

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General



May 29, 2009

The Honorable Adrian M. Fenty
Mayor
District of Columbia
Mayor's Correspondence Unit, Suite 316
1350 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

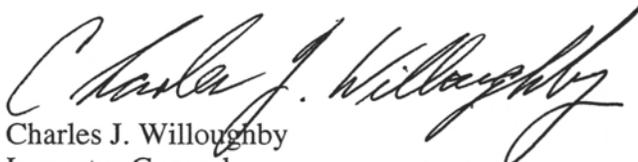
Dear Mayor Fenty:

Enclosed please find a copy of a Management Alert Report (MAR 09-I-006) issued May 8, 2009, to the D.C. Department of Human Resources (DCHR), Benefits and Retirement Administration (BRA). The MAR addresses our finding that BRA is not properly safeguarding sensitive information (e.g. Social Security numbers and bank/investment account numbers) submitted by and/or pertaining to D.C. government employees and retirees. DCHR's response to the MAR, dated May 22, 2009, is also enclosed.

Although the OIG is conducting an ongoing inspection of BRA for which a report will be completed later this year, we are providing this information to you now so that you are aware of the importance of the issues addressed in the MAR and the corrective actions proposed by DCHR.

If you have questions, please contact Alvin Wright, Jr., Assistant Inspector General for Inspections and Evaluations, at (202) 727-2540.

Sincerely,


Charles J. Willoughby
Inspector General

CJW/mdj

Enclosures

cc: See distribution list

DISTRIBUTION:

Mr. Neil O. Albert, City Administrator, District of Columbia (1 copy)
The Honorable Vincent C. Gray, Chairman, Council of the District of Columbia (1 copy)
The Honorable Mary M. Cheh, Chairperson, Committee on Government Operations and the Environment, Council of the District of Columbia (1 copy)
Ms. Brender L. Gregory, Director, D.C. Department of Human Resources (1 copy)
Ms. Karla Kirby-Sumpter, Associate Director, D.C. Department of Human Resources, Benefits and Retirement Administration (1 copy)
Mr. Andrew T. Richardson, III, General Counsel to the Mayor (1 copy)
Ms. Carrie Kohns, Chief of Staff, Office of the Mayor (1 copy)
Ms. Bridget Davis, Director, Office of Policy and Legislative Affairs (1 copy)
Ms. Mafara Hobson, Director, Office of Communications (1 copy)
Mr. William Singer, Chief of Budget Execution, Office of the City Administrator (1 copy)
Ms. Cynthia Brock-Smith, Secretary to the Council (13 copies)
Mr. Peter Nickles, Attorney General for the District of Columbia (1 copy)
Dr. Natwar M. Gandhi, Chief Financial Officer (4 copies)
Mr. Robert Andary, Executive Director, Office of Integrity and Oversight, Office of the Chief Financial Officer (1 copy)
Ms. Deborah K. Nichols, D.C. Auditor (1 copy)
Ms. Kelly Valentine, Director and Chief Risk Officer, Office of Risk Management (1 copy)
Ms. Jeanette M. Franzel, Managing Director, FMA, GAO, Attention: Sandra Silzer (1 copy)
The Honorable Eleanor Holmes Norton, D.C. Delegate, House of Representatives, Attention: Bradley Truding (1 copy)
The Honorable Edolphus Towns, Chairman, House Committee on Oversight and Government Reform, Attention: Ron Stroman (1 copy)
The Honorable Darrell Issa, Ranking Member, House Committee on Oversight and Government Reform (1 copy)
The Honorable Stephen F. Lynch, Chairman, House Subcommittee on the Federal Workforce, Postal Service, and the District of Columbia, Attention: William Miles (1 copy)
The Honorable Jason Chaffetz, Ranking Member, House Subcommittee on the Federal Workforce, Postal Service, and the District of Columbia (1 copy)
The Honorable Joseph Lieberman, Chairman, Senate Committee on Homeland Security and Governmental Affairs, Attention: Holly Idelson (1 copy)
The Honorable Susan Collins, Ranking Member, Senate Committee on Homeland Security and Governmental Affairs (1 copy)
The Honorable Daniel K. Akaka, Chairman, Senate Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia (1 copy)
The Honorable George Voinovich, Acting Ranking Member, Senate Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia (1 copy)
The Honorable David Obey, Chairman, House Committee on Appropriations, Attention: Beverly Pheto (1 copy)
The Honorable Jerry Lewis, Ranking Member, House Committee on Appropriations (1 copy)

The Honorable José E. Serrano, Chairman, House Subcommittee on Financial Services and
General Government, Attention: Dale Oak (1 copy)
The Honorable Jo Ann Emerson, Ranking Member, House Subcommittee on Financial Services
and General Government (1 copy)
The Honorable Daniel K. Inouye, Chairman, Senate Committee on Appropriations,
Attention: Charles Houy (1 copy)
The Honorable Thad Cochran, Ranking Member, Senate Committee on Appropriations (1 copy)
The Honorable Richard Durbin, Chairman, Senate Subcommittee on Financial Services and
General Government (1 copy)
The Honorable Sam Brownback, Ranking Member, Senate Subcommittee on Financial Services
and General Government (1 copy)



DISTRICT OF COLUMBIA
OFFICE OF THE INSPECTOR GENERAL

CHARLES J. WILLOUGHBY
INSPECTOR GENERAL

INSPECTIONS AND EVALUATIONS DIVISION
MANAGEMENT ALERT REPORT

D.C. DEPARTMENT OF
HUMAN RESOURCES:
BENEFITS AND RETIREMENT ADMINISTRATION

DOCUMENTS CONTAINING DISTRICT EMPLOYEES’
AND RETIREES’ PERSONAL DATA NOT
SAFEGUARDED

MAR 09-I-006

MAY 8, 2009

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General



May 8, 2009

Brender L. Gregory
Director
D.C. Department of Human Resources
441 4th Street, N.W.
Suite 330 South
Washington, D.C. 20001

Karla Kirby-Sumpter
Associate Director
Benefits and Retirement Administration
D.C. Department of Human Resources
441 4th Street, N.W.
Suite 340 North
Washington, D.C. 20001

Dear Ms. Gregory and Ms. Kirby-Sumpter:

This is a Management Alert Report (MAR 09-I-006) to inform you that during our inspection of the D.C. Department of Human Resources (DCHR) Benefits and Retirement Administration (BRA), the Office of the Inspector General (OIG) determined that BRA is not properly safeguarding sensitive information submitted by and/or pertaining to D.C. government employees and retirees. The OIG provides these reports when it believes a matter requires the immediate attention of District government officials.

Background

BRA is responsible for administering policies and benefits programs (e.g., health care, disability insurance, life insurance, and deferred compensation) that cover approximately 32,000 eligible District employees and retirees. In this capacity, BRA oversees plan management, responds to employees' and retirees' requests for assistance, monitors service contractors, and coordinates the communication of information to program participants and prospective participants.¹ BRA employs 14 human resources specialists and 4 human resources assistants.

¹ See <http://www.dchr.dc.gov/dcop/cwp/view,a,3,q,528755,dcopNav,%7C31663%7C,dcopNav,%7C31798%7C.asp> (last visited March 24, 2009).

Observations

Many documents containing sensitive, personal information are not properly secured and are therefore vulnerable to theft and misuse.

The District Personnel Manual (DPM) Chapter 31A, Section 3105, entitled “Safeguarding Information About Individuals,” provides:

3105.1 Controls shall be established in accordance with the following:

(a) The purpose of the controls is to ensure the integrity, security, and confidentiality of personnel records, regardless of form.

(b) The [DCHR] and each Independent Personnel Authority shall establish and ensure the maintenance of administrative, technical, and physical controls to protect personnel records from unauthorized access, use, modification or disclosure.

(c) Persons whose official duties require access to and use of personnel records are responsible and accountable for safeguarding them and ensuring that the records shall be secured whenever they are not in use or under the direct control of authorized persons.

(d) Personnel records shall be held, processed, or stored only where facilities and conditions are adequate to prevent unauthorized access.

3105.2 Personnel records shall be stored in metal filing cabinets when the records are not in use, or in a secured room. Alternative methods may be employed if they furnish an equivalent or greater degree of security.

• • •

3105.4 Only employees whose official duties require access shall be allowed to handle and use personnel records.

3105.5 To the extent feasible, entry into the personnel records storage areas shall be limited.

Through on-site observations, the OIG inspection team (team) learned that BRA is not securing employees’ and retirees’ personal information. Documents bearing data such as names, home addresses, telephone numbers, social security numbers, bank account and investment account numbers, and retirement plan distribution selections² are stored in unlocked filing cabinets and unlocked desks. Some filing cabinets are in cubicles that do not have locks. (See attachment 1.)

² An example of a retirement plan distribution selection is when an employee requests to have the full value of his/her pension transferred to a checking or savings account. In this instance, the distribution form processed by DCHR requires the employee to provide the name of the financial institution and the account number.

Other unlocked filing cabinets containing personal, sensitive information, including medical information, are in an unlocked copy room adjacent to a visitors' waiting area. (See attachments 2, 3, and 4.)

When customers enter the BRA office suite, they should be assisted promptly by a BRA employee and either escorted to a cubicle or office or directed to a seat in the visitors' waiting area. The reception desk is a busy location and is usually staffed by two employees. However, these employees' attention may not always be focused on the customers seated in the waiting area because they are also expected to complete other tasks, such as answer the telephone and review paperwork. If the employees on the desk are distracted, a customer can walk unnoticed into the copy room adjacent to the visitors' waiting area. In fact, on a recent Friday, a team member arrived at the main entrance of BRA when the reception desk was staffed by two employees who were busy. The team member was able to enter the copy room seemingly unnoticed.

The team also observed that the BRA suite is accessible to other DCHR employees (i.e., non-BRA employees) via a side entrance. This entrance appeared to be locked at all times and only accessible using an electronically coded badge, as is the main entrance to the suite after business hours. The team asked a senior BRA official to identify the number of DCHR employees whose coded badges allow them entry into the BRA suite, but s/he was unable to furnish the information. In addition, the building's cleaning staff moves through the suite after business hours unescorted.³

A senior BRA official said that s/he believed there were internal written policies and procedures regarding access to, accountability for, and storage of files maintained at BRA, and that these policies and procedures had been communicated verbally to employees. On three occasions—March 6, March 11, and March 16, 2009—the team asked the official to provide the OIG with a copy of those policies and procedures. As of this writing, the OIG has not received them.

Conclusion

An unspecified number of DCHR employees, as well as the building's cleaning staff, are able to access the BRA suite. Entry into the copy room where some documents containing sensitive information are kept is not well controlled; documents are also stored in unlocked filing cabinets and desks in open cubicles. Consequently, unsecured, sensitive information is vulnerable to unauthorized

³ A senior BRA official stated that pursuant to the cleaning contract, the cleaning staff are bonded. The OIG inspection team reviewed a copy of the District's city-wide janitorial services contract with R&R Janitorial, Painting and Building Services, Inc., which includes 441 4th Street, N.W., the District building that houses BRA. This contract does not require a surety bond, nor does it contain any provisions regarding theft by employees. (A surety bond is a "bond issued by an entity on behalf of a second party, guaranteeing that the second party will fulfill an obligation or series of obligations to a third party. In the event that the obligations are not met, the third party will recover its losses via the bond." A surety bond, however, is performance related, and does not ensure against theft. See http://www.investorwords.com/5813/surety_bond.html (last visited April 29, 2009).)

access, which could lead to theft and misuse. According to the Social Security Administration, "Identity theft is one of the fastest growing crimes in America."⁴

Recommendations

The OIG recommends that DCHR take the following actions:

1. Immediately safeguard all BRA documents and the information contained in them from unauthorized review, use, disclosure, and theft.
2. Ensure that BRA and all other DCHR components have written policies and procedures that comply with DPM Chapter 31A, Section 3105 and provide clear, detailed requirements for safeguarding all documents containing sensitive, personal information. Copies of these policies and procedures, if they currently exist, should be forwarded to the OIG upon receipt of this MAR, or as soon as they are drafted and approved by DCHR management.

Please provide your comments to this MAR by May 22, 2009. Your response should include actions taken or planned, dates for completion of planned actions, and reasons for any disagreement with the concerns and recommendations presented. Please distribute this MAR only to those who will be directly involved in preparing your response.

Should you have any questions prior to preparing your response, please contact [REDACTED], Director of Planning and Inspections, at [REDACTED].

Sincerely,



Charles J. Willoughby
Inspector General

CJW/mj

Attachments

cc: The Honorable Adrian M. Fenty, Mayor, District of Columbia
Mr. Daniel M. Tangherlini, City Administrator and Deputy Mayor
The Honorable Vincent C. Gray, Chairman, Council of the District of Columbia
The Honorable Mary M. Cheh, Chairperson, Committee on Government
Operations and the Environment

⁴ U.S. SOCIAL SECURITY ADMINISTRATION, IDENTITY THEFT AND YOUR SOCIAL SECURITY NUMBER, *available at* <http://www.ssa.gov/pubs/10064.html> (last visited April 20, 2009).

Attachment 1: Sensitive information on the desk and in the overhead filing cabinets of a cubicle that is not locked.



Attachment 2: Unlocked filing cabinets in the copy room that contain files with sensitive information.



Attachment 3: Unlocked filing cabinets in the copy room that contain files with sensitive information.



Attachment 4: Open, unlocked copy room door.



GOVERNMENT OF THE DISTRICT OF COLUMBIA
Department of Human Resources



Office of the Director

May 22, 2009

Charles J. Willoughby
Inspector General
Office of the Inspector General
717 14th Street, N.W., 5th Floor
Washington, D.C. 20005

Dear Mr. Willoughby:

This is in response to your May 8, 2009 Management Alert Report (MAR 09-I-006) wherein you provide a summary of your findings of a recent inspection of the Department of Human Resources (DCHR), Benefits and Retirement Administration (BRA). More specifically, your summary raises concerns about the protocols and safeguards BRA staff uses to ensure the confidentiality of employee benefit and retirement files in accordance with the procedures set forth in Chapter 31A, Section 3105 of the District Personnel Manual. DCHR is pleased to provide a response to the MAR and to outline the steps taken to address your concerns.

First, DCHR recognizes that the proper custody, use, and preservation of official information related to the day-to-day operations of the human resources functions of DCHR cannot be overemphasized. To this end, it is essential that all DCHR employees strictly comply with applicable provisions of law regarding confidentiality and the safeguarding of sensitive information. As such, rest assured that DCHR considers the issues you raise in the MAR to be of paramount importance and have already reviewed its current processes that are in place to ensure that they are sufficient to comply with both the spirit and the intent of the regulations regarding the protection of sensitive and personal information. These actions are set forth below along with DCHR's timeline for resolving these issues in their entirety:

Recommendation

Immediately safeguard all BRA documents and the information contained in them from unauthorized review, use, disclosure and theft.

DCHR Response

The suite which houses BRA staff has been closed to incoming customers to further secure personnel documents. Customer/employees must be escorted from the DCHR main reception area to receive benefits assistance.

All BRA staff have been provided with cabinets that lock and have been directed to secure all documents prior to leaving their assigned workstation. The copier area of the BRA suite is scheduled to have card reader access installed to prevent the entrance of any unauthorized persons.

All customer/employee counseling will be conducting in customer service cubicles and not at assigned work stations in order to further segregate personnel documents from incoming customer traffic.

Recommendation

Ensure that BRA and all other DCHR components have written policies and procedures that comply with DPM Chapter 31A, section 3105 and provide clear, detailed requirements for safeguarding all documents containing sensitive personal information. Copies of these policies and procedures if they currently exist, should be forwarded to the OIG upon receipt of the MAR, or as soon as they are drafted and approved by DCHR management.

DCHR Response

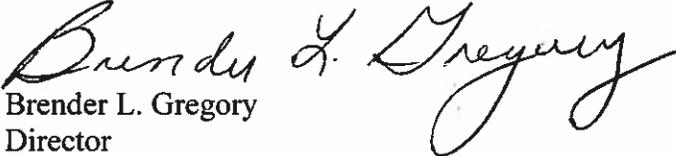
While DCHR agrees that it can strengthen its procedures with respect to these matters, DCHR disagrees with the MAR conclusion that access to the BRA offices by other DCHR employees represents a failure in safeguarding documents. Please note that all DCHR employees are considered confidential employees and as such have access to employee records whether those records consist of benefits and retirement information as in the case of BRA, other employment data such as information contained in the official personnel files; medical and other personal information contained in employee litigation and employee relations files. All DCHR employees need to have access to these records in order to carry out their day-to-day job responsibilities. Accordingly, while DCHR can ensure that DCHR employees safeguards these records whenever they have a need to access them to carry out their jobs; DCHR employees must have access to all units within DCHR as there are overlapping job responsibilities that require DCHR employees to work together to resolve issues. For this reason, DCHR has each employee sign a confidentiality form that underscores the need to safeguard documents and maintain confidentiality and outlines the consequences for violating the agency's confidential policies. Further, all BRA staff have been formally advised of the procedures and polices regarding the safeguarding of employee information, to include a written acknowledgement of Chapter 31, section 1305 of the District Personnel Manual.

Charles Willoughby
Office of the Inspector General
MAR-09-I-006
Page 3

With respect to access to DCHR offices by cleaning staff, DCHR agrees with your assessment and has taken measures to resolve this issue.

Thank you for allowing me the opportunity to respond to your report.

Sincerely,


Brender L. Gregory
Director

Enclosure(s)

cc: Karla Kirby-Sumpter
Associate Director for Benefits & Retirement

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Department of Human Resources



Protocol for the Security and Confidentiality of Government Employee Data

Employee Acknowledgment Form

I acknowledge receipt of DPM Chapter 31A – Records Management and Privacy of Records, Section 3105 – Safeguarding Information About Individuals.

3105 SAFEGUARDING INFORMATION ABOUT INDIVIDUALS

3105.1 Controls shall be established in accordance with the following:

(a) The purpose of the controls is to ensure the integrity, security, and confidentiality of personnel records, regardless of form.

(b) The D.C. Department of Human Resources and each Independent Personnel Authority shall establish and ensure the maintenance of administrative, technical, and physical controls to protect personnel records from unauthorized access, use, modification or disclosure.

(c) Persons whose official duties require access to and use of personnel records are responsible and accountable for safeguarding them and ensuring that the records shall be secured whenever they are not in use or under the direct control of authorized persons.

(d) Personnel records shall be held, processed, or stored only where facilities and conditions are adequate to prevent unauthorized access.

3105.2 Personnel records shall be stored in metal filing cabinets when the records are not in use, or in a secured room. Alternative methods may be employed if they furnish an equivalent or greater degree of security.

3105.3 Subject to the restrictions and conditions set forth in these regulations, the data subject may have access to his or her personnel records.

3105.4 Only employees whose official duties require access shall be allowed to handle and use personnel records.

3105.5 To the extent feasible, entry into the personnel records storage areas shall be limited.

3105.6 Documentation of the removal of records from the storage area shall be kept to ensure--

- (a) That adequate control is maintained; and
- (b) That removed records are returned on a timely basis.

3105.7 D.C. Government records shall be disposed of and destroyed in accordance with procedures issued by the D.C. Department of General Services.

3105.8 Federal records shall be disposed of in accordance with the procedures of the U.S. General Services Administration.

3105.9 In addition to following the security requirements of this section, managers of automated personnel records shall establish administrative, technical, physical, and security safeguards on data about individuals in automated records, reports, punched cards, magnetic tapes, disks, online computer storage, and other records maintained under the authority of the Act. The safeguards shall be in writing and, as a minimum, shall be sufficient to accomplish the following:

- (a) Prevent careless, accidental, or unintentional disclosure, modification, or destruction of identifiable personal data.
- (b) Minimize the risk that skilled technicians or knowledgeable persons could improperly obtain access to, modify, or destroy identifiable personal data.
- (c) Prevent casual entry by unskilled persons who have no official reason for access to such data.
- (d) Minimize the risk of an unauthorized disclosure where use is made of identifiable personal data in testing of computer programs.
- (e) Control the flow of data into, through, and from agency computer operations.
- (f) Adequately protect identifiable data from environmental hazards and unnecessary exposure.
- (g) Ensure adequate internal audit procedures to comply with these safeguards.
- (h) Dispose of identifiable personal data in automated files in such a manner as to make the data unobtainable by unauthorized personnel. Unneeded personal data stored in reusable media such as magnetic tapes and disks shall be erased prior to release of the media for reuse.

I understand that the purpose of the controls is to ensure the security, confidentiality and integrity of personnel records, regardless of form. Failure to adequately protect the records entrusted to me will result in administrative action.

Employee's Printed Name

Employee's Signature

Date

Distribution:
Employee
Official Personnel Folder