

GOVERNMENT OF THE DISTRICT OF COLUMBIA  
Office of the Inspector General

Inspector General



October 20, 2010

The Honorable Adrian M. Fenty  
Mayor  
District of Columbia  
Mayor's Correspondence Unit, Suite 316  
1350 Pennsylvania Avenue, N.W.  
Washington, D.C. 20005

Dear Mayor Fenty:

Enclosed please find a copy of a Management Implication Report (MIR 10-I-001), entitled *Inadequate Safeguarding of Sensitive Employee, Customer, and Client Information in District Agencies: A Recurrent Failure*, that the Office of the Inspector General (OIG) issued to the Office of the City Administrator (OCA) on September 2, 2010. OCA's response to the MIR, dated October 13, 2010, is also enclosed.

The MIR points out that since February 2000, the OIG has issued 17 reports that include findings of instances in which District agencies were not properly safeguarding sensitive, and in certain cases legally-protected information and documents, such as Social Security numbers, law enforcement records, and medical and personal financial data. The OIG published this MIR in an effort to address this persistent operational weakness and mitigate, among other things, the potential for future loss or misuse of information.

We are providing this information so that you will be aware of the importance and prevalence of the issues cited in the MIR and the corrective actions planned as stated by the OCA.

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

Sincerely,

  
Charles J. Willoughby  
Inspector General

CJW/ef

Enclosures

cc: See distribution list

**DISTRIBUTION:**

Mr. Neil O. Albert, City Administrator and Deputy Mayor, District of Columbia (1 copy)  
Ms. Valerie Santos, Deputy Mayor for Planning and Economic Development, 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, Department of Human Resources  
Mr. Andrew T. Richardson, III, Interim Director and Chief Risk Officer, Office of Risk Management  
Ms. Stephanie Scott, Secretary of the District of Columbia, Office of the Secretary of the District of Columbia  
Mr. Bryan Sivak, Chief Technology Officer, Office of the Chief Technology Officer  
Ms. Kai A. Blissett, Interim 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)  
Ms. Merav Bushlin, Chief of Budget Development and 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. William DiVello, 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. Jeanette M. Franzel, Managing Director, FMA, GAO, Attention: Norma J. Samuel (1 copy via email)  
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, 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 Susan Collins, 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 IMPLICATION REPORT***

**OFFICE OF THE CITY ADMINISTRATOR**

**INADEQUATE SAFEGUARDING OF SENSITIVE  
EMPLOYEE, CUSTOMER, AND CLIENT INFORMATION  
IN DISTRICT AGENCIES:  
A RECURRENT FAILURE**

**MIR 10-I-001**

**SEPTEMBER 2, 2010**

---

**Inspections and Evaluations Division**  
**Mission Statement**

The Inspections and Evaluations (I&E) Division of the Office of the Inspector General is dedicated to providing District of Columbia (D.C.) government decision makers with objective, thorough, and timely evaluations and recommendations that will assist them in achieving efficiency, effectiveness, and economy in operations and programs. I&E goals are to help ensure compliance with applicable laws, regulations, and policies, to identify accountability, recognize excellence, and promote continuous improvement in the delivery of services to D.C. residents and others who have a vested interest in the success of the city.

GOVERNMENT OF THE DISTRICT OF COLUMBIA  
Office of the Inspector General

Inspector General



September 2, 2010

Neil O. Albert  
City Administrator and Deputy Mayor  
Office of the City Administrator  
1350 Pennsylvania Avenue, N.W., Suite 533  
Washington, D.C. 20004

Dear Mr. Albert:

This is a Management Implication Report (MIR 10-I-001) to inform you that the Office of the Inspector General (OIG) has observed numerous instances in which District agencies were not properly safeguarding sensitive employee, customer, and client information. Since February 2000, the OIG has issued 17 reports that include findings on this matter. The OIG issues MIRs on matters of priority concern that affect multiple District agencies.

### **Background**

The U.S. Government Accountability Office (GAO) report entitled *Internal Control Management and Evaluation Tool* states that an agency should ensure that “[t]he risk of unauthorized use or loss is controlled by restricting access to resources and records only to authorized personnel.”<sup>1</sup>

The District Personnel Manual (DPM) § 3100 states:

All official personnel records of the District Government shall be established, maintained, and disposed of in a manner designed to ensure the greatest degree of applicant or employee privacy while providing adequate, necessary, and complete information for the District to carry out its responsibilities under the District of Columbia Government Comprehensive Merit Personnel Act of 1978, D.C. Law 2-139, ... and other laws governing personnel management in the District of Columbia Government.

Additionally, DPM § 3105.1(c) states:

Persons whose official duties require access to and use of personnel records are responsible and accountable for safeguarding

---

<sup>1</sup> GOVERNMENT ACCOUNTABILITY OFFICE, INTERNAL CONTROL MANAGEMENT AND EVALUATION TOOL, GAO-01-1008G, 42 (August 2001).

them and ensuring that the records shall be secured whenever they are not in use or under the direct control of authorized persons.

The DPM further provides that the “Office of Personnel and agency employees whose official duties involve personnel records shall be sensitive to individual rights to personal privacy and shall not disclose information from any personnel record unless disclosure is part of their official duties or required by regulation or statute (e.g., required by the D.C. Freedom of Information Act [D.C. FOIA]).”<sup>2</sup> The D.C. FOIA does not *per se* prohibit the release of employee Social Security numbers, but rather grants agencies the discretion to “exempt from disclosure ... [i]nformation of a personal nature where ... public disclosure ... constitute[s] a clearly unwarranted invasion of personal privacy.” See D.C. Code § 2-534(a)(2)(Supp. 2009).

Some of our reports included criteria about safeguarding sensitive information beyond personnel records and employees’ Social Security numbers. For instance, the Health Insurance Portability and Accountability Act’s (HIPAA) Privacy Rule protects the privacy of “individually identifiable” health information; the HIPAA Security Rule sets national standards for the security of electronic protected health information.<sup>3</sup> Similarly, the Code of the National Association of Social Workers (NASW) § 1.07(l) entitled Privacy and Confidentiality states, in part, “Social workers should protect the confidentiality of clients’ written and electronic records and other sensitive information.”

The OIG reviewed publications from other District and federal agencies to assess whether they had procedures on safeguarding sensitive information. In October 2008, the U.S. Department of Homeland Security (DHS) issued a *Handbook for Safeguarding Sensitive Personally Identifiable Information*. Applicable to every DHS employee, contractor, detailee, and consultant, the handbook provides guidance on how to identify, protect, and dispose of Sensitive Personally Identifiable Information (Sensitive PII), such as Social Security numbers. DHS’ handbook defines “Sensitive PII” as: “personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.”<sup>4</sup>

## Observation

### **Recurring detection of problems with safeguarding sensitive information in District agencies.**

As illustrated in Table 1 on the following page, the OIG has detected lapses in the proper security, use, and disposal of sensitive information in numerous District agencies. In particular, from February 2000 through April 2010, the OIG issued findings on this matter in 17 different reports. These reports include Management Alert Reports (MARs) and Reports of Inspection

---

<sup>2</sup> *Id.* § 3106.2

<sup>3</sup> <http://www.hhs.gov/ocr/privacy/> (last visited August 17, 2010).

<sup>4</sup> U.S. DEPARTMENT OF HOMELAND SECURITY, HANDBOOK FOR SAFEGUARDING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION, 4 (October 31, 2008)(emphasis omitted).

(ROIs) issued by the Inspections and Evaluations Division, as well as reports and MARs issued by our Audit and Investigations Divisions and the Medicaid Fraud Control Unit.

**Table 1 – Reports Issued by the OIG Regarding Inadequate Safeguarding of Sensitive Information (July 2000 – April 2010)**

<b>Report</b>	<b>Agency</b>	<b>Date</b>	<b>Key Issues</b>	<b>Risk</b>
MAR 10-I-002	<b>Department of Human Services (DHS)</b>	April 2010	Inadequate safeguarding of case files with sensitive and legal information within DHS' Adult Protective Services.	Invasion of privacy; identity theft; exploitation of vulnerable citizens.
ROI 10-I-0033DH	<b>Public Service Commission</b>	Feb. 2010	EEO <sup>5</sup> records improperly stored (Pages 2 and 14).	Sensitive personnel and personal information exposed to unauthorized use and theft.
MAR 09-I-009	<b>Metropolitan Police Department (MPD)</b>	Sept. 2009	Lack of security of videotapes, case records with juvenile arrest, and child abuse information within MPD's Youth Investigations Division.	Legally protected, sensitive information exposed to unauthorized use and theft.
MAR 09-I-006	<b>Department of Human Resources (DCHR)</b>	May 2009	Inadequate safeguarding of sensitive information of D.C. government employees and retirees.	Identity theft; delays and disruption of benefits.
Audit OIG-07-2-31FB	<b>Fire and Emergency Medical Services Department</b>	March 2009	Inadequate protection of Patient Care Records within the Ambulance Billing unit (Pages 14-19).	Sensitive medical information exposed to unauthorized use and theft.
ROI 08-I-027CF	<b>Department of Mental Health</b>	Nov. 2008	Students' clinical records not properly controlled and maintained (Pages 68-71).	Legally protected, sensitive clinical information exposed to unauthorized persons.
MAR 08-I-008	<b>Alcoholic Beverage Regulation Administration</b>	Aug. 2008	Inadequate security of sensitive information of applicants for alcoholic beverage licenses.	Identity theft; fraudulent and illegal business operations.
ROI 07-I-026CF	<b>DCHR</b>	May 2008	Official Personnel Files not transported in a secure manner (Page 86).	Loss of confidential personnel information; delay or halt of personnel actions; identity theft.
MAR 2-ID-2008	<b>Department of Consumer and Regulatory Affairs (DCRA)</b>	Dec. 2007	Release of sensitive information during an ongoing investigation.	Sensitive information exposed to unauthorized persons; hindrance of ongoing investigations.

<sup>5</sup> EEO refers to Equal Employment Opportunity.

**Table 1 – Reports Issued by the OIG Regarding Inadequate Safeguarding of Sensitive Information (July 2000 – April 2010) – continued**

<b>Report</b>	<b>Agency</b>	<b>Date</b>	<b>Key Issues</b>	<b>Risk</b>
ROI 07-0022-SEO	State Education Office <sup>6</sup>	July 2007	File room containing tuition applications with Social Security numbers not secure (Pages 6, 54-56).	Identity theft; tuition fraud.
ROI 06-0018-CR (Part II)	DCRA	Sept. 2006	Security deficiencies in handling licensing documents: No written security procedures for photo ID badges; business license applications not properly filed and stored. (Pages 23-27).	Issuance of fraudulent licenses; creation of false IDs; operation of illegal businesses.
MAR 06-A-12	District of Columbia Public Schools	Aug. 2006	Improper release of school employees' Social Security numbers via a FOIA request.	Identity theft.
MAR 06-M-02	Mental Retardation and Developmental Disabilities Administration <sup>7</sup>	July 2006	Disclosure of clients' Social Security numbers on Incident Report Forms.	Identity theft.
ROI 03-0011CM	Office of the Chief Medical Examiner	Sept. 2003	Case records containing private, sensitive, vital personal information not properly secured, stored in areas of uncontrolled access (Pages 88-89).	Identity theft.
ROI 02-00002FL	Department of Corrections (DOC)	Oct. 2002	Inmate records handled insecurely; quality control lacking within DOC's Central Detention Facility (Pgs 28-29, 32-33).	Misidentification of inmates; errors in inmate release.
ROI 00-0002HC	Medical Assistance Administration <sup>8</sup>	July 2000	Confidential patient records thrown in trash without shredding (Pages 30-31).	Identity theft; exposure of confidential medical information.

<sup>6</sup> Currently named the Office of the State Superintendent of Education.

<sup>7</sup> Currently named the Department on Disability Services.

<sup>8</sup> Currently named the Department of Health Care Finance.

**Table 1 - Reports Issued by the OIG Regarding Inadequate Safeguarding of Sensitive Information (July 2000 – April 2010) – continued**

Report	Agency	Date	Key Issues	Risk
ROI 00-0001KV	Department of Motor Vehicles (DMV)	Feb. 2000	Cards containing identifying personal information for driver's licenses and ID cards not securely maintained (Pages 27-30).	Identity theft; personal property threat.
			Voter registration forms with personal information not securely maintained (Page 30).	Identity theft; voter fraud; personal property threat.
			Discarded applications and forms with DMV customers' personal information put in regular trash containers without shredding (Page 44).	Identify theft; personal property threat.
			No secure, restricted access to and storage of title documents, validation stickers, registration cards, license plates, inspection stickers, and residential parking permits. Workstation that dispensed these instruments was vulnerable to unauthorized access (Pages 46-50).	Identity theft; auto theft and misuse; parking permit fraud; government information tampering and theft.

**Conclusion**

The OIG has detected numerous instances in multiple agencies where proper safeguards for sensitive information were not in place. Consequently, this information was vulnerable to loss, theft, misuse, or alteration, and there is potential harm to District, commercial, and private interests. The OIG recommended that many of the aforementioned agencies develop/improve and disseminate policies and procedures regarding the use and storage of sensitive information and ensure that employees who handle such information are trained to implement these policies and procedures. Consequently, some agencies may have these components in place. However, given the pattern of deficient internal control noted in Table 1, the OIG believes that District-wide policies, procedures, and training regarding the identification, use, protection, and disposal of sensitive information are necessary. Additionally, the GAO *Internal Control Management and Evaluation Tool* provides that continuous program monitoring is a necessary component of

internal control.<sup>9</sup> The development of a District-wide oversight mechanism may help mitigate the potential loss or misuse of sensitive information.

Safeguarding sensitive information is of particular concern because, according to the Social Security Administration, “identity theft is one of the fastest growing crimes in America.”<sup>10</sup> Over the years, our reports have found that the District has compromised sensitive information due to a lack of proper safeguards. For example, in June 2006, ING informed the District government that one of its computers, which contained sensitive information on participants in the District’s 457 Deferred Compensation Plan (DCPLUS) and the 401(a) Defined Contribution Pension Plan, was stolen. Because unencrypted data were not secured, the Social Security numbers, birthdates, and addresses of over 14,000 D.C. employees and retirees may have been compromised.<sup>11</sup>

## Recommendations

The OIG recommends that the City Administrator:

1. collaborate closely with the Office of the Secretary, the Office of Risk Management, the Department of Human Resources, and the Office of the Chief Technology Officer to promulgate District-wide government information security policies and procedures<sup>12</sup> that define: a) criteria for sensitive information; b) how to properly use, protect, and dispose of such information; and c) steps an employee should take if he/she thinks sensitive information may have been compromised;
2. collaborate with the Office of the Secretary and the Office of Risk Management, and other District agencies as necessary (e.g., the Workforce Development Administration), to develop or recommend training on the promulgated information security policies and procedures;
3. direct District agency heads to:
  - a. designate an information security official who will monitor the handling, maintenance, and proper disposal of sensitive information. This official might also ensure that employees are trained on how to carry out these responsibilities;
  - b. report semi-annually to the City Administrator and the District’s Office of Risk Management regarding agency compliance with information security policies and procedures, any violations or deficiencies identified, and any planned or corrective actions taken to address these items; and

---

<sup>9</sup> GOVERNMENT ACCOUNTABILITY OFFICE, INTERNAL CONTROL MANAGEMENT AND EVALUATION TOOL, GAO-01-1008G, 59 (August 2001).

<sup>10</sup> U.S. SOCIAL SECURITY ADMINISTRATION, IDENTITY THEFT AND YOUR SOCIAL SECURITY NUMBER, *available at* <http://www.ssa.gov/pubs/10064.html> (last visited August 4, 2010).

<sup>11</sup> See [http://dchr.dc.gov/dcop/cwp/view,a.1221.q.635792.dcopNav\\_GID.1518.asp](http://dchr.dc.gov/dcop/cwp/view,a.1221.q.635792.dcopNav_GID.1518.asp) (last visited August 4, 2010).

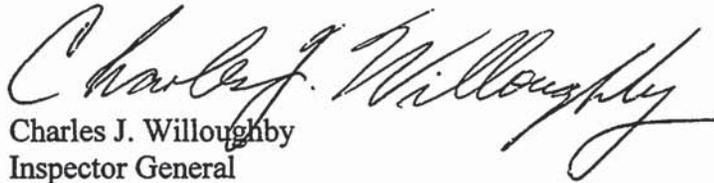
<sup>12</sup> In August 2010, the OIG spoke with an official from the Office of the Secretary who was not aware of any comprehensive, city-wide policy on safeguarding sensitive information.

4. develop an oversight mechanism to assess agency compliance with information security policies, procedures, and training requirements. The mechanism should include annual and unscheduled inspections, and the results of these inspections should be reported to the City Administrator and the respective agency head with recommendations for improvement.

Please provide your comments to the MIR by September 17, 2010. 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 MIR only to those who will be directly involved in preparing your responses.

Should you have any questions prior to preparing your response, please contact Alvin Wright, Jr., Assistant Inspector General for Inspections and Evaluations, on (202) 727-8452.

Sincerely,



Charles J. Willoughby  
Inspector General

CJW/ebs

cc: The Honorable Mary M. Cheh, Chairperson, Committee on Government Operations and the Environment, Council of the District of Columbia  
Mr. Peter Nickles, Attorney General for the District of Columbia, Office of the Attorney General  
Ms. Brender L. Gregory, Director, Department of Human Resources  
Mr. Andrew T. Richardson, III, Interim Director and Chief Risk Officer, Office of Risk Management  
Ms. Stephanie Scott, Secretary of the District of Columbia, Office of the Secretary of the District of Columbia  
Mr. Bryan Sivak, Chief Technology Officer, Office of the Chief Technology Officer



**Government of the  
District of Columbia**

**Office of the Inspector General**

*Report Fraud, Waste,  
Abuse, or Mismanagement to:*

**Charles J. Willoughby  
Inspector General**

**Toll Free Hotline:**

**1-800-521-1639  
or 202-724-TIPS (724-8477)  
or [hotline.oig@dc.gov](mailto:hotline.oig@dc.gov)**

**All calls are Confidential.**

**Address:**

**Office of the Inspector General  
717 14th Street, NW  
Suite 500  
Washington, D.C. 20005**

**Web Page: [www.oig.dc.gov](http://www.oig.dc.gov)**

---

GOVERNMENT OF THE DISTRICT OF COLUMBIA  
EXECUTIVE OFFICE OF THE MAYOR



Office of the City Administrator

October 13, 2010

Mr. Charles J. Willoughby  
Inspector General  
Government of the District of Columbia  
717 14<sup>th</sup> Street NW  
Washington DC 20005

Dear Mr. Willoughby:

Thank you for forwarding on the Management Implication Report (MIR 10-I-001) entitled "Inadequate Safeguarding of Sensitive Employee, Customer, and Client Information in District Agencies: A Recurrent Failure." That report highlighted 17 incidents of that nature that were reported in District agencies from February 2000 through April 2010. The rest of this letter will serve as responses to your specific recommendations in that report.

*Recommendation 1: Collaborate closely with the Office of the Secretary, the Office of Risk Management, the Department of Human Resources, and the Office of the Chief Technology Officer to promulgate District-wide government information security policies and procedures that define: a) criteria for sensitive information; b) how to properly use, protect, and dispose of such information; and c) steps and employee should take if he/she thinks sensitive information may have been compromised.*

Response: The City Administrator will direct the Office of Risk Management (ORM) to take the lead with developing a policy document that covers these topics. ORM will be required to submit the policy document to the City Administrator by November 30<sup>th</sup>, 2010. The City Administrator will review the policy document and disseminate to all agency directors by December 7<sup>th</sup>, 2010.

*Recommendation 2: Collaborate with the Office of the Secretary and the Office of Risk Management, and other District agencies as necessary (e.g., the Workforce Development Administration), to develop or recommend training on the promulgated information security policies and procedures.*

Response: The City Administrator will direct ORM to develop a portion of its web-site that will post the policy, answers to frequently asked questions about the policy, and links to several press stories about how the issue has caused major problems for other government agencies. This will be live by December 31, 2010.

*Recommendation 3: Direct District agency heads to: a) designate an information security official who will monitor the handling, maintenance and proper disposal of sensitive*

*information. This official might also ensure that employees are trained on how to carry out these responsibilities; and b) report semi-annually to the City Administrator and the District's Office of Risk Management regarding agency compliance with information security policies and procedures, any violations or deficiencies identified, and any planned or corrective actions taken to address these items.*

Response: The City Administrator will direct ORM to include a call for the designated information security official for each agency into the policy memo. ORM will also develop and maintain a roster of agency information security officials. The agencies will submit a name to ORM by December 31<sup>st</sup>, 2010. In terms of reports, we will direct ORM to include a recommendation for a monitoring protocol within their policy memo to be submitted to OCA by November 30, 2010.

*Recommendation 4: Develop an oversight mechanism to assess agency compliance with information security policies, procedures and training requirements. The mechanism should include annual and unscheduled inspections, and the results of these inspections should be reported to the City Administration and the respective agency head with recommendation for improvement.*

Response: The City Administrator will direct the ORM to define an oversight mechanism in its policy memo due to the City Administrator by November 30<sup>th</sup>, 2010.

Please let me know if you have any questions.

Sincerely,



Neil O. Albert  
City Administrator