Internet access:
  - ...2. Individuals using DIA systems are subject to having all activities conducted on these systems monitored. Information derived from system monitoring may be used as a basis for administrative, disciplinary or criminal proceedings.

...E. Management and Administration

- ...3. The display of any kind of sexually explicit image or document on any company system is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.
- ...4. The City uses independently supplied software and data to identify inappropriate or sexually explicit Internet sites.... If you find yourself connected accidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately...

***b. The arguments.***

The Agency asserts that its conclusion, that Appellant was responsible for the inappropriate web contacts, is supported by a preponderance of the evidence. The Agency basically posits that given the facts in this case, there are only three possibilities, and that in each case Appellant is responsible for the breach. Either Appellant actively and deliberately engaged in these communications himself, or he was negligent in allowing his password to become known by another user who then gained access to the sites, or Appellant negligently allowed someone to access the internet through his computer when he left the office and his screen saver was set for thirty minutes.

The Agency first asserts that the evidence clearly implicates Appellant as a willing and deliberate initiator of the objectionable Internet communications. Appellant admits to having engaged in the first set of contacts which resulted in his Verbal Reprimand dated June 5, 2000, showing Appellant has a penchant for surfing inappropriate material on the web. In addition, the evidence establishes that the only way the list in Exhibit 5 could have been generated is through the combined use of Appellant's user name and his password, and that there is no evidence that Appellant has disclosed his password to another. Appellant himself denies having done this. Third, the patterns revealed in the list clearly indicate that it resulted from intentional, repetitive seeking by the responsible individual, not an isolated mistake or accident. Finally, the "cookies" Appellant admits to having deleted from his system could only have been generated by activity initiated at his terminal. Therefore, Appellant had to have deliberately pursued this activity, and it is not the product of an accident. The Agency points to the fact that Appellant's deletion of the "cookies" suggests that he was attempting to subvert the records in his machine indicating the requests originated there.

The Agency posits that there are only two other alternatives. The first arises from Appellant's negligent revelation of his password. Mr. Wright testified that the only two ways of ascertaining an employee's password are through the use of a decoder program available only to himself and another network administrator, or the negligent or deliberate disclosure by Appellant himself. Such disclosure can be either through the spoken word, the placement of the password in writing left in an unsecured place where it is observed by another, or through the observation by another with a keen eye while the employee is actually typing in his password.

The only remaining possibility is Appellant's failure to use his screen saver in a reasonable manner by leaving it set at thirty minutes, allowing anyone who might gain access to his office during that period of time to use Appellant's system without having to know the password.

Appellant responds adamantly, and has from the beginning of this action, that he did not intentionally generate these solicitations. He presents the following arguments in response to the Agency's case.

Appellant points to the fact that anyone at any terminal could have generated the list in Exhibit 5 by employing Appellant's user name and password, but that the Agency has never taken available steps to ascertain which terminal this activity was actually occurring from, despite their ability to do so. Second, Appellant argues that the Agency never did an on-site inspection of his office to observe the possible security problems he pointed out during the predisciplinary meeting, such as the possibility of someone coming over the wall through the ceiling outside his office, or the possibility of picking the lock on his lever-handled door, which handles Appellant asserts are easily picked.

Appellant argues that the Agency's failure to investigate these additional possibilities deprived him of the steps required by the Agency in the CSR Rules governing disciplinary actions. *See*, CSR Rule 16-30. Appellant asserts that the Agency's failure to investigate substantially impacted his rights under 16-54 D. in violation of the process he was due. He claims the Agency has failed to exhaust other alternative explanations for this occurrence, has assumed he is guilty, and consequently the burden of proving himself innocent has been placed upon him.

The Agency replies with two primary arguments. First, whether someone else's terminal was used is irrelevant, since this alternative still suggests Appellant was negligent in allowing someone else access to his password. Second, the Agency argues that even if his office was somehow compromised and his computer accessed before the screen saver turned itself on, thirty minutes is an unreasonably long period of time for the screen saver to be effective in guarding a terminal from unauthorized use. Therefore, even if Appellant did not, in fact, initiate the inappropriate contacts himself, the contacts were therefore still his ultimate responsibility as set forth in Policy 2005 II. B (cited in relevant part above; *see*, Exhibit 6). The Agency holds this failure as equally deserving of a five-day suspension.

Second, the Agency maintains that it did consider Appellant's mitigating responses during the predisciplinary meeting, and did investigate his suggestions with MIS, who concluded that they lacked merit, for the same reasons that either Appellant negligently permitted his password to be learned and used by another, or he negligently allowed his computer equipment to be accessed while he was away from his desk.

*c. The hearing officer's analysis and conclusions.*

The hearing officer would have felt much better informed if the Agency had in fact ascertained which terminal was used to make the contacts. However, the Agency's burden of

proof in this matter is a preponderance of the evidence. In lay terms, this simply means that the Agency must show it is more likely than not (a likelihood of greater than fifty percent) that Appellant did what it alleges he did. The Agency did not determine which terminal the contacts came from because it considered Appellant's user name and password to be a more precise way of determining who was responsible for the contacts, either through his own direct actions or through the negligent disclosure of his security information to another.

The hearing officer agrees that the Agency reasonably ruled out suggestions that the incidents were either a mistake, or were generated by existing residual contacts from Appellant's prior admitted web activity through the "cookies" in his database, as unsupported by the evidence. First, the pattern appearing in Exhibit 5 clearly exhibits intentional, continuing "surfing" activity spanning several minutes and including numerous changes among similar sites. Second, credible Agency testimony by a witness highly trained in computer science established that "cookies," which are generated by activities initiated at the terminal where they are located, do not spontaneously generate undetected solicitations from outside Internet sources.<sup>1</sup> This evidence clearly supports the Agency's conclusion that the activity represented in Exhibit 5 was intentional and not the product of unsolicited external communications.

Similarly, the hearing officer concludes that the Agency did not substantially prejudice Appellant's due process rights when it failed to investigate the security problems concerning accessibility to his office. Both Appellant and Mr. Adams testified that they come and go unpredictably from the office. The record is clear that most of the Internet contacts occurred at various times during the middle of the workday, in an office on a well-traveled corridor. It cannot reasonably be presumed possible that some individual either picked the lock, crawled over the wall through the ceiling, or simply walked through the usually locked door, when none of the office occupants who have unpredictable schedules happened to be there, then made the contacts, then escaped, all without being detected, *not once, but on at least six separate occasions*, some occurring only hours apart in the course of a single day. Furthermore, this accomplished individual also either had to have access to Appellant's password, or he had to make his secreted entry within thirty minutes of Appellant's departure. The application of common sense eliminates this entire scenario as a reasonable possibility.

In addition, the hearing officer agrees that any reasonable person should have known thirty minutes is too long for the screen saver function to serve its purpose. Appellant's own argument that this time period might have allowed for unauthorized access by another demonstrates the Agency's point. The minute Appellant stepped away from his office and left his terminal unattended without the screen saver activated, he was in violation of the clear intent

---

<sup>1</sup> The hearing officer is not persuaded that Appellant's deletion of the "cookies" from his temporary files was a deliberate attempt to obfuscate the Agency's investigation of who was responsible for these contacts. If this were the case, he would not have set this action forth at the predisciplinary meeting as a mitigative step he had taken to correct the problem. The hearing officer is further unpersuaded that Appellant's deletion of the cookies evidences his knowledge of the Internet was greater than he professed at the meeting. On the contrary, that he offered this as a mitigating action only demonstrates that he did not understand the significance of what he was doing. Appellant's demeanor and line of questioning at the hearing clearly indicate he did not understand what these devices were until the hearing. In addition, while Appellant may still qualify as a "novice" in the field, he is obviously highly intelligent and could have stumbled on these addresses while poking around in his system trying to ascertain where the problem was coming from.

of Policy 2005 II. B (cited above). Appellant acknowledges had already received the Policy well before the breaches in question occurred. He was therefore responsible for abiding by its mandates, or his failure to do so.

For all the reasons set forth above, the hearing officer concludes that the Agency's failure to determine which terminal was used, and to do an on-site security inspection in the course of its investigation, did not substantially prejudice Appellant's due process rights.

The hearing officer is troubled by the fact that she found Appellant's consistent, adamant assertions of his innocence, from the first moment he learned of the allegations, as well as his demeanor during the hearing, to be very credible. However, the hearing officer is charged with the responsibility of weighing all the evidence, assigning weight to that evidence based on her best and most reasonable judgment, and rendering a decision in light of the totality of that evidence. The hearing officer is procedurally bound to apply the preponderance standard in that process.

Whoever did this had to have Appellant's password. There appears to have been virtually no probability that Appellant revealed his password to anyone, and he himself denies doing so. Only the two aforementioned MIS officials had the capacity to crack his password, and only through the use of a complex deciphering device. Mr. Wright testified under oath that he has not used this deciphering system to crack Appellant's password, and to his knowledge, his partner has not, and would not have any reason to, do the same.

In light of the above analysis, none of the alternatives offered by Appellant make any sense under close scrutiny and in the face of concrete evidence. Therefore, while Appellant appears very credible in his denials, in light of the totality of evidence in this case, the hearing officer must conclude it is more likely than not that Appellant in fact had a deliberate hand in the generation of the Internet contacts in question.

***d. Severity of the discipline.***

The Agency posits that its suspension of Appellant was proper under the relevant portions of the following CSR Rule:

**Section 16-20 Progressive Discipline**

- 1) In order of increasing severity, the disciplinary actions which an appointing authority or designee may take against an employee for violation of career service rules, the Charter of the City and County of Denver, or the Revised Municipal Code of the City and County of Denver include:
  - a) Verbal reprimand, which must be accompanied by a notation in the supervisor's file and the agency's file in the employee;
  - b) Written reprimand, a copy of which shall be placed in the employee's personnel file kept at Career Service Authority;

- c) Suspension without pay, a copy of the written notice shall be placed in the employee's personnel file kept at Career Service Authority...

The hearing officer is not persuaded that a suspension would be warranted in this case were the Agency's only showing that Appellant negligently allowed his password or equipment to be accessed. In this case, suspension is being exercised as progressive discipline, which presumes that this act is connected with that which warranted the initial Verbal Reprimand. There has been no suggestion that Appellant's failure to safeguard the security of his computer was an issue in the Verbal Reprimand. If Appellant's only offense in this case were the disclosure of his password or failure to secure his terminal, this offense would therefore not be directly connected with his unacceptable activities on the Internet giving rise to the Verbal Reprimand.

However, given the hearing officer's conclusion set forth above, she does not need to ascertain the appropriate level of discipline assuming Appellant's negligent disclosure of his password or access to his computer were the only offense. Because given the totality of the evidence, the hearing officer concludes the Agency has shown it is more likely than not that Appellant engaged in the inappropriate activity in question, this disciplinary action is therefore connected with the activity giving rise to the Verbal Reprimand. Appellant was warned that there may be more severe penalties down the road for additional such infractions. Mr. Thomas testified that given the similarities between a Verbal Reprimand and a Written Reprimand, and in light of the apparent ineffectiveness of the Verbal Reprimand, they decided to proceed to the next level of discipline, which is suspension. Finally, as an exempt employee, Appellant must be suspended in no less than five-day increments pursuant to CSR Rule 16-20 3).

The hearing officer finds the Agency's analysis set forth above to be reasonable. Under all these circumstances, she concludes that the five-day suspension was reasonably related to the offense in question.

### CONCLUSIONS OF LAW

1. The Agency has demonstrated by a preponderance of evidence that Appellant used Agency computer equipment for inappropriate purposes on the dates giving rise to the disciplinary act in question.
2. In light of this showing, the Agency has demonstrated that Appellant engaged in:
  - a) Failure to observe departmental regulations, specifically Aviation Department Standard Policy and Procedure No. 2005, in violation of CSR Rule 16-51 A. 5).
  - b) Unauthorized use of Agency equipment in violation of CSR Rule 16-51 A. 7).
  - c) Failure to comply with the instructions of an authorized supervisor in violation of 16-51 A. 10).

- d) Conduct not specified in CSR Rule 16-50 and 16-51, which may otherwise be cause for discipline.
3. The Agency has failed to demonstrate that Appellant engaged in:
    - a) Gross negligence in violation of CSR Rule 16-50 A. 1). No damage to the Agency, to Appellant's work product, or otherwise has been shown to warrant such a severe characterization of Appellant's indiscretions in this case.
    - b) Sexual harassment in violation of Aviation Department Standard Policy and Procedure No. 100-15.1 and CSR Rule 16-51 A. 5). The Agency has not shown involvement by anyone other than Appellant himself. The hearing officer knows of no precedent wherein sexual harassment has been found where only one person is involved in the inappropriate activity, and where there is therefore no victim, as is the case here.
    - c) Refusing to comply with the orders of an authorized supervisor in violation of CSR Rule 16-50 A. 7). 16-51 A. 10) is a "lesser-included offense" of this charge and is more appropriately applicable to Appellant's non work- related indiscretion in this case.
  4. The Agency has demonstrated just cause for disciplining Appellant by a preponderance of the evidence.
  5. In light of the totality of evidence in this case, the Agency's five-day suspension of Appellant is reasonably related to the seriousness of the offense.

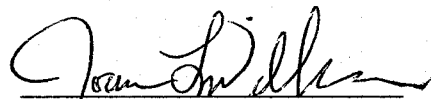
### **DECISION AND ORDER**

Based on the Findings and Conclusions set forth above, the Director's decision to suspend Appellant for five days is AFFIRMED.

The Agency is ORDERED to MODIFY the Letter of Suspension in Appellant's files to delete the alleged violations, set forth above in Paragraph 3 of the hearing officer's Conclusions of Law, as unsubstantiated. The existing Letter of Suspension shall be removed from Appellant's files and replaced with the modified version.

This case is hereby DISMISSED

Dated this 4 th day of May, 2001.



Joanna L. Wilkerson  
Hearing Officer for the  
Career Service Board

**CERTIFICATE OF MAILING**

I hereby certify that I have forwarded a true and correct copy of the foregoing **FINDINGS AND ORDER** by depositing same in the U.S. mail, postage prepaid, this 7<sup>th</sup> day of May, 2001, addressed to:

Steve Smith  
17123 E. Kent Dr.  
Aurora, CO 80013

I further certify that I have forwarded a true and correct copy of the foregoing **FINDINGS AND ORDER** depositing same in interoffice mail, this 7<sup>th</sup> day of May, 2001, addressed to:

Robert D. Nespor  
Assistant City Attorney

James Thomas  
Department of Aviation  
Denver International Airport

V. Granada