Biscayne Building
19 West Flagler St., Suite 220
Miami, FL 33130
Phone (305) 375-1946
Fax (305) 579-2656
www.miamidadeig.org

Office of the Inspector General
Miami-Dade County

FINAL REPORT

To: George M. Burgess, County Manager

Received by Date

From: Christopher R. Mazzella, Inspector General

Date: April 27, 2004

Re: Violations of County Internet Service and E-mail Policies among MDAD Employees.

This report was issued in draft form on April 1, 2004. Copies were provided to Miami-Dade Aviation Department (MDAD) Director, Angela Gittens, and the Miami-Dade County Chief Information Officer, Judy Zito. Personalized draft reports were also issued to each of the 28 identified MDAD and former MDAD employees (see Appendix B-2). Of those 28 employees, ten (10) elected to respond in writing to the OIG and their responses are collectively included in Appendix C-2. Individualized final reports are not being issued to each employee, in as much as there are no changes from the draft to the final. This is the only final report being issued with respect to the instant matter.

The Aviation Department in its response, Appendix C-1, states that it has implemented corrective action in the form of "a compliance education program to familiarize employees with County Administrative Orders and Aviation Department Written Directives." It also notes that "appropriate disciplinary action" has been or will be taken against individuals identified "as having violated County and Departmental computer use policies."

In light of these on-going efforts, the OIG requests to be provided with a status report by July 30, 2004, which should detail the progress of the compliance education program, including copies of the training materials. The status report should also provide an update on the disciplinary actions undertaken by the department.

cc: Honorable Chairperson Barbara Carey-Shuler, Ed.D.
Honorable Katy Sorenson, Vice Chairperson
Honorable Dennis C. Moss, Chairperson, Transportation Committee
Bill Johnson, Assistant County Manager
Judy Zito, Chief Information Officer
Angela Gittens, Director, Miami-Dade Aviation Department
Antonio Bared, Chief, Miami-Dade Fire Rescue
Clerk of the Board (copy filed)

Received by Date

SYNOPSIS

In September 2003, the Office of the Inspector General (OIG) received information that a Miami-Dade Aviation Department (MDAD) supervisor was utilizing Miami-Dade County's (the County) Internet web access to download pornographic material and then send the sexually explicit materials to other County employees using the County's Microsoft Outlook Electronic Mail (e-mail) system (Outlook system). Based on these initial allegations, the OIG's review necessitated tracking the prohibited e-mails to other MDAD employee accounts. The OIG's review, reported herein, identifies 28 MDAD employees, who have transmitted pornographic or otherwise sexually explicit materials through the use of their county-assigned e-mail accounts. This review was limited to the last two years.

Initially, a review of MDAD e-mail files for the identified employee confirmed that the employee transmitted at least twelve (12) e-mails containing materials prohibited under Miami-Dade County Administrative Order (A.O.) 6-7 and the MDAD Standards Manual. The e-mails contained attachments of nude photographs and other sexually oriented materials, and were forwarded by this employee to other County employees, the majority of whom are MDAD employees, and to outside e-mail accounts. The e-mails subsequently forwarded were received by this employee from both County and non-County sources. The Outlook system does not screen the attachments of incoming e-mails, thus allowing prohibited materials to enter the County network.

The distribution of prohibited materials through e-mails has been prevalent within the MDAD Outlook system, with incidents occurring back to at least 2001, and continuing on a routine basis. In this investigation, the OIG determined that 28 MDAD employees, including supervisory personnel, have transmitted one or more prohibited e-mails using their County assigned Outlook accounts.

BACKGROUND

MDAD's Information Systems Division (ISD) maintains all computer-related operations, including the Outlook e-mail system, for the department and its employees. The MDAD computer network functions independently from other County departments, although the e-mail system interfaces with the County's main network. It also interfaces with external service providers. MDAD's computer system, like the countywide system, allows employees to send and receive e-mail messages internally and externally and access the Internet.

ISD estimates there are over 1,100 computers assigned within the MDAD network, which includes Miami International Airport (MIA), the Department's general aviation airports, and off-terminal office buildings and other facilities. ISD is responsible for the maintenance of all computer hardware, software applications and Internet-related services, including e-mail accounts, within the MDAD network. Individual e-mail accounts are assigned to employees, and are accessible by password upon logging onto the network. The Outlook system allows employees to send and receive e-mails and save items, as chosen. Attachments may also be

opened and saved separately. The system also automatically saves e-mails within the employee's account, if not deleted completely. Furthermore, employees may create personal sub-folders to save items.

All employee e-mails are ultimately stored in the Outlook data server physically located at MIA. The files are stored according to each individual employee's MDAD-assigned account. The backed-up data is available to ISD personnel by administrative password for monitoring purposes.

With very few exceptions, most MDAD employees have restricted access to the Internet. On or around June 8, 2003, the Miami-Dade County Information Technology Department (ITD) installed the Web Sense program on the MDAD network's Internet browser. This program restricts users from connecting to adult (i.e., pornographic) and other Internet sites deemed to be inappropriate and/or prohibited according to County policies and procedures. However, the Web Sense program does not affect the Outlook system, and there is no method to filter incoming or outgoing e-mails and their attachments. Consequently, employees can easily receive and send e-mails, both internally and externally, containing prohibited materials.

GOVERNING AUTHORITIES

Miami-Dade County Administrative Order 6-7, *Access To and Use of Internet Services and Electronic Mail (E-Mail)*, effective December 12, 1999, (A.O. 6-7) establishes the baseline standard for all Miami-Dade County employees. Furthermore, MDAD has its own standards manual for its employees, which sets additional standards regarding the use of computers and telecommunications systems.

A.O. 6-7 states in part:

> This Administrative Order governs the appropriate use of these tools [Internet Services and E-mail] to ensure that their use is in the best interest of the County. Improper use of these tools can raise many issues, including: Violation of the public records laws; Invasion of privacy; Subjecting the County to criminal or civil charges; Loss of productivity; Jeopardizing security of County information systems. This Administrative Order delineates those activities that are prohibited, and it is the responsibility of each County employee who is granted access to these tools to follow this Administrative Order when using the Internet and e-mail.

The *Public Records* section of A.O. 6-7 reads in part:

> As such, Miami-Dade County reserves the right to review employees' files, documents, e-mails, or use any data created or stored by a user, as it deems appropriate. The County reserves the right to monitor and review the usage of

all electronic equipment. The County's Internet services and e-mails are currently being monitored and this information is considered public record.

A.O. 6-7 further establishes *Prohibited Activities* regarding e-mails and Internet Services that include, but are not limited to:

> 1. Activity, which could subject the County to civil or criminal liability, but are not limited to: Discrimination, such as use of e-mail or the Internet to illegally discriminate against a person or group of persons based on race, nationality, ethic origin, religion, sex, or other protected class. . .
>
> 3. Usage intended for personal or commercial financial gain (e.g. advertising).
>
> 8. Utilization of e-mail or the Internet to distribute offensive, abusive, threatening, pornographic, sexually explicit or hate messages or images.
>
> 9. Sending e-mail messages, images or sounds to others that are offensive to a reasonable person because the message contains lewd language or comments of an inappropriate personal nature, are intended to harass or annoy, or are otherwise offensive.

Similarly, MDAD has its own *Information Systems Division Computer Use Policies and Procedures (ISD Policies and Procedures)*, which were last known to be circulated department-wide in June 1999. Many of the same standards are reiterated in MDAD's *Standards Manual.*

Governing personal computers, the MDAD *ISD Polices and Procedures*, Section II (C) states:

> The use of personal computers, their hardware, software, and peripherals for the creation, storing, displaying, posting, distribution of obscene or slanderous material is strictly prohibited.

The same holds true for network access, *ISD Polices and Procedures*, Section IV (C):

> The use of the network, or network resources for the creation, storing, displaying, posting, distribution of obscene or slanderous material is strictly prohibited.

Regarding e-mail, the *ISD Policies and Procedures*, Section VII, in line with County A.O. 6-7, prohibits:

- Distribution of pornographic or hate material.
- Sending or publishing material containing offensive, abusive, threatening or other inappropriate language.
- Sending or publishing sexually oriented messages or images.

In July of 1999, all MDAD employees were provided a copy of the *ISD Policies and Procedures* and were required to sign an *End User Sign-Off Agreement Acknowledgment Form*, stating they have read, understood, and accepted the terms and conditions as specified in MDAD's *ISD Policies and Procedures*. The signed forms were placed in each employee's personnel file and a copy of the *ISD Policies and Procedures* and form were to be included in each new hire packet.

FINDINGS

A. Initial Complaint

Based on an initial complaint received in September 2003, the OIG reviewed the e-mail files of the identified MDAD employee. The OIG found twelve (12) e-mails stored in the employee's *Sent Items* folder as saved on the MDAD ISD Outlook data server, which contained photographs of nude females and other sexually explicit materials. The tracking documentation contained in these twelve (12) e-mails reflect that ten (10) were sent to the employee's Outlook account from outside web accounts and two (2) were received internally from other MDAD employee e-mail accounts. Further tracking of the two (2) internally received e-mails, back to its original source, could not be determined.

These twelve (12) e-mail files were reproduced/reprinted by the OIG. We also tracked the forwarding of these e-mail images from the named employee's e-mail account to other employee accounts within the County. Our review disclosed that four (4) images were transmitted to a total of six (6) other MDAD employees. One sexually explicit e-mail was sent to a family member employed at the Miami-Dade County Corrections Department. Ten (10) e-mails were sent to 17 web accounts outside the County.

The OIG's review of this employee's computer temporary Internet files for the period of May 12, 2003 to September 26, 2003, indicates no apparent misuse of the Internet relating to accessing otherwise restricted pornographic and/or sexually explicit websites. Further, since the installation of the Web Sense program on June 8, 2003, the Internet access was restricted.

B. Additional Identified Employees

In reviewing the named employee's e-mail files, several other airport employees engaged in the sending or receiving of prohibited e-mails were identified. A review of those employees' files revealed that numerous MDAD employees, both male and female, exchanged prohibited materials on a fairly routine basis. The OIG reviewed hundreds of e-mails and their attachments which contained prohibited material of varying degrees of content. The materials ranged from photographs of homosexual acts, male and female nudity, masochistic pictures and drawings, and numerous other sexually-oriented and/or offensive items, such as jokes,

cartoons, and video clips. There were hundreds of other e-mails that, although not sexually-oriented, were clearly unrelated to County business.

Most airport employees have restricted Internet access, and therefore are unable to access adult websites and other sites not deemed appropriate by MDAD. Most of the employees identified in this case have the block on their Internet access.[1] This restriction does not affect the e-mail system, and employees can still receive and send e-mails with attachments.

The OIG selected 61 e-mails as the basis of its reported review. The e-mails were traced beginning from the named employee and tracked outward as they were sent to other MDAD employees. In all, 61 e-mails were selected because of their pornographic, sexually explicit, lewd, offensive, or otherwise inappropriate content. A total of 28 MDAD employees, including supervisors, have been identified as having used the County's e-mail system **to send** these identified prohibited materials. Sixty-six percent (66%) of the selected e-mails originated from sources outside the County's system, and were then sent electronically to the Outlook accounts of the MDAD employees. Once received, the e-mails were then sent/forwarded to other employees. E-mails received by MDAD employees were also sent to other County employees outside the MDAD system, and to external private Internet accounts.

Through the course of this review, the OIG also examined hundreds of other types of e-mails prohibited under A.O. 6-7, including chain letters, greeting cards, prayers, business opportunities, pictures of the Iraqi war and text jokes that were not sexual in nature but clearly not related to County business. These e-mails were transmitted to hundreds of employees. As previously mentioned, the OIG selected 61 e-mails for this report because of their pornographic, sexually explicit, lewd, offensive, or otherwise inappropriate content.

As previously mentioned, the OIG's inquiry expanded to include 28 MDAD employees who had used their e-mail account, on at least one occasion, to send one of the aforementioned 61 depictions. Employees who were traced as having received only (and not forwarded) one of the 61 prohibited e-mails were excluded from this review. Overall, the 61 selected e-mails (and images) were forwarded to over 350 airport employees e-mail accounts and in excess of 140 outside accounts.

The OIG's investigation revealed that many of the e-mails circulated quickly throughout the MDAD network being passed along to multiple employees. Examples include: one e-mail containing 12 photographs of partially nude females forwarded by one employee simultaneously to 21 other employees; an e-mail attachment of a calendar containing 12 photographs of obese females wearing swim suits was forwarded by three different employees to 54 other employees; and a third example of a 90 second video clip (e-mail attachment) that was forwarded by five MDAD employees to a total of 39 MDAD and 13 external e-mail

[1] Research of four employees' Internet Temporary Files indicates that one employee has made several attempts to gain access to adult sites on the County Internet access, and was blocked by the Web Sense program.

accounts. Patterns of e-mails received by several MDAD employees suggest that they are seemingly part of a group that exchanges these types of e-mails routinely.

Among the prohibited e-mails, 16 video clips were discovered, most with audio and ranging in length from 11 seconds to over 2 minutes. Many of the video clips were sexually oriented, including foreign commercials, and other miscellaneous topics of minimal value to the viewer—none pertaining to County business. The videos were forwarded to numerous personnel, although the exact number could not be calculated. The videos were stored in multiple employees' Outlook *Inbox* or *Sent Items* folders. This allows the employee to view the e-mail at anytime, or forward it on to other employees or outside parties. It was common for employees to forward the same stored video clip on more than one occasion.

The use of the Outlook system to forward the prohibited e-mails was prevalent in the MDAD Outlook system. It is so common that at least two employees created sub-folders within their personal Outlook accounts in order to store their favorite e-mails. One employee referred to the folder as *Great E-Mails*, which contained 76 items, and another employee had a *Jokes* folder with 153 saved items.

C. End User Sign-Off Agreements

The OIG was told that in 1999 the end user agreements were distributed in mass to all MDAD departments with instructions to have the MDAD employee review and sign the forms, which would then be forwarded to their MDAD personnel files. The OIG was also advised that the form was also forwarded to MDAD's Administrative Services Division for inclusion in the MDAD new hire packets. New hires after the initial distribution in 1999 should have completed the form as part of their initial employment at MDAD.

For the 28 employees reviewed, the OIG only found five (5) agreements in the MDAD personnel files. The five (5) agreements were all signed by individuals employed at MDAD at the time of initial mass distribution. All five (5) of these forms bear dates indicating that they were signed in July of 1999. The OIG subsequently learned from the MDAD Administrative Services Division that the form was not being included in the new hire packets, although we were also told by the Information Systems Division that they should have been included.

CONCLUSION

Numerous MDAD employees have utilized the Outlook system to disseminate prohibited materials since 2001. The prohibited materials selected by the OIG, 61 in total, contained photographs of nudity, and other sexually oriented images including homosexual acts, video clips of various sexually oriented themes, cartoons and drawings, and sexual related jokes.

The 61 e-mails documented by the OIG were traced to MDAD employees Outlook accounts. Twenty-eight (28) employees were identified as having sent/forwarded one or more e-mails containing prohibited materials to other employees or e-mail accounts outside the County. These transmissions are in violation of A.O. 6-7 *Access To and Use of Internet Services and Electronic Mail (E-Mail)* and MDAD's *Information Systems Division Computer Use Policies and Procedures (ISD Policies and Procedures).*

As illustrated by the attached Matrix, three employees forwarded the majority of the e-mails containing nudity and strong sexually oriented images, with the other 25 employees forwarding at least one prohibited e-mail. Employees of both genders, including supervisors, were sending the inappropriate e-mails to male and female employees throughout the County network.

The OIG investigation determined the majority of the prohibited e-mails entered the MDAD Outlook system from outside the MDAD network as attachments to messages sent to employees. The OIG also realizes that County employees from other departments also forward prohibited materials from their county computers to MDAD employees. The Outlook system does not have the capability to review or filter the materials contained within attachments, thus allowing prohibited material to enter the County Outlook system undetected. The receiving employee can then easily forward the materials to other employees countywide, or to non-county e-mail addresses. Further, employees have unlimited space within the Outlook server to save messages for months or years for viewing and re-forwarding.

RECOMMENDATIONS

The OIG makes the following recommendations to MDAD officials[2] based on the abuses documented in this investigation:

1. MDAD officials should ensure that all supervisors and managers understand their supervisory responsibilities regarding employees that misuse county computers.

---

[2] While the scope of this review focused on abuses specifically within MDAD, **the OIG observed that some of these same e-mails were forwarded to MDAD employees from other County accounts outside the MDAD network**. MDAD employees also forwarded some of these e-mails to County employees in various departments. The OIG did not expand this review to follow the chain of e-mail outside the MDAD network, even though there is sufficient reason to believe that these abuses are occurring countywide and are not isolated to MDAD. And while the findings and recommendation listed herein are specifically directed to MDAD, **it is the OIG's hope that the County's Chief Information Officer implement similar corrective measures countywide. Furthermore, it is the OIG's intention to expand this scope of review outside the MDAD network, and issue additional reports to County employees, as identified.**

2. All MDAD supervisors and managers must be made aware and understand the liability in which the County is exposed due to their inaction whenever they observe misuse of computers, or themselves participate in those abuses.

3. MDAD should conduct training for airport employees with computer access stressing the proper use of computer equipment, specifically relating to the use of the Internet and Outlook systems. This training should conclude with the employee affirmatively indicating (through an *End User Sign-Off Agreement*) that they fully understand A.O. *Access To and Use of Internet Services and Electronic Mail (E-MAIL)* and will agree to abide by all MDAD specific requirements, including the *Standards Manual* and *ISD Policies and Procedures*.

4. MDAD Administrative Services Division should explain why only five (5) *End User Agreements* were found in the personnel files of the 28 employees reviewed.

5. MDAD should take strong and appropriate disciplinary action on all employees deemed to be in violation of the aforementioned policy and procedures governing Internet and E-mail usage for the distribution of prohibited materials.

MDAD, in its response to the OIG draft report, see Appendix C-1, indicates that it is taking action in the form of educational compliance training and is taking appropriate disciplinary action. And while a very brief response, it appears to address four of the five recommendations, albeit without sufficient detail. As mentioned in the outset of this report, ***the OIG requests to be provided with a status report by July 30, 2004.*** *This status report should detail the components of the compliance training program and should include copies of training materials.*

Incorporated as ***"Attachment A"*** *to this report is a Matrix listing the 28 MDAD employees identified in the course of this review as having sent a prohibited e-mail for the time period reviewed. Listed across the top of this Matrix are the 61 aforementioned e-mails. For each individual listed, the Matrix shows the total number of e-mails sent/forwarded with checkmarks indicating which of the 61 e-mails each individual is attributed to having sent/forwarded.*

For those 28 employees identified in the course of this review, each received an individualized draft report describing each person's findings. The OIG received ten (10) responses and they are contained in Appendix C-2. The Matrix also includes a new column indicating which individuals submitted a written response to the OIG's draft report.

The OIG has not attached the 61 prohibited e-mail images and attachment materials due to their graphic and offensive nature; however, they are available on a compact disk, referenced as ***"Attachment B"*** *to this report. Paper copies of individual exhibits are also available.*

ATTACHMENT A – MATRIX

ATTACHMENT B – CD with Exhibits 1-61 (contains graphic material)

APPENDIX A

OIG NOTIFICATION LETTERS TO RECIPIENTS OF THE OIG DRAFT REPORT

A-1. Notice to Angela Gittens, Director, Miami-Dade Aviation Department

A-2. Notice to Judy Zito, Chief Information Officer, Miami-Dade County

A-3. Composite: 28 notices to all identified MDAD and former MDAD employees receiving a copy of a personalized draft report.

APPENDIX B

PERSONALIZED DRAFT REPORTS (NO INDIVIDUAL FINAL REPORTS BEING ISSUED.)

B-1. Copy of the OIG's draft report (boilerplate) received by each of the 28 individuals.

B-2. Composite: copies of personalized draft reports received by each of the 28 individuals.

APPENDIX C

RESPONSES RECEIVED TO DRAFT REPORTS

C-1. Response received from Angela Gittens, Director, Miami-Dade Aviation Department.

C-2. Composite: Ten (10) responses received from individuals who were provided a copy of their personalized draft report. (See OIG Attachment A, Matrix, for individualized details.)