South Florida Water Management District

Protector of the Everglades since 1949

Audit of the Worker Separation Process

Project # 10-17

Prepared by
Office of Inspector General

John W. Williams, Esq., Inspector General
J. Timothy Beirnes, CPA, Director of Auditing
Jankie Bhagudas, CPA, Lead Consulting Auditor

SOUTH FLORIDA WATER MANAGEMENT DISTRICT

April 13, 2011

Audit and Finance Committee Members:
Mr. Charles J. Dauray, Chair
Mr. Joe Collins, Member
Glenn J. Waldman, Esq., Member

Re: Audit of the Worker Separation Process
Project No. 10-17

This audit was performed pursuant to the Inspector General's authority set forth in Chapter 20.055, F.S. The objectives focused on examining the internal controls over disabling access to District information systems and facilities and retracting District property when employees, interns, and contract workers separate from the District. This report was prepared by Tim Beirnes and Jankie Bhagudas.

Sincerely,

John W. Williams, Esq.
Inspector General

TABLE OF CONTENTS

BACKGROUND

In accordance with the Office of Inspector General's Fiscal Year 2010 Audit Plan, we conducted an Audit of the Separation Process that examined the internal controls over disabling access to District information systems and facilities and retracting District property when employees, interns, and contract workers separate from the District.

The Human Resources Solutions Department (Human Resources Solutions) is situated in the Corporate Resource Area and is responsible for enabling the District to achieve its mission by attracting and retaining a high quality, diverse workforce; and to provide guidance, service and development that enables employee success. As of the June 15, 2010, the District's full-time equivalent employees totaled 1,842. In addition, the District uses contract workers to supplement its workforce. Contract workers are used for short term projects and are also used to perform activities that are long-term, recurring, and permanent in nature. In many cases, contract workers are utilized for particular positions or functions because of full-time equivalent employees limits for District staff. The District also employs a limited number of paid interns, usually during the summer months.

Employees, interns, and contract workers are separated from the District either voluntarily (normal separations may be due to resignation, retirement, and death) or involuntarily separations. Human Resources Solutions and the Information Technology Department are primarily responsible for the separation process. Depending on the separation method, the process can be initiated by the following:

- Human Resources Solutions
- Information Technology Department's Security Department
- Contract end date recorded in the Human Resources module of SAP (SAP HR)

In June 2009, the District implemented the Identity Management System (IDM) that automated the account creation process for certain Information Technology systems and requires a single sign-on to access certain accounts (i.e., District users have to remember only one password to access various District systems). The Identity Management System is also programmed to: 1) automatically disable access to the District's network once the separation process is initiated; 2) generate an e-mail notification to a pre-determined list of District staff, which requires some staff to take action, for example, disable manual system access and cancel procurement cards; and 3) generate Remedy system tickets for retrieving equipment such as laptops and personal computers.

The table below and Appendix A summarizes how separations are triggered and the results of these actions.

METHOD OF SEPARATION	ACTION INITIATATING SEPARATION	RESULTS
• Employee and Interns – Voluntary (Normal) • Contract Workers (before the contract end date)	Human Resources Solutions separating the employee, intern, or contract worker in SAP HR	After the separation action, the Identity Management System starts the disabling and notification process. In instances where contract workers leave at the end of their contract date, Human Resources Solutions has to separate the contract worker in SAP HR.
Contract workers (on their contract end date)	Automatically by the Identity Management System based on the contract end date	
Involuntary – employees, interns, and contract workers	Information Technology Security disabling the employee, intern, or contract worker in the Identity Management System	Information Technology Security disables access to certain District systems and triggers the e-mail separation notification. It should be noted that Information Technology Security can perform any separation, if necessary.

As indicated above, upon separation from the District access to some District accounts are disabled automatically and others must be done manually. The Identity Management System is designed to automatically disable access to the following:

- *Active Directory (AD)* – A repository used for authenticating users when they login to the District network. A user must be created in the Active Directory before they can access District network. Access to this account is required for accessing secondary accounts, such as, Oracle database accounts.
- *Microsoft Exchange* – A system used by the District for e-mails.
- *Oracle Internet Directory (OID)* – A repository used for authenticating users when they login to the District Portal. A user must be created in the Oracle Internet Directory before they can access the District Portal.

- *UNIX* – Account used by some District users to run information technology applications on the District server. Several District application run only on the Sun Solaris System. Users must have a UNIX account to run these applications.
- *SAP R/3* – Software used by the District to manage its business processes.
- *SAP Portal* – Provides access to the Employee Self Service.
- *Remedy Account* – Remedy is an incident management system for service requests. e.g., tickets are generated to retrieve personal computers and laptops.
- *Cisco's Unity Voicemail* – System used for voicemail.

Further, the Identity Management System automatically generates an e-mail notification of each separation from the District to relevant staff and groups (for example, Human Resources Solutions, Information Technology Department, SAP Solution Center, and CERP Security). Certain staff on the e-mail separation notification list are responsible for manually disabling access to those systems not automatically disabled by the Identity Management System and for retrieving and disabling access to District property. For example, the e-mail separation notification is sent to pertinent staff in the following departments to take specific actions:

- Human Resources Solutions to separate employees, interns, and contract workers in SAP in cases where separations are performed by Information Technology Security and to determine whether education reimbursements have to be repaid to the District.
- Information Technology Department to disable Oracle database accounts, Supervisory Control and Data Acquisition (SCADA) systems, and VPN tokens; cancel and retrieve wireless devices; and retrieve personal computer equipment.
- Procurement Department to cancel procurement cards.
- SAP Solution Center Security to terminate access to SAP Business Intelligence (SAP BW).
- District Security to deactivate security badges.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our audit objective focused on examining the internal controls over disabling access to District information systems and facilities and retracting District property when employees, interns, and contract workers separate from the District.

To accomplish our objectives we obtained an understanding of the separation process and procedures by interviewing key personnel in Human Resources Solutions and the Information Technology Department and reviewing relevant policies and procedures, for example, the District's Separation Policy. We analyzed relevant information maintained by Human Resources Solutions (e.g., SAP HR data), Information Technology Department (e.g., Identity Management System and Oracle Database), SAP Solution Center, Procurement Department, and by various other sources to accomplish our audit objectives.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

AUDIT RESULTS

Executive Summary

Overall, we found that there are sufficient controls in place to ensure that access to District accounts are disabled, District property is retrieved, and security access is deactivated when employees, interns, and contract workers separate from the District. Specifically, once the separation process is initiated the Identity Management System automatically disables access to the District network principal accounts, generates an e-mail separation notification to relevant District staff responsible for manually disabling access to those systems not automatically disabled, and generates Remedy system tickets for retrieving equipment such as laptops and personal computers.

It should be noted that we found the controls over disabling Active Directory accounts in the Identity Management System were effective. The Identity Management System is often referred to a "single sign-on" system, which eliminates the users' need to remember multiple user IDs and passwords. Thus, once such account is deactivated it also prevents access to other key systems that can only be accessed by first signing onto the District's network. (See list of such systems on pages 2 and 3). Thus, even if access to these other systems is not disabled in a timely manner, the former worker would still be unable to access the systems that require the user to first sign-on to the District's network.

We found that procurement cards issued to separated employees were terminated in a timely manner. However, we identified certain improvements could be made to further strengthen the separation process, as summarized below.

- In instances where Human Resources Solutions is responsible for initiating the separation process in SAP HR, we found that the process was not always initiated in a timely manner. As a result, employees', interns', and contractor workers' access to District systems remained active after they were no longer with the District. For example, our review of 125 separated contract workers revealed that Human Resources Solutions did not initiate the separation process for 39 of the 125 (31%) contract workers until 2 to 23 days after they left the District.
- Human Resources Solutions did not always manually separate contract workers in SAP HR in a timely manner after they were separated by the Identity

Management System. As a result, contract workers appeared as active in SAP HR until they were separated. Our review of 109 separated contract workers disclosed that 44 (40%) appeared active in SAP HR anywhere from 21 to 50 days after they left the District.

- Oracle database accounts are required to be manually disabled upon separation; however, our review disclosed that 52 of 77 (68%) separated employees, interns, and contract workers District Oracle database accounts were not disabled until 100 – 323 days after they separated from the District. Failure to lock these accounts promptly could pose a security threat to District information.
- SAP Business Warehouse accounts are required to be manually disabled upon separation; however, it appears that the SAP Solution Center's Security Team was not on the list of the staff/groups that receive the e-mail separation notification. The SAP Solution Center Security Team became aware of some separations though conversations with District staff and other controls they have in place to ensure that SAP is accessed only by authorized staff. We noted that 10 of the 21 (48%) separated employees and contract workers accounts in the SAP Business Warehouse were not terminated until 5 to 70 days after they separated from the District. During our audit, the Security Team was added to the notification list.
- Wireless devices were not terminated in a timely manner upon separation from the District. We noted that seven separated employees were assigned District wireless devices and that four of the seven wireless devices remained active anywhere from 23 – 126 days after the employees separated from the District.
- A review of desktop and laptop retrieval information for 29 separated employees and contract workers revealed that in eight instances the equipment was not retrieved until 7 – 24 working days after the e-mail separation notification. In these instances, no specific reasons were provided for the delay. Further, there are no specific timeframe within which to retrieve desktops and laptops after separation.
- Deactivation of security badges could be improved and only about 25% of the actual badges are returned to the Safety, Security & Emergency Management

Department. It is important that badges be deactivated and returned upon separation since they can be used to access District facilities.

- The Information Technology Security Unit strengthened the process for disabling RSA tokens and Supervisory Control and Data Acquisition (SCADA) Systems access during our audit.
- In accordance with District policies, a separated employee should have repaid the District $1,135 for educational reimbursement he received during his last year of employment with the District. This amount was not recouped due to an oversight by Human Resources Solutions.
- A listing of separated employees, interns, and contract workers from the Identity Management System did not include a total of 39 separations that we determined were indeed disabled in the Identity Management System. Information Technology Department staff is working to resolve this issue.

Timeliness of Initiating the Separation Process Should be Improved

We found that once the separation process is initiated by Human Resources Solutions or the contract end date in SAP HR, the Identity Management System automatically disables access to certain principal accounts and generates an e-mail separation notification to relevant District staff informing them of the separation. The Identity Management System interfaces with SAP HR and constantly checks the separation date fields for information. Data in this field triggers the separation process and access is disabled and notifications are generated. However, our review disclosed that in cases where the separation process has to be initiated by Human Resources Solutions, the process was not always initiated in a timely manner.

Employee Separations Initiated in SAP HR by Human Resources Solutions

During the period from July 1, 2009 to March 31, 2010, a total of 45 employees were separated from the District (35 were voluntary separations that were initiated by Human Resources Solutions and 10 were involuntary separations that were initiated by Information Technology Security). For the 35 voluntary separations, we compared the effective separation dates (i.e., the day after the employee's last day with the District) to the dates that Human Resources Solutions separated the employees in SAP HR (as this action triggers the Identity Management System to disable the employee's user ID and sends out the e-mail termination notification). Based on our comparison, voluntary separations were usually not processed by Human Resources Solutions on the day employees separated from the District as detailed in the following table:

Voluntary Employee Separations Initiated by Human Resources Solutions		
Separation Action by Human Resources Solutions in SAP HR	**Number of Employees**	**%**
On the employee’s last day or the employee’s effective separation date (i.e., the day after the employee separated from the District)	10	*29%*
1-2 days after the employee's effective separation date	7	*20%*
3-5 days after the employee's effective separation date	13	*36%*
6-10 days after the employee's effective separation date	3	*9%*
Over 10 days after the employee's effective separation	2	*6%*
Total	**35**	***100%***

Human Solutions Resources staff explained that separations were not processed on the employee’s last day or the effective separation date because of the following:

- The employee’s department did not forward the separation paperwork needed to separate the employee in SAP HR in a timely manner.
- Human Resources Solutions received the separation paperwork prior to the separation date but did not separate the employee in SAP HR in a timely manner.

Contract Worker and Intern Separations Initiated in SAP HR by Human Resources Solutions

In instances where contract workers separate from the District before their contract end date, access is either disabled by Human Resources Solutions when the separation is voluntary or by Information Technology Security when the separation is involuntary. We reviewed 125 instances, during the period from July 1, 2009 to March 31, 2010, where contract workers voluntarily left the District before their contract end date to determine whether Human Resources Solutions initiated the separation process in SAP HR on the contract workers’ last day with the District. We noted the following:

- 86 of the 125 (69%) contract workers were separated in SAP HR on the same day or the day after they left the District. As a result, certain District accounts were automatically disabled by the Identity Management System and the separation e-mail notification in a timely manner.
- 39 of the 125 (31%) contract workers were not separated on the same day as their last day. These contract workers' accesses were disabled anywhere from 2 to 23

days after they left the District. As a result, the contract workers' District accounts that are automatically disabled by the Identity Management System were not disabled, the e-mail separation notifications were not generated to staff to manually disable other account accounts, retrieve equipment, and de-active security access, and the Remedy tickets were not created until 2 to 23 days after the contract workers left the District.

Human Solutions Resources staff explained that separations may not have been processed on the contract workers last day because they were not notified that the contract workers left the District. They explained that e-mails are sent to District project managers who supervise contract workers at the start of each month, two weeks before the contract end date, and 48 hours before the contract end date. These e-mails inform them to report any changes in the contract workers status to Human Resources Solutions so that contract worker's data in SAP HR can be updated. Human Resources Solutions staff also stated that they may have been informed of the separation on time but did not update SAP HR in a timely manner.

It should be noted that a total of 23 District interns separated from the District during the period July 1, 2009 to March 31, 2010. Our review disclosed that 13 of the 23 (57%) interns were not separated the day after their last day with the District. These interns' access were disabled anywhere from 6 to 28 days after they separated from the District.

In instances where the separation process is initiated in SAP HR by Human Resources Solutions, it is important that the process be initiated on the employee's, intern's or contract worker's last day with the District or the day after. Recognizing that initiating the separation process in SAP HR requires departments to submit paperwork in a timely manner, it is important that the process be completed timely in order to trigger the Identity Management System process. If not, their accounts that are automatically disabled by the Identity Management System remain active, staff are not notified of the separation to disable other account access manually (for example, Oracle database and Supervisory Control and Data Acquisition (SCADA)) and retrieve District property, and Remedy tickets were not generated. Accounts that are not disabled in a timely manner could present a security risk to the District.

Separation Records Should be Updated in a More Timely Manner

In instances where a contract worker's last day with the District is the same as their contract end date, as indicated in SAP HR, the Identity Management System is programmed to automatically disable the contract workers' access to the District network, generate the e-mail notification of the separation to relevant staff, and create Remedy tickets, one day after the contract end date. In these instances, Human Resources Solutions has to separate the contract worker in SAP HR. If this action is not performed, the contract worker will appear as active in SAP HR.

As part of our tests, we reviewed 109 of these instances that occurred during July 1, 2009 to March 31, 2010. We concluded that Human Resources Solutions did not separate the contract workers in SAP HR in a timely manner. Our conclusion is based on the following:

Human Resources Solutions' Update of SAP HR when Contract Workers' Separate on their Contract End Date

Timing of Separation by Human Resources Solutions in SAP HR	**Number of Contract Workers**	**%**
On the same day or within five days of separation	46	*42%*
6 - 20 days after separation	15	*14%*
21 - 50 days after separation	44	*40%*
Over 50 days after separation	4	*4%*
Total	**109**	***100%***

Further, we noted that three contract workers were separated by Information Technology Security. As a result, Human Resources Solutions had to separate the contract workers in SAP HR to reflect the separations. However, Human Resources Solutions did not separate the contract workers in SAP HR until 21 days later after they left the District.

We also noted four instances where contract workers separated from the District in June 2009 prior to the end of their contract term. However, it appears that their District access was not disabled until their contract end dates (September 30, 2009 and January 13, 2010). As a result, access to their District accounts were active 111 days to 201 days after their separation. According to Information Technology Department staff, the Identity Management System was implemented in June 2009 and there may have been a glitch in the system.

It is important that Human Resources Solutions update SAP HR in a timely manner to reflect separations. Failure to update SAP HR distorts the actual number of contract workers with the District at any given time.

Oracle Database Accounts and SAP Business Warehouse Accounts Should be Disabled in a More Timely Manner

Overall, we found that 38 Oracle database accounts for separated employees, interns, and contract workers, were not locked (disabled) and SAP Business Warehouse accounts were not terminated in a timely manner. District Oracle databases and SAP Business Warehouse accounts are not disabled automatically by the Identity Management System; accounts have to be disabled manually. Designated District staff are responsible for disabling accounts upon the receipt of an Identity Management System e-mail separation notification.

Disabling Oracle Database Accounts

An Information Technology Department Database Administrator is primarily responsible for disabling Oracle database accounts upon the separation of employees, interns, and contract workers. During the period July 1, 2009 to March 31, 2010, 28 employees and 49 interns and contract workers who separated from the District had Oracle database accounts. Based on a comparison of the date the e-mail separation notifications were generated to the date the Oracle database accounts were locked, we concluded that 52 (68%) instances where accounts were not locked until more than 100 days after the employee, intern, or contract worker separated from the District. The results of our review are detailed in the following table.

Number of Days Before Oracle Database Accounts Locked (*when compared to the Identity Management System e-mail separation notification*)	**Number (%) of Separated Workers**					
	Employees		**Contract Workers and Interns**		**Total**	
On the same day as the separation notification	8	*29%*	2	*4%*	10	*13%*
1-15 days after the separation notification	7	*25%*	4	*8%*	11	*14%*
16-100 days after separation notification	4	*14%*	0	*0%*	4	*5%*
101-200 days after separation notification	2	*7%*	13	*27%*	15	*20%*
201-300 days after separation notification	7	*25%*	28	*57%*	35	*45%*
Over 300 days after the separation notification	0	*0%*	2	*4%*	2	*3%*
Total	**28**	***100%***	**49**	***100%***	**77**	***100%***

It should be noted that all accounts were locked as a result of our audit.

<u>Disabling SAP Business Warehouse User Accounts</u>

The SAP Business Warehouse (BW) is the District's SAP reporting tool for all major SAP modules. As part of our audit, we determined whether separated employees' and contract workers' SAP Business Warehouse user accounts were terminated in a timely manner. Our examination disclosed that 21 separated employees' and contract workers' SAP Business Warehouse user accounts access were not terminated in a timely manner. The results of our review are illustrated in the following table.

SAP Business Warehouse User Accounts	**Number (%) of Separated Employees and Contract Workers**	
All user accounts disabled prior to, same day of, or the day after separation from the District	8	*38%*
User accounts disabled after the separation date; late separations ranged from 5 to 70 days after separation the District	10	*48%*
User accounts disabled after the separation date; however, late BW access termination was justified	3	*14%*
Total	**21**	***100%***

The SAP Solution Center's Security Team is responsible for terminating access. However, it appears that they were not on the list of staff/groups that receive the e-mail separation notification. The SAP Solution Center's Security Team became aware of some separations though conversations with District staff and other controls they have in place to ensure SAP is accessed only be authorized staff. During our audit, the Security Team was added to the notification list.

Wireless Devices Assigned to Separated Employees Not Terminated in a Timely Manner

Our audit disclosed that wireless devices were not terminated in a timely manner upon separation from the District. Further, in instances where the devices were reassigned to current employees, invoices were not updated in a timely manner to reflect the new users. Specifically, our review of the wireless invoices for the period July 2009 to February 2010, disclosed that a total of seven employees[1] who separated from the District were assigned wireless devices because their names appeared on the wireless invoices. Based on our review, we concluded the following:

- Four of the seven wireless devices remained active anywhere from 23 – 126 days after the employees separated from the District. It should be noted that in three instances the monthly costs were minimal. However, in the remaining instance the wireless device cost the District about $84.00 per month and remained active for 55 days after the employee separated from the District. These devices should have been terminated in a timely manner.
- Two of the seven devices were reassigned in a timely manner; however; the new users' names were not reflected on the wireless invoices. Instead, the wireless invoices reflected the names of the former employees for at least three to five months after they separated. The line assignments should have been updated in a timely manner to reflect the new users. Failure to update the billing information in a timely manner indicates inadequate controls.
- One of the seven devices remained active for over a month after the employee, a former senior staff, separated from the District. However, in this case the employee requested to use the District phone for a month after his separation and

[1] Two other employees were assigned wireless devices; however, we did not include them in our analyses because enough time had not passed since their separation in order for us to determine whether their devices were cancelled or re-assigned and whether relevant records were updated in a timely manner.

management authorized the use. Thus, we do not consider this instance an exception since it was known and specifically authorized by management and the cost to the District was minimal.

It should be noted that the Information Technology Department staff responsible for administering wireless devices is on the e-mail list of District staff who receive separation notifications. However, it appears that the staff did not act upon the receipt of the notification.

Retrieval of Personal Computer Equipment Should be Improved

As part of our audit, we analyzed desktop and laptop retrieval information for 29 separated employees and contract workers. Specifically, we compared the date equipment assigned to the separated employees and contract workers were retrieved by the Information Technology Department to the date that the Identity Management System generated a Remedy system retrieval ticket (date is the same as the Identity Management system separation date). Based on information provided by the Information Technology Department, we concluded the following:

Retrieval Information	**Number of Separated Employees / Contract Workers**
Retrieval not required; re-assigned to department staff. Re-assigned by the department within ***2 to 99*** working days	6
Retrieved ***within 5*** working days after the separation notification	10
Retrieved ***7 – 24*** working days after the separation notification. In these instances, no specific reasons were provided for the retrieval delay	8
Retrieved ***11 – 28*** working days after the separation notification partly because assignment was at local off-site locations (e.g., West Palm Beach Field Station and Skees Road)	4
Retrieved ***18*** working days after the separation notification based on the department's request	1
Total	**29**

Information Technology Department staff explained that all personal computers and monitors are locked to the desks, regardless of the assigned location. This ensures that the equipment will remain in place until the Information Technology Department unlocks it for retrieval. Further, there is no specific timeframe within which to retrieve desktops and laptops after a Remedy retrieval ticket is generated. Information Technology Department staff stated that they attempt to retrieve the equipment as quickly as possible; however, delays may occur due to various reasons. For example,

- The number of contract workers assigned to assist with the retrieval process has been reduced from five to three.
- Contract workers assigned with retrieval responsibilities may have other issues to resolve that take priority over retrievals, for example, assisting current users with computer issues.
- Local offsite retrievals (e.g., West Palm Beach Field Station) consistently take longer because coordinating the pickup generally needs to be scheduled due to security access and differences in working hours.

Employees and contract workers responsible for retrieving personal computers and laptops are required to document the steps in the retrieval process; however, this is not done in a consistent manner. Thus, we noted eight instances where there were no reasons documenting why the personal computers and laptops were not retrieved until 7 - 24 working days after the employee / contract worker separated from the District.

Disabling Security Access Should be Strengthened

As part of the separation process, we determined whether access to District facilities were deactivated (i.e., the date security badges were deactivated) in a timely manner. We requested that the Safety, Security & Emergency Management Department provide the dates that security access of the 45 employees within our audit scope was deactivated. We also selected a sample of 65 contract workers and requested the same information. Based on the deactivation dates for the 45 separated employees, which was obtained from the District's Photo Identification Card System (Picture Perfect software), we concluded the following:

Security Access Deactivated by District Physical Security	Number of Separated Employees
On the effective separation date (the day after the employee separated from the District)	29
5 -11 days after the separation notification	6
Deceased employee (274 days after the separation notification)	1
No record of employee in Security System	4
Incorrect de-activation date attributed to a software glitch	5
Total	**45**

The Safety, Security & Emergency Management Department provided de-activation dates for 27 of the 65 sample contract workers. Department staff stated that information was not available for all 65 sampled contract workers because they may have been assigned to offsite locations or badges were never issued. Our review of the 27 dates provided disclosed that the results were similar to those we found for the separated employees.

Department staff stated that the separated employees' and contract workers' department supervisors are responsible for collecting the actual badges upon separation. However, only about 25% of the badges are returned to the Safety, Security & Emergency Management Department. It is important that badges be returned upon separation since they can be used as a visual aide to access District facilities, for example, a person wearing a badge can enter main entrances without being questioned by security.

Process for Disabling RSA Tokens and SCADA Access Strengthened During Audit

Information Technology Security is responsible for manually disabling RSA VPN tokens and Supervisory Control and Data Acquisition (SCADA) systems access of separated employees and contract workers because access cannot be disabled automatically by Identity Management System.

An active District-issued RSA VPN token can be used to access District applications from a remote computer location if certain conditions are met, for example, if employee's or contract worker's user name and password to the District's Active

Directory are active. As a result, we wanted to determine whether RSA tokens issued to separated employees and contract workers are disabled in a timely manner. However, based on the information available we could only verify whether separated employees and contract workers were not on the list of current RSA token holders; we could not determine when the RSA tokens were disabled. We concluded that nine contract workers who separated from the District during the period July 1, 2009 to March 31, 2010 were on the list of active RSA tokens holders. This is not an issue as these contract workers left the District during the audit scope, but have since been re-contracted. However, it should be noted that once a workers Active Directory account is disable, they no longer have access to the District's network and therefore are unable to use the RSA tokens.

The SCADA system is the infrastructure that remotely operates the District's water control structures and provides operations and hydro-meteorological data. Based on data provided by Information Technology Security, access to the SCADA systems was enabled for an employee who separated from the District in November 2009. Information Technology Security staff explained that the employee's access was disabled after separation. However, it is possible that management re-activated his account to review the account activity and did not disable access after the review. Staff stressed that the active account did not pose a security risk because in order to access the SCADA system the employee would have to use a District computer at District facilities. This helps provide a compensating control.

As a result of our audit inquiries, Information Technology Security has developed scripts that will run on a weekly basis to ensure that separated employees and contract workers with VPN tokens and SCADA system access are disabled upon separation.

Educational Reimbursement not Recouped after Employee Separation

Based on District policies, all full-time employees are eligible for educational reimbursement. However, upon separation from the District an employee participating in the education reimbursement program is required to pay back the education reimbursements received within one year prior to separation.

Our review of data maintained in SAP HR disclosed that only 1 of the 45 separated employees in our audit scope received education reimbursement during the last year of employment with the District. Specifically, we noted that the employee separated from the District on August 7, 2009, and received two educational reimbursements during his last year with the District. He received an educational reimbursement of $1,190.58 on December 17, 2009, and this amount was repaid upon his separation in accordance with District policies. However, we also noted that he was reimbursed $1,135.26 on August 27, 2008; however, this amount was not paid as required by District policies. Human Resources Solutions stated that this was an oversight.

Discrepancy in Identity Management System Report of Disabled Users

In order to perform several audit tests, we requested a report from the Identity Management System of separated employees, interns, and contract workers whose accounts were disabled during the period July 1, 2009 to March 31, 2010. To validate the information on the report, we compared data on this report to e-mail separation notifications obtained from Information Technology Security and SAP HR reports of separated employees, interns, and contract workers obtained from Human Resources Solutions and the SAP Solution Center. We concluded that 39 of the separated employees, interns, and contract workers on the e-mail separation notification list and on the SAP HR lists were not on the Identity Management System list. We concluded that the 39 separated employees, interns, and contract workers were indeed disabled in Identity Management System. Information Technology Department staff provided the following explanation regarding this discrepancy:

> All of the 39 separations in questions experienced issues during the process of disabling the accounts preventing the automated process developed in IDM from completing the separation process. Consequently, these accounts were disabled in IDM manually after some period of time. It is evident that the standard Oracle IDM report of accounts disabled during a specified date range did not include these accounts in the report. While there were other accounts in addition to these 39 that were manually disabled during that time period, only these 39 were omitted from the

report. In five of the cases, the individual was converted from a contingent employee to an FTE, which would explain why they do not show up on the report (after the conversion the IDM account is once again active). Information Technology is investigating the reason for the remaining omissions; however, since the transactions logs from this time period are no longer available it will take some time and effort to research the problem and determine the root cause.

Recommendations

1. **Human Resources Solutions should establish a written procedure to initiate the separation process in SAP HR on the workers last day, or the day after a separation for voluntary employee and intern separation, and for contract worker separations that occur before their contract end dates.**

   Management Response: Management agrees with this recommendation. To strengthen the contract worker separation process moving forward, HR Solutions will run a BW report on a biweekly basis to identify any active contract workers with expired contract end dates in SAP to ensure that contract workers are off-boarded shortly after the contract end date has expired.

   Responsible Department: Departments, Project Managers, and Human Resources Solutions

   Estimated Completion: Completed

2. **Require that relevant department staff forward all separation paperwork to Human Resources Solutions on the employee's or intern's last day of work with the District. In addition, remind project managers who supervise contract workers to report service end date changes promptly to Human Resources Solutions.**

Management Response: Human Resources Solutions has capitalized on numerous opportunities to discuss the importance/criticality of this paperwork being submitted in a timely manner through various venues, quarterly department Human Resources representatives meeting, monthly Sr. HR representative meetings, MAT/MDT meetings (managers).

Responsible Department: Departments, Project Managers, and Human Resources Solutions

Estimated Completion: Ongoing

3. **Human Resources Solutions should separate contract workers in SAP HR promptly when contract workers leave the District on their contract end date.**

   Management Response: Management agrees with this recommendation. As confirmed with Information Technology, the contract worker is disabled in IDM at 12:01am the day after the last day of the contract. Therefore, even if they are not separated in SAP HR, there is no risk to the District regarding potential access to systems. In addition, to strengthen the contract worker separation process moving forward, Human Resources Solutions will run a BW report on a biweekly basis to identify any active contract workers with expired contract end dates in SAP to ensure that contract workers are off-boarded shortly after the contract end date has expired.

   Responsible Department: Departments, Information Technology Department, and Human Resources Solutions

   Estimated Completion: Completed

4. **Information Technology Department should ensure that separated employees', contract workers', and interns' District's Oracle database accounts are disabled upon receipt of the Identity Management System e-mail separation notification.**

Management Response: Management agrees with this recommendation. To ensure the Oracle Database accounts are disabled in a more timely fashion, we have added additional staff and the Section Leader to the automated email notification list. Additionally, when the enhancements to Identity Management system are completed, the Oracle Accounts will also be automatically disabled.

Responsible Department: Information Technology Department

Estimated Completion: Completed

5. **Information Technology Department should cancel wireless devices assigned to separated employees and contract workers upon receipt of the e-mail separation notification, unless otherwise instructed. In addition, ensure that wireless records are updated if the devices will be reassigned.**

   Management Response: Management agrees with this recommendation. Procedures for cancellation of wireless devices have been reviewed with appropriate staff and the Division Director and the Section Leader will review the status of this process periodically.

   Responsible Department: Information Technology Department

   Estimated Completion: Completed

6. **Consider establishing a timeframe guideline within which to retrieve computer equipment after a separation from the District. In addition, ensure that any retrieval delays are adequately documented.**

   Management Response: Management agrees with this recommendation. The written procedure for retrieval of equipment will be revised to establish a timeframe guideline for retrieval.

   Responsible Department: Information Technology Department

Estimated Completion: June 1, 2011

7. **Remind relevant department staff that security badges must be collected and deactivated upon separation from the District.**

   Management Response: Management agrees with this recommendation; however, it will not be necessary for Security to physically receive the badge due to electronic controls in place to deactivate the badge through our computer system. Recommend the employee's supervisor physically collect the employee badge and destroy it upon employee check out procedures.

   Responsible Department: Employee's Department/Security Office

   Estimated Completion: June 1, 2011

8. **Instruct Human Resources Solutions staff to carefully review educational reimbursements made to separating employee to ensure that reimbursements within the last year amounts are repaid to the District.**

   Management Response: Management agrees with this recommendation. A secondary review has been established for all separation/education reimbursement information going to Payroll.

   Responsible Department: Human Resources Solutions

   Estimated Completion: Completed

9. **Determine why all separated employees, interns, and contract workers are not reflected on the Identity Management System report of disabled users.**

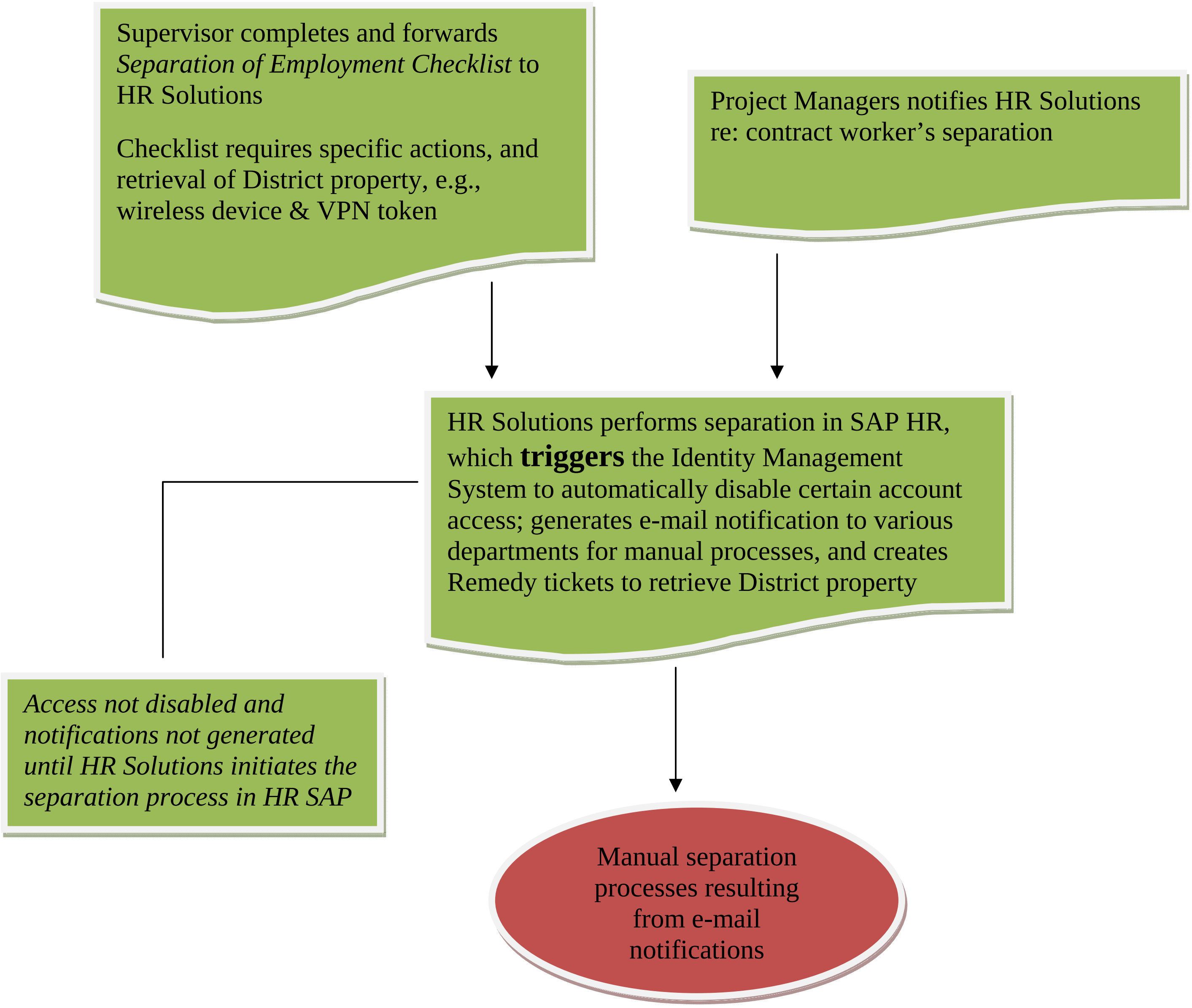
Management Response: Management agrees with this recommendation. Accounts that were manually disabled did not show up in the automated report. However, we are currently enhancing the Identity Management System and we will perform testing to ensure that the report reflects the accurate status of disabled accounts.

Responsible Department: Information Technology Department

Estimated Completion: December 31, 2011

APPENDIX A

Voluntary Separation by Employees/Interns and Separation of Contract Workers Prior to their Contract End Date



Supervisor completes and forwards *Separation of Employment Checklist* to HR Solutions

Checklist requires specific actions, and retrieval of District property, e.g., wireless device & VPN token

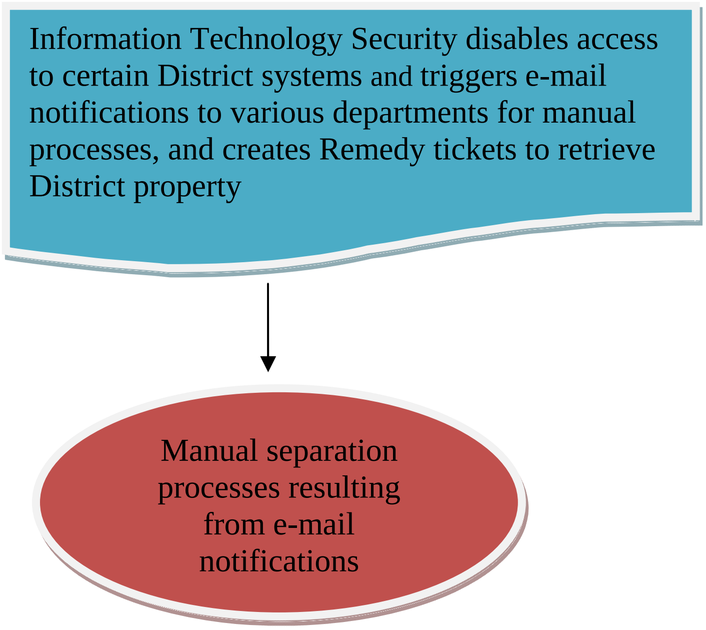
Project Managers notifies HR Solutions re: contract worker's separation

HR Solutions performs separation in SAP HR, which **triggers** the Identity Management System to automatically disable certain account access; generates e-mail notification to various departments for manual processes, and creates Remedy tickets to retrieve District property

Access not disabled and notifications not generated until HR Solutions initiates the separation process in HR SAP

Manual separation processes resulting from e-mail notifications

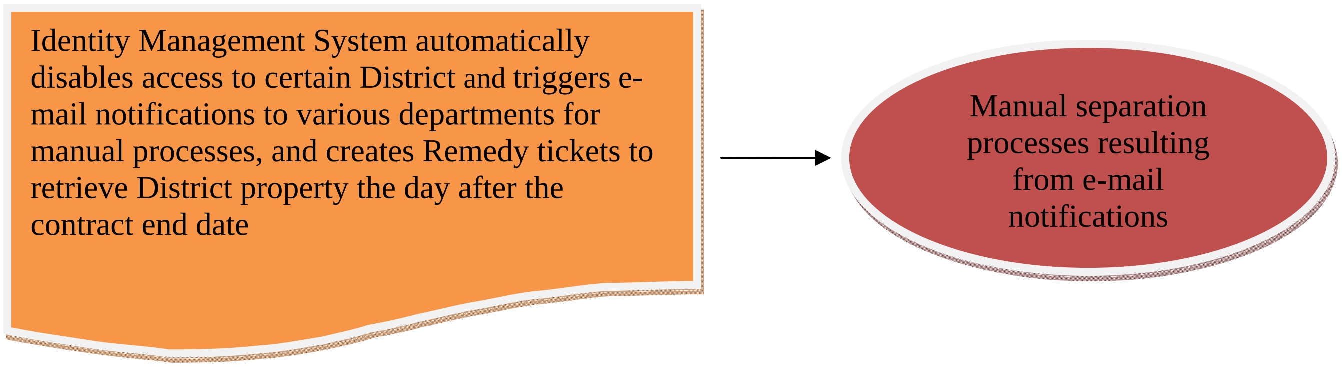
Involuntary Separation by Employees / Interns / Contract Workers



Information Technology Security disables access to certain District systems and triggers e-mail notifications to various departments for manual processes, and creates Remedy tickets to retrieve District property

Manual separation processes resulting from e-mail notifications

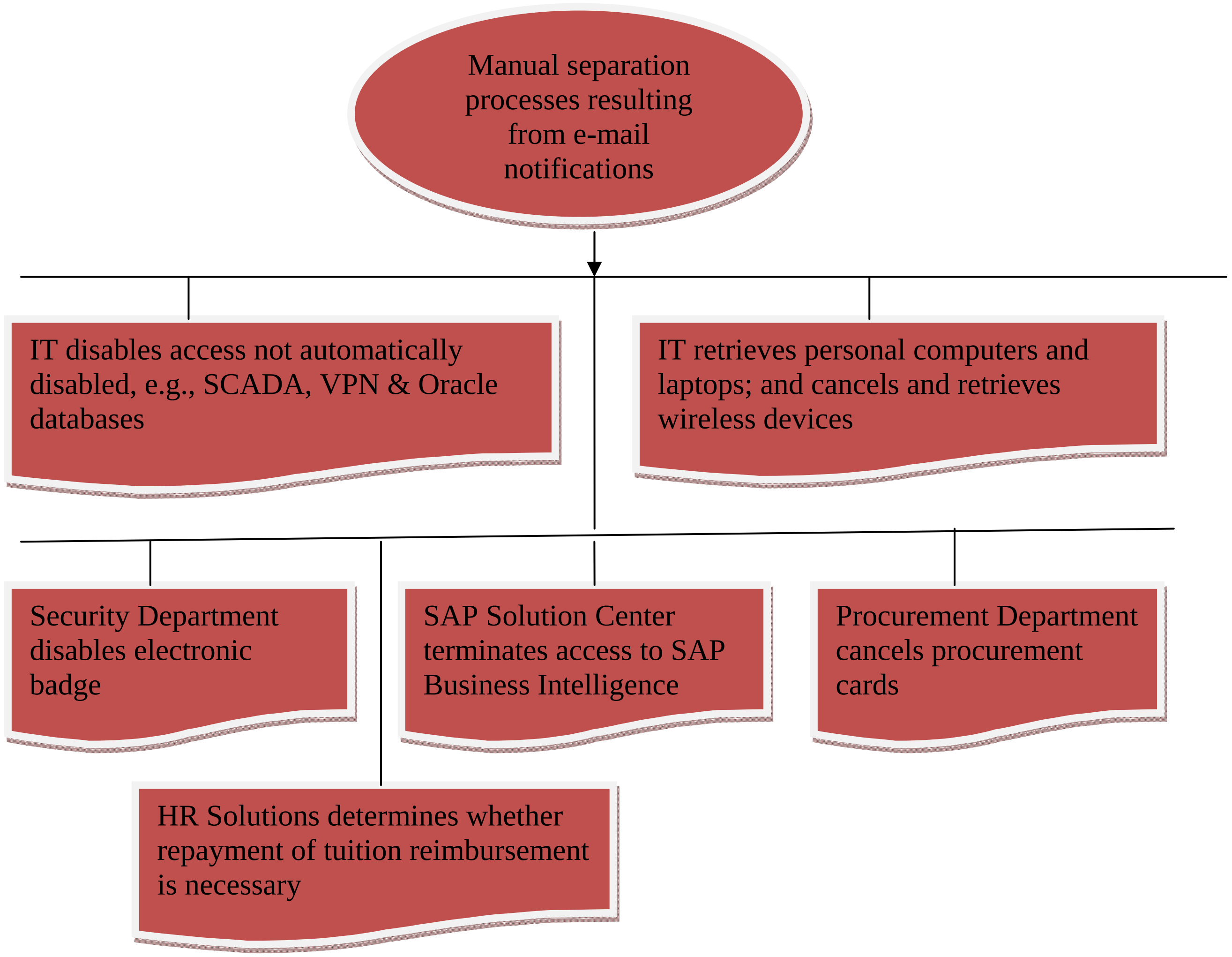
Separation by Contract Workers on Scheduled Contract End Date



Identity Management System automatically disables access to certain District and triggers e-mail notifications to various departments for manual processes, and creates Remedy tickets to retrieve District property the day after the contract end date

Manual separation processes resulting from e-mail notifications

Details of Manual Separation Processes Resulting from E-mail Notifications



Manual separation processes resulting from e-mail notifications

IT disables access not automatically disabled, e.g., SCADA, VPN & Oracle databases

IT retrieves personal computers and laptops; and cancels and retrieves wireless devices

Security Department disables electronic badge

SAP Solution Center terminates access to SAP Business Intelligence

Procurement Department cancels procurement cards

HR Solutions determines whether repayment of tuition reimbursement is necessary