Department of Education

Internal Audit

eHR Post-Implementation Review

Issue Date: July 2013

Report Number: 2013-03

REVIEW OF:	DATE:	REVIEW RATING:
eHR Post-Implementation	Fieldwork performed June 2013 – July 2013	Acceptable [**X**] Marginal [ ] Unacceptable [ ]

INTRODUCTION:

In connection with the Department of Education's (DOE) updated Risk Assessment & Audit Plan, Internal Audit (IA) performed an *"eHR Post-Implementation Review"* as was approved by the Board of Education (BOE) at the February 2013 meeting.

BACKGROUND:

In 2005, the Office of Human Resources (OHR) within the DOE awarded Business Solution Technologies, Inc. (BST) a portion of a contract to build a new human resources information system (HRIS) that would replace several aging legacy systems within the department. The project's name was titled, Collaborative Human Resources Automation Project (CHAP). CHAP was composed of three main areas:

- **PDE^3** – An employee professional development management system

- **eHR** – A HRIS that would support multiple functions within OHR

- **Roadmap** – An effort to build a culture of continuous improvement within OHR

The eHR system is more than just a HRIS, it also provides schools/offices with academic financial planning tools such as projected school lists, budget reports and direct access to buy/sell positions. eHR also helps to integrate and automate information previously contained in different manual forms, processes and electronic applications.

eHR is comprised of nine (9) main components:

1. **System Maintenance** – Component responsible for maintaining all setup/core tables that drive other components within eHR. Important tables within System Maintenance include, but are not limited to locations, school calendars, financial plan setup, security, countries, lookup codes, qualifications, qualification events, verbiages and salary schedules.

2. **Job Classes** – Component responsible for tracking specific classes of work within the DOE such as Teacher, Principal, Custodian, etc. Also allows users to track specific attributes such as qualifications and documents that may need to be stored such as job descriptions.

3. **Position Management** – Component responsible for tracking specific job classes at a given location. Also allows users to track specific attributes such as how it is being funded, which salary schedule is to be used, qualifications that any individual within that position must have and documents that may need to be stored.

4. **Employee Transactions** – Component responsible for tracking all persons within the DOE. Users of the system are able to use this component to track relevant information such as date of birth, social security number, phone numbers, email addresses, addresses, names, qualifications, qualification events, background checks and documents (such as *Notification of Personnel Action Forms* (Form 5)).

5. **Recruitment** – Component responsible for tracking the need to fill specific positions, allow applicants (both external and internal to the DOE) to apply online and for users to review and select applicants. This includes requests to fill, online applications and referral lists.

   There are a variety of recruitments processed through eHR:
   - Classified Support Services Personnel (CSSP) Recruitment (approx. 47 applications screened/day)
   - Teacher Recruitment (approx. 48 applications screened/day)
   - Educational Officer (EO) Recruitment (approx. 25-40 applications screened/month)

6. **Financial Planning** – Allows users to plan how they will use allocated funds for a specific location by school year. Users are able to attribute full-time equivalents (FTEs) to a specific budget program.

7. **Processes** – Allows users to define self-service processes by taking advantage of a custom built workflow engine and any of the components previously described. Examples of existing processes are the Online Application, Financial Planning, Projected School List and the Teacher Appointment and Transfer Program (TATP) process.

8. **Reports** – Allows users to run pre-defined reports to either MS Excel or Adobe PDF formats. Currently there are over one hundred thirty (130) reports that users can access.

9. **Highly Qualified Teacher Processing** – Allows users to enter, analyze and track teachers, their assignments and the "highly qualified" status of those assignments. The system allows for manual entry of qualification components (such as license, degree, praxis examinations and course credit information), but the generation of most "highly qualified" qualifications is an automated nightly processing. This nightly processing also determines whether a teacher is deemed "highly qualified" for the courses they are assigned to teach.

eHR went online in different phases and modules were implemented as noted below:
- November 2009 – Academic Financial Plan
- January 2010 – Projected School List
- March 2010 – TATP
- June 2010 – Position Management & Employee Transactions
- December 2010 –Teacher Recruitment application & Employee Background Checks
- September 2011 – CSSP Internal Recruitment application
- January 2012 – CSSP External Recruitment application
- July 2012 – EO Recruitment (state office/district) application
- Spring 2014 (Tentative Rollout) – EO Recruitment (schools) online application

Users of the eHR program include but are not limited to:
- Applicants (limited to their own application information only)
- OHR Employees
- State/District Office/Administrative Staff Management
- School Level Management
- Budget/Payroll Staff
- Production Support Team
- Consultants (subject matter experts that are contracted by the DOE for projects that utilize personnel data)

Policies and procedures are kept on the eHR website that provides the end users with "Quick Sheets" to guide them through the system. Through research and discussion with Management, IA identified two documents that eHR users must comply with, the "Network Support Services Acceptable User Guidelines-DOE Network and Internet Servers" for the network system and "Hawaii State DOE Acknowledgement of General Confidentiality Expectations" agreement that employees must sign annually.

There are only three (3) System Administrators in OHR that work in conjunction with BST in maintaining and updating the eHR system.

A high-level summary of eHR's flow of data is depicted below. The intent of this diagram is to show where eHR receives data from and where some of eHR's data gets distributed.
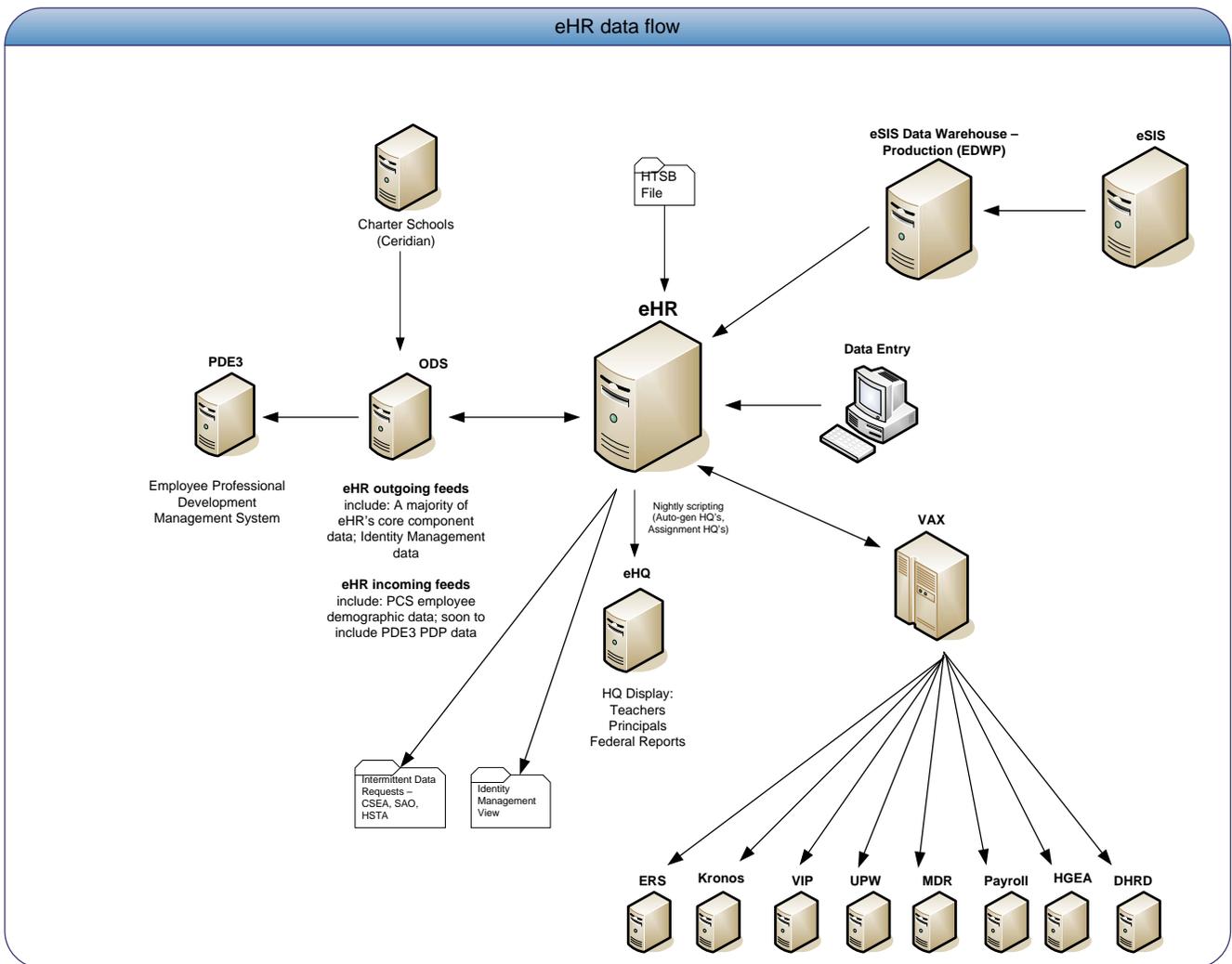
SCOPE and OBJECTIVES:

The scope of our review included an examination of the effectiveness of the eHR system. We reviewed the design and operating effectiveness of the existing control procedures over the input, processing and output processes to ensure that information captured is complete and accurate and information generated is accurate, reliable and timely. The scope of our review specifically focused on the processes related to the following subcategories:

1. Employee Transactions
2. Recruitment/Online Application Processing

The scope of the detailed testing covered the period July 1, 2012 through April 30, 2013. For employee transactions, data for the detailed testing was obtained from the eHR system and samples selected for testing were randomly selected for five (5) various days. For access controls, data for the detailed testing was obtained from the eHR system and 100% of all active (employees and consultants) users were tested.

The objectives of our review included the following:
1. To review, evaluate and test the design and operating effectiveness of procedures and controls over input, processing and output of the eHR system application processing module and employee transactions module.
2. To ensure that information captured is complete and accurate.
3. To ensure that information generated is accurate, reliable and timely.
4. To ensure that access controls are implemented in accordance with policies and procedures.
5. To ensure that access controls are properly monitored.

OBSERVATIONS:

Based upon our review, we found the DOE's controls related to the eHR system operations are functioning at an "acceptable" level. An acceptable rating indicates that no significant deficiencies exist, while improvement continues to be appropriate; controls are considered adequate and findings are not significant to the overall unit/department.

Please refer to the Risk Ratings section of this report for a complete definition of the ratings used by IA and the Observations and Recommendations section for a detailed description of our findings.

We discussed our preliminary findings and recommendations with management and they were receptive to our findings and agreed to consider our recommendations for implementation. In addition, we provided management with some leading practice recommendations that could help to improve efficiencies and strengthen processes.

Each observation presented in this report is followed by specific recommendations that will help to ensure that control gaps are addressed and, if enforced and monitored, will mitigate the control weaknesses. In summary, our audit observations are as follows:

1. System and control weaknesses identified in the eHR system.
2. Lack of proper monitoring over access controls.
3. Lack of policies and procedures for monitoring System Administrators' activity for eHR.

PLANNED FOLLOW UP BY MANAGEMENT AND INTERNAL AUDIT:

IA will follow up with management on their progress of completion for their action plans, and report accordingly through the audit committee quarterly updates.

Rating Scale Definitions

OVERALL RATING SCALE	
Acceptable	No significant deficiencies exist, while improvement continues to be appropriate; controls are considered adequate and findings are not significant to the overall unit/department.
Marginal	Potential for loss to the auditable unit/department and ultimately to the DOE. Indicates a number of observations, more serious in nature related to the control environment. Some improvement is needed to bring the unit to an acceptable status, but if weaknesses continue without attention, it could lead to further deterioration of the rating to an unacceptable status.
Unacceptable	Significant deficiencies exist which could lead to material financial loss to the auditable unit/department and potentially to the DOE. Corrective action should be a high priority of management and may require significant amounts of time and resources to implement.

OBSERVATION RATING SCALE	
High (1)	1 - The impact of the finding is <u>*material*</u>[1] and the likelihood of loss is probable in one of the following ways: ➢ A material misstatement of the DOE's financial statements could occur; ➢ The DOE's business objectives, processes, financial results or image could be materially impaired; ➢ The DOE may fail to comply with applicable laws, regulations or contractual agreements, which could result in fines, sanctions and/or liabilities that are material to the DOE's financial performance, operations or image. *Immediate action is recommended to mitigate the DOE's exposure*
Moderate (2)	2 - The impact of the finding is <u>*significant*</u>[1] and the likelihood of loss is possible in one of the following ways: ➢ A significant misstatement of the DOE's financial statements could occur; ➢ The DOE's business objectives, processes, financial performance or image could be notably impaired; ➢ The DOE may fail to comply with applicable laws, regulations or contractual agreements, which could result in fines, sanctions and/or liabilities that are significant to the DOE's financial performance, operations or image. *Corrective action by management should be prioritized and completed in a timely manner to mitigate any risk exposure.*
Low (3)	3 – The impact of the finding is moderate and the probability of an event resulting in loss is possible. *Action is recommended to limit further deterioration of controls.*

---

[1] The applications of these terms are consistent with the guidelines provided by the Institute of Internal Auditors.

Observations

The detailed observations noted herein were based on worked performed by IA through the last date of fieldwork and are generally focused on internal controls and enhancing the effectiveness of processes for future organizational benefit.

Obs. No.	Description	Page #
1	System and control weaknesses identified in the eHR system.	8-9
2	Lack of proper monitoring over access controls.	10-12
3	Lack of policies and procedures for monitoring System Administrators' activity for eHR.	13

Observation Number: 1	
Observation: System and control weaknesses identified in the eHR system	**Rating: Low**

During our interviews with management, testing performed on the eHR system and feedback from a survey conducted by IA, we noted the following system weaknesses:

1. **Edit routines are not embedded in all fields within the application program**
   Based on IA's testing of the online application module, we noted that eHR does not validate all data fields except those that are marked as required. We noted that in the Work Experience section it allows future dates to be entered as the start date and in the Middle Name and City fields the system allows numeric characters instead of only alpha. Per discussion with OHR-Records and Transaction Section's (RTS) supervisors, they do review and correct an applicant's data such as the name and SSN if the applicant is selected to be hired.

2. **System is slow, especially during busy times**
   Based on responses to the survey conducted by IA, half of the respondents suggested expanding the server capacity to increase the speed of the system, especially during busy times when the schools are doing their Academic Financial Plans.

During our interviews with RTS supervisors we noted the following control weakness in the design of the process:

1. **Records and Transactions clerks can edit their own personnel files in eHR**
   Based on our discussion with RTS supervisors, we noted that RTS clerks can edit their own records which includes pay rate. IA noted that transaction change(s) are documented on an employee's Form 5 and that the transaction change(s) cannot be deleted from the employee's record once the Form 5 is printed. For any changes to be made in employee benefits or payroll, the respective offices must receive a Form 5 from OHR to update an employee's record. IA noted that although clerks are able to change their own records, they do not have access to print a Form 5. Only the supervisors in RTS can print Form 5s and they review the forms along with supporting documents to ensure the transaction changes were proper before forwarding the Form 5s to Employee Benefits or the Payroll section for implementation.

Impact
The control weaknesses identified in the eHR system may lead to: ➢ Possible invalid/incorrect data collected from the applicants. ➢ Possible invalid/incorrect data change to an employee's personnel record.

Recommendation
Recommendations to correct the control weaknesses in the eHR system include: ➢ Management should embed more edit routines into fields in the eHR system for applications. ➢ IT management may also want to consider increasing the server capacity if funds are available. ➢ Management was already aware of the problem with RTS clerks being able to edit their own records and it is currently on their list of edits/changes to fix.

Observations

Management Plan
OHR will develop and implement a plan to determine how the embedding of edit routines into certain fields will affect the overall efficient functioning of eHR. Anticipated Completion Date: Development of Plan – December 2013 OHR has begun conversations with OITS in developing an implementation plan for adding additional server instances to the existing domain environment. Should additional funds and/or hardware resources become available, OHR in collaboration with OITS will execute the plan. Anticipated Completion Date: Implementation of Plan – January 2014 RTS has already requested a change in eHR to ensure that employees are not able to edit their own records to be implemented in eHR by end of the year. Currently, RTS conducts audits on staff edits and changes to ensure that employees are not updating their own records. Also, only supervisors have the ability to print a Form 5 that would authorize the Payroll section from processing any change in record. The Payroll section also audits the Form 5 prior to processing. Anticipated Completion Date: December 2013 Contact Person: Kerry Tom, Director, Personnel Management Branch Office of Information Technology Services (OITS) is working with the infrastructure staff and planning to add a second Application server to the server environment.   The Application server function is to process all user sessions, both the ones from external applicants and the ones from eHR staff, and it initiates data transactions as needed from the database servers. Currently there is a single Application server in front of the database servers and we anticipate that adding a second one will result in a significant improvement in performance under heavily loaded conditions. (Our analysis shows that the database servers are not heavily loaded and are not causing the performance issue.) Anticipated Completion Date: November 2013 Contact Person: Allan Stone, Director, Enterprise Systems
Responsible Office
OHR/OITS

Observation Number: 2

| **Observation: Lack of proper monitoring over access controls** | **Rating: Moderate** |

eHR is a part of the DOE's Single Sign On (SSO) system, which utilizes a user's lotus notes login to access multiple IT systems. Therefore, to obtain eHR access, an employee/consultant needs to first obtain a lotus notes account. eHR then sets up the employee's access level automatically based on their position (Principal, Secretary, CAS, etc.) and location. Most position roles are for school-level roles (Principal, Vice Principal, SASAs, etc.) and these roles do not have access to confidential information and are limited to the location of the user.

eHR has the ability to maintain security by user, role (user assigned to a role), processes (role assigned to a process), and row level (role confined to view/update specific types of data on specific screens). Once a user terminates employment with the DOE, their access is automatically expired in the eHR system. If a user moves positions or locations, their access needs to be manually changed by the System Administrators. For temporary users such as consultants and temporary assignments, System Administrators need to manually expire the user's access. However, IA did note that one control in the SSO system is that if the lotus notes user ID is expired, the access to eHR will also expire.

DOE employees & outside consultants who need to obtain "confidential" personnel information in eHR for their position/job must complete an "eHR Request Form" and a "DOE Confidentiality of Personnel Information Agreement." This completed form must be approved by their Administrator and sent to RTS, who decides whether or not to approve the access. If approved, the approved form is sent to the System Administrators to set up the user's access.

During our testing performed, we noted the follow findings and control weaknesses:

1. **"eHR Request Forms" were not completed properly and lacked important data fields**
   IA noted that although all forms tested had an approval signature on it, only one (1) of the thirty-five (35) forms tested had the box checked off as "approved" while the other forms did not have any box checked off. The forms also did not have fields for the "expiration date of the access" nor did it have a field for the "type of access." However, this information was noted in an empty space on the form by the RTS supervisor.

2. **Lack of monitoring over access controls**
   a. IA selected a sample size of 35 employees/consultants who had access to "confidential" personnel information in eHR to test for proper documentation. IA collected each users "eHR Request Form" and "DOE Confidentiality of Personnel Information Agreement" from RTS. IA noted the following exceptions:

Exception Noted:	**No. of Exceptions out of the Sample Size**	**% of Sample Size**
Forms were missing	1/35	2.9%
Form was not updated for new position in OHR	1/35	2.9%

Observations

b. IA tested 100% of all active eHR user accounts (users with read/write access) to test if the employee/consultant had proper access rights. IA noted the following exceptions:

Exception Noted:	No. of Exceptions out of the Sample Size	% of Sample Size
Employees with improper access rights[1]	19/1335	1.4%
Consultants with improper access rights[2]	6/1335	.45%

IA noted that per our discussion with RTS's supervisors, OITS would check with the offices that are working with the consultants to see if the consultants still needed access and if the office didn't respond, they would keep the consultant active.

IA also noted that on the discrepancy report tested, there were nine (9) users that had improper access rights. The System Administrators noted that they review these reports on a weekly basis but did not have any documentation that the discrepancies were followed up on.

Notes:
[1]Access rights were not removed from either the employee's previous position or temporary assignment. For 18 of the 19 employees, their access was limited by role and/or location. Only one (1) had access to statewide employee information.

[2]Access rights were not removed from consultants (from the same firm) no longer working on a DOE employee leave project that involved the utilization of personnel data. All six (6) consultants had access to statewide employee information.

Impact

The lack of proper monitoring over access controls may lead to:
> ➤ Possible unauthorized access to confidential information by employees or outsiders.
> ➤ Possible violation of confidentiality laws.

Recommendation

Recommendations for the lack of proper monitoring over access controls:
> ➤ RTS should consider updating the "eHR Request Form" to include a section to write the type of access given and the expiration date of the access.
> ➤ RTS should also enforce the proper completion of forms.
> ➤ Employees and consultants with access to confidential information in eHR should update their "eHR Request Forms" whenever they move positions or no longer need the access.
> ➤ Management has currently addressed the problem with consultants' temporary access by entering either the calendar year end or fiscal year end (whichever is closer) date as the expiration date for the vendor's access. OITS has also issued a policy as of March 2013 to check with the office working with the consultant every three (3) months to verify if the access is still needed. If no response is given after two weeks, then the consultant's access will be automatically removed.
> ➤ Management has currently addressed the problem with temporary assigned employee access by entering the fiscal year end date as the expiration date for access. The office working with the temporary assigned employee must contact the System Administrators if they still need access.

Observations

> ➢ Management may also want to consider tracking temporary assignments in the DOE to assist System Administrators with access rights.
> ➢ System Administrators should document discrepancy report follow ups to include information such as "date followed up" and "action taken/not taken."

Management Plan
RTS will implement an updated "eHR Request Form" to include the type of access given and the expiration date of the access. RTS has already taken steps to properly monitor the completion of the "eHR Request Form." RTS will also follow up with users, if need be, to ensure compliance. RTS along with eHR System Administrators will be finalizing "eHR System Access Guidelines" to ensure compliance with access provisions. The guidelines will ensure that proper system controls are in place to better track employee movements and overall eHR access. Currently, OHR provides access to consultants either to the end of the calendar year or to the end of the fiscal year, whichever is sooner, or an earlier date if access requested is for a shorter time period. Anticipated Completion Date:　　September 2013 OHR will develop and implement a solution to track security roles of employees who have been temporarily assigned to another position other than the one they were hired for. Anticipated Completion Date:　　Implement solution by January 2014. OHR will implement a solution to document edits made to user's roles and locations based off of system discrepancy reports. Recommended fields, "date followed up" and "action taken/not taken" will be included in the tracking document(s). Anticipated Completion Date:　　October 2013 Contact Person: Kerry Tom, Director, Personnel Management Branch
Responsible Offices
OHR

Observations

Observation Number: 3	
Observation: Lack of policies and procedures for monitoring System Administrators' activity for eHR	**Rating: Low**

During our interviews, IA noted that System Administrators do not have a policy or procedure regarding the monitoring of system administrator activity for eHR. It is important to have a policy that clearly explains a System Administrator's job responsibilities, regulations they have to follow, access rights and authorization privileges to the eHR system.

The System Administrators have procedures explaining how to perform certain tasks such as adding/editing a user's access. They also follow "eHR Bug Reporting Process Standards" that utilizes a program called "Bugzilla" to track complaints or problems with the eHR system. This program allows the users to report any bugs/problems they are having with eHR and it helps to track the status of these problems. This reporting process does have proper procedures in place for users to submit their complaints.

System Administrators also follow OITS change management procedures when performing major changes/edits to the eHR system, which includes meetings and testing on their parallel and test systems prior to being implemented in the main eHR system.

Impact

The lack of policies and procedures for monitoring System Administrators' activity may lead to:
  ➢ Possible unauthorized program changes to the eHR system.
  ➢ Possible unauthorized change/removal of data from the eHR system.

Recommendation

Recommendations for the lack of policies and procedures for monitoring System Administrators' activity include:
  ➢ OHR should create a policy for monitoring System Administrator activity that includes job responsibilities, regulations to be followed, access rights, as well as proper controls such as sign-offs and approvals for any changes or updates to the system or data in the system.

Management Plan

OHR will draft, develop, and enforce policies for monitoring the activity of System Administrators. The policies will cover all of the points stated in the Recommendation.

Anticipated Completion Date: Policies in effect by School Year 2014-2015

Contact Person: Kerry Tom, Director, Personnel Management Branch

Responsible Office
OHR

Acknowledgements

We wish to express our appreciation for the cooperation and assistance afforded to the review team by management and staff during the course of this review.