Human Resources-
Immigration Services

Audit Report # 18-108

September 17, 2018

The University of Texas at El Paso

Office of Auditing and Consulting

”Committed to Service, Independence and Quality”

The University of Texas at El Paso
Office of Auditing and Consulting Services

500 West University Ave
El Paso, Texas 79968
915-747-5191
WWW.UTEP.EDU

September 17, 2018

Dr. Diana Natalicio
President, The University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Natalicio:

The Office of Auditing and Consulting Services has completed a limited scope audit of the Human Resources Department- Immigration Services. During the audit, we identified opportunities for improvement and offered the corresponding recommendations in the audit report. The recommendations are intended to assist the department in strengthening controls and help ensure that the University's mission, goals and objectives are achieved.

We appreciate the cooperation and assistance provided by Human Resources staff during our audit.

Sincerely,

Lori Wertz

Lori Wertz
Chief Audit Executive

Report Distribution:

University of Texas at El Paso:

Mr. Richard Adauto III, Executive Vice President

Mr. Mark McGurk, Vice President for Business Affairs

Dr. Victor Pacheco, Interim Associate Vice President for Human Resources

Ms. Arizvé Ochoa-Retana, Associate Director Human Resources

Ms. Sandra Vasquez, Assistant Vice President for Equal Opportunity (EO) and Compliance

University of Texas System (UT System):

System Audit Office

External:

Governor's Office of Budget, Planning and Policy

Legislative Budget Board

Internal Audit Coordinator, State Auditor's Office

Sunset Advisory Commission

Audit Committee Members:

Mr. David Lindau

Mr. Fernando Ortega

Dr. Carol Parker

Mr. Benjamin Gonzalez

Dr. Gary Edens

Dr. Roberto Osegueda

Dr. Stephen Riter

Auditors Assigned to the Audit:

Cecilia Estrada

Christy Marquez

Victoria Morrison

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Office of Auditing and Consulting Services has completed a limited scope audit of the Human Resources Department with a focus on Immigration Services. The objectives of the audit were to assess the efficiency of operations, verify compliance with employment eligibility regulations for new and current employees, and to ensure that the immigration data at rest or in transit is secured and in compliance with State and University Security Controls.

During the audit we noted the following:

- The visa information section in PeopleSoft does not accurately reflect the employees' current visa status.
- Nine H1-B visa holders' public access files (PAF) were tested with the following results:
  - Three files did not contain an employee benefits memo
  - Internal auditors found instances where H1-B files tested did not contain information on the dates and locations of the Labor Conditions Application (LCA) notice posting. However, this information was provided before the end of the audit.
- Two of nine TN visa holders tested did not contain current Form I-94 records on file. During the course of fieldwork, HR contacted the employees and a current form is now on file.
- Auditors tested Form I-9 Employment Eligibility Verification records for 32 employees which resulted in eight employees not in compliance:
  - Employment eligibility was not verified timely for four employees.
  - A valid Form I-9 was not on file for four different employees.

BACKGROUND

The University of Texas at El Paso employs individuals from diverse national backgrounds to better serve the student population. UTEP's Human Resources Department Immigration Services (HR) is dedicated to assist faculty and staff interested in obtaining different types of visas, to include:

- **H1-B Specialty Occupations**: An employer sponsored and position-specific visa which requires the applicant to have completed, at minimum, a bachelor's degree and meet all job qualifications imposed by the employer. The H1-B visa is initially valid for three years, and can be extended one time for up to a combined total of six years.

- **TN North American Free Trade Agreement (NAFTA) Nonimmigrant Professional**: The TN visa allows citizens of Canada or Mexico, as temporary NAFTA professionals, to work in the United States (U.S.). The TN visa may be sponsored by an employer or be self-sponsored. The initial visa period can last up to three years, with ability to reapply for an extension in three year increments.

- **Lawful Permanent Residence (LPR):** Permanent residency authorizes a foreign national to live and work in the U.S. indefinitely. UTEP sponsors only selected employment based permanent residency visa petitions. Standard application processing time is a minimum of two years, and HR recommends to initiate the process prior to the 4th year of H1-B status to avoid interruptions in employees' work eligibility.

- **O-1 Individuals with Extraordinary Ability or Achievement**: A U.S. employer sponsored visa that must meet the criteria of a date specific contract, written or oral, and a written consultation/advisory from a peer group in the area of specific and extraordinary ability. Initial period of stay may extend up to three years, with unlimited one year extensions as long as visa holder continues in the same position or activity for which the O-1 was granted.

The department collaborates with immigration attorneys throughout the application process for the types of visas listed. In addition, HR is responsible for verifying and monitoring the status of employees' work eligibility to ensure compliance with federal requirements.

AUDIT OBJECTIVES

The objectives of this audit were to:

- assess the efficiency of HR-Immigration Services' operations,
- verify compliance with employment eligibility regulations for new and current employees, and
- ensure that the immigration data at rest or in transit is secured and in compliance with State and University Security Controls.

SCOPE AND METHODOLOGY

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and the authoritative guidelines of the *International Professional Practice Framework* issued by the Institute of Internal Auditors.

The audit criteria includes Title 8: Aliens and Nationality of the Code of Federal Regulations (8 CFR), United States Citizenship and Immigrations Services (USCIS) guidelines, UTEP's Business Process Guidelines- Hiring Foreign Nationals, and UTEP's Information Security Policies and Standards.

The scope of the audit included a random sample of 32 employee records tested for compliance with Form I-9, and 23 employee records related to H1-B, J1, TN, and O1 visas tested for compliance with the appropriate federal regulations. The time period for the audit was June 2016 through February 2018.

Audit procedures included interviewing key personnel, reviewing applicable regulations, verifying the existence of appropriate institutional policies and procedures through inspection of supporting documentation, and verifying security controls of HR's information systems containing confidential data.

RANKING CRITERIA

All findings in this report are ranked based on an assessment of applicable qualitative, operational control and quantitative risk factors, as well as the probability of a negative outcome occurring if the risk is not adequately mitigated. The criteria for the rankings are as follows:

Priority - an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.

High – A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level.

Medium – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level.

Low – A finding identified by internal audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level.

AUDIT RESULTS

A. PeopleSoft Records

Visa expiration monitoring is part of HR's internal process to ensure the University stays in compliance with federal immigration employment regulations. HR uses information from PeopleSoft to track visa expiration dates and sends out reminder notifications to employees. The reminders are sent six months prior to expiration in order to process updated information or renew visa status.

Employee records in PeopleSoft are not maintained by HR; the information is entered and updated by the Electronic Data Management office. However, HR is responsible for validating the accuracy of records.

Auditors requested a list of current employees with an active visa. The information was analyzed to corroborate that the complete population of employees was identified by HR and consequently monitored. The following issue was noted:

A.1. Inaccurate Visa Information

Internal Audit accessed electronic records from PeopleSoft and physical records from HR. Auditors found data entry and validation errors in PeopleSoft, which causes inaccurate employee records and incorrect reporting. Without accurate information, manual adjustments to the reports downloaded from PeopleSoft are necessary to obtain a correct list of employees with a visa. HR's ability to monitor visa employees could be limited, creating a risk for noncompliance with federal immigration regulations.

Recommendation:

HR should have the ability to update employee visa records in PeopleSoft. In addition, a review of the current information should be conducted to ensure records are correct and up to date.

Level: This finding is considered **Medium** due to the fact that inaccurate records produce inaccurate reports to be utilized for time sensitive information, which in turn may cause the University to not be in compliance with federal immigration regulations.

Management Response:

We concur with the recommendation that HR should be given the ability to update employee visa records in PeopleSoft. HR will work with the Electronic Data Management unit to establish new data entry procedures for visa information. HR will also establish procedures to review that information is correct and up-to-date.

Responsible Party:

Arizve Ochoa-Retana

Implementation Date:

October 31, 2018

B. Visa Documentation (H1-B and TN)

HR assists faculty and staff in obtaining various nonimmigrant visas for employment at the University. Each type of visa requires specific conditions to be met and documentation that must be maintained by its employer as per federal regulations. The list of active employees with a visa provided by HR contained 655 records. Internal auditors tested a sample of 23 H1-B, TN, O1, and J1 visas for compliance to federal regulations and internal policies and procedures. In the case of the one O1 and four J1 visas tested, no exceptions were found. On the other hand, the following three exceptions were noted in the H1-B and TN visa samples:

B.1. Benefit Memo Not on File

Internal auditors tested a sample of nine out of 46, or 20 percent, of H1-B visa holders. Three out of nine, or 30 percent, of H1-B files tested did not contain a benefits memo. The benefits memo requirement is fulfilled through the Actual Wage Memo which states that H1B workers will be offered benefits on the same basis, and in accordance with, the same criteria as is offered to US workers.

Per the CFR Title 20 §655.760 (a)(6), "*a summary of the benefits offered to U.S. workers in the same occupational classifications as H-1B nonimmigrants*" must be included in the employee's Public Access File (PAF) (See Appendix A: H1-B Visa Criteria). Failure to follow federal regulations can lead to fines, civil and/or criminal penalties.

Recommendation:

HR should make it a practice to regularly review and update all public access files to ensure that all information is complete and up to date. A summary of benefits provided to U.S. citizens and nonimmigrant workers should be separately placed in the H1-B PAF as supporting documentation.

Level: This finding is considered **MEDIUM** due to the fact that noncompliance with federal immigration regulations may lead to civil and/or criminal penalties or the possible loss of visa sponsorship to the University.

Management Response:

We disagree with this finding. We have previously provided a written legal opinion from our immigration attorneys supporting our position that HR is currently in compliance with the regulations.

B.2. Lack of Dates in LCA Notice Posting

Internal auditors found instances where H1-B files tested did not contain information on the dates and locations of the Labor Conditions Application (LCA) notice posting. However, this information was provided before the end of the audit.

CFR Title 20 §655.734 sets requirements for the LCA notice including occupational classification, wages offered, period and location of employment, public access availability, and a statement of complaints procedure. Per CFR Title 20 §655.734 (b) "*the employer shall develop and maintain documentation sufficient to meet its burden of proving the validity of the statement referenced in paragraph (a) of this section and attested to on Form ETA 9035 or 9035E… the employer shall note and retain the dates when, and locations where, the notice was posted and shall retain a copy of the posted notice.*" (See Appendix A: H1-B Visa Criteria). Failure to follow federal regulations can lead to fines, civil and/or criminal penalties.

B.3. Current Form I-94 Not on File for TN Visa Holders

TN visa holders must have a valid passport and an unexpired Form I-94 to maintain work eligibility as required by 8 CFR §Sec 214.6.

Two of nine TN visa holders' files tested, or 22 percent, did not contain a current Form I-94 Arrival/Departure Record. One of the two had an expiration date of 02/06/18 on May

29, 2018, the testing date. The Form I-94 for the other employee was not found. Failure to follow federal regulations can lead to fines, civil and/or criminal penalties.

During the course of fieldwork, HR contacted the employees with the missing/expired I-94 and a current form is now on file. Both employees are in compliance as of July 2018.

C. Form I-9 Employment Eligibility Verification

According to U.S. Citizenship and Immigration Services (USCIS), employers are required to only hire individuals who may legally work in the United States: U.S. citizens, noncitizen nationals, LPRs, and aliens authorized to work. To comply with the law, employers must verify the identity and employment authorization of every person they hire, and complete and retain a Form I-9, Employment Eligibility Verification, for each employee.

C.1. Late Submission of Form I-9

Human Resources prepares a Late I-9 Tracking Report. On a quarterly basis, HR notifies College Administrative Officers (CAO) if new hires from their college did not complete the employee portion of Form I-9 on or before the first day of employment.

During testing, auditors noted that employment eligibility was not verified timely via the mandatory Form I-9 for four different employees. Although the employees had legitimate F1, F3, and J1 visas and were eligible to work, the employees worked at the University before this was confirmed; a violation of 8 CFR §274. Failure to follow federal regulations can lead to fines, civil and/or criminal penalties.

Recommendation:

HR should work with colleges and departments around campus to ensure employment eligibility is verified timely through Form I-9 and in accordance with USCIS regulations.

Level: This finding considered **Medium**, due to the risk of non-compliance which could lead to federal fines, civil and/or criminal penalties.

Management Response:

The lateness of I-9s results from departments hiring individuals prior to employment eligibility being verified by Human Resources. Human Resources will continue to utilize an I-9 tracking spreadsheet implemented in February 2017 to identify late I-9 submissions and notify departmental staff and administrators needing training in this area. In addition, Human Resources will continue to communicate, instruct, and guide administrators, staff, and employees through orientation training, to include increasing the number of onboarding/pre-employment training sessions available on a campus-wide basis. This training will include I-9 pre-hiring requirements.

Responsible Party:

Arizve Ochoa-Retana

Implementation Date:

October 1, 2018

C.2. Form I-9 Not On File

There was no support of employment eligibility via the mandatory Form I-9 on file for one non-visa employee, two J1 visa employees, and one F1 visa employee. Failure to follow federal regulations can lead to fines, civil and/or criminal penalties.

During the course of audit fieldwork, HR contacted these employees to obtain the necessary documents to be in compliance.

Information Technology

D. Confidential Data (Immigration) At Rest or In-Transit

Internal Audit tested immigration data at rest and in transit. Data "*at rest*" is data stored in a digital device and data "*in-transit*" is data moving through the UTEP's network and the internet. The criteria used is found in APPENDIX B: Information Technology Criteria

D.1. Departmental Network Share Drives

The Internal Auditor tested the intended access and actual access to the network share drive where immigration data "*at rest"* is stored. The Immigration Services folder is restricted to authorized users, and users having the correct permission level. A daily backup is taken of the fileserver where network shares reside, and the backup tapes are taken offsite to a secured site. Internal Audit reviewed the backup logs.

No exceptions noted.

D.2. Transmission of Confidential Data

The immigration data, "*in-transit*", is transmitted over a secured and encrypted connection. The Human Resources department is aware that the access to the vendor's website needs to be removed when an employee leaves the HR department.

No exceptions noted.

CONCLUSION

Based on the results of audit procedures performed, we conclude that the processes and data security controls at the Human Resources Department- Immigration Services are generally effective. We did, however, identify opportunities for improvement in the area of compliance with federal immigration regulations.

In responding to the recommendation made in *B.1 Benefit Memo Not on File*, we did review the legal opinion provided. However, as previously stated, the criteria for our testwork was CFR Title 20 §655.760 (a)(6), "a summary of the benefits offered to U.S. workers in the same occupational classifications as H-1B nonimmigrants" must be included in the employee's Public Access File (PAF) (See Appendix A: H1-B Visa Criteria). As the results of our audits must be based on applicable rules, regulations, policies or procedures, we stand by our recommendation.

We wish to thank the management and staff of the Human Resources Department for their assistance and cooperation provided throughout the audit.

APPENDIX A: H1-B VISA CRITERIA

Benefits Memo not on File Criteria

20 CFR 655.760 What records are to be made available to the public, and what records are to be retained? (a) Public Examination. (6) *A summary of the benefits offered to U.S. workers in the same occupational classifications as H-1B nonimmigrants,* a statement as to how any differentiation in benefits is made where not all employees are offered or receive the same benefits (such summary need not include proprietary information such as the costs of the benefits to the employer, or the details of stock options or incentive distributions), and/or, where applicable, a statement that some/all H-1B nonimmigrants are receiving "home country" benefits (see § 655.731(c)(3));

Labor Conditions Application Notice Posting Criteria

20 CFR 655.734 - What is the fourth LCA requirement, regarding notice? An employer seeking to employ H-1B nonimmigrants shall state on Form ETA 9035 or 9035E that the employer has provided notice of the filing of the labor condition application to the bargaining representative of the employer's employees in the occupational classification in which the H-1B nonimmigrants will be employed or are intended to be employed in the area of intended employment, or, if there is no such bargaining representative, has posted notice of filing in conspicuous locations in the employer's establishment(s) in the area of intended employment, in the manner described in this section.

(b)Documentation of the fourth labor condition statement. The employer shall develop and maintain documentation sufficient to meet its burden of proving the validity of the statement referenced in paragraph (a) of this section and attested to on Form ETA 9035 or 9035E. Such documentation shall include a copy of the dated notice and the name and address of the collective bargaining representative to whom the notice was provided. Where there is no collective bargaining *representative, the employer shall note and retain the dates when, and locations where, the notice was posted and shall retain a copy of the posted notice.*

APPENDIX B: INFORMATION TECHNOLOGY CRITERIA

STATE:

Texas Administration Code Title 1, Part 10, Chapter 202, Subchapter C,

RULE §202.76 Security Control Standards Catalog

Texas Department of Information Resource ***Security Control Standards Catalog Version 1.3***

AC–Access Control

AU–Audit and Accountability

IA–Identification and Authentication

MA–Maintenance

SC-8: Transmission Confidentiality and Integrity

RULE §202.72 Staff Responsibilities

Information owners, custodians, and users of information resources shall, in consultation with the institution IRM and ISO, be identified, and their responsibilities defined and documented by the state institution of higher education. The following distinctions among owner, custodian, and user responsibilities should guide determination of these roles:

(1) Information Owner Responsibilities. The owner or his or her designated representative(s) are responsible for:

(A) classifying information under their authority, with the concurrence of the state institution of higher education head or his or her designated representative(s), in accordance with institution of higher education's established information classification categories;

(B) approving access to information resources and periodically review access lists based

on documented risk management decisions;

(C) formally assigning custody of information or an information resource;

(D) coordinating data security control requirements with the ISO;

(E) conveying data security control requirements to custodians;

(F) providing authority to custodians to implement security controls and procedures;

(G) justifying, documenting, and being accountable for exceptions to security controls. The information owner shall coordinate and obtain approval for exceptions to security

controls with the institution of higher education information security officer; and

(H) participating in risk assessments as provided under §202.75 of this chapter.

(2) Information Custodian Responsibilities. Custodians of information resources, including third party entities providing outsourced information resources services to state institutions of higher education shall:

(A) implement controls required to protect information and information resources

required by this chapter based on the classification and risks specified by the information

Texas Administrative Code Page 1 of 2
http://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_... 5/1/2018
owner(s) or as specified by the policies, procedures, and standards defined by the

institution of higher education information security program;

(B) provide owners with information to evaluate the cost-effectiveness of controls and monitoring;

(C) adhere to monitoring techniques and procedures, approved by the ISO, for detecting, reporting, and investigating incidents;

(D) provide information necessary to provide appropriate information security training to employees; and

(E) ensure information is recoverable in accordance with risk management decisions.

(3) User Responsibilities. The user of an information resource has the responsibility to:

(A) use the resource only for the purpose specified by the institution or information owner;

(B) comply with information security controls and institutional policies to prevent unauthorized or accidental disclosure, modification, or destruction; and

(C) formally acknowledge that they will comply with the security policies and procedures in a method determined by the institution head or his or her designated representative.

(4) Institution information resources designated for use by the public shall be configured to enforce security policies and procedures without requiring user participation or intervention. Information resources must require the acceptance of a banner or notice prior to use.

***Source Note:** The provisions of this §202.72 adopted to be effective March 17, 2015, 40*

UTEP Information Security Policies

UTEP Standard 1: Information Resources Security Responsibilities and Accountability >

...

"1.7 (n) specify and require use of appropriate security software such as anti malware, firewall, configuration management, and other security related software on Computing Devices owned, leased, or under the custody of any department, operating unit, employee, or other individual providing services to the Institution; "

...

1.9 Information Resources Owners

1.9 Information Resources Owners. For Information Resources and Data under their authority, Owners shall:

(a) grant access to Information Systems and Data;

(b) control and monitor access to data based on data sensitivity and risk;

(c) classify data based on the Institution's Data Classification Standard;

(d) conduct risk assessments that identify the Information Resources under their authority and the level of risk associated with the Information Resources and the vulnerabilities, if any, to the Institution's information security environment;

(e) define, recommend, and document acceptable risk levels for Information Resources and risk mitigation strategies;

(f) document and justify, in collaboration with the ISO, any exceptions to specific program requirements due to extenuating circumstances within the Owner's area of responsibility;

(g) ensure data is securely backed up in accordance with risk management decisions;

(h) ensure data is maintained in accordance with the applicable University records retention schedule and procedures;

(i) provide documented permission and justification for any User who is to store Confidential University Data on a Portable Computing Device or a Non-University Owned Computing Device;

(j) ensure that High Risk Computing Devices and Confidential Data are encrypted in accordance with requirements specified in UTS165 Standard 11 - Safeguarding Data;

UTEP Standard 4: Access Management

UTEP Standard 5: Administrative/Special Access Accounts

UTEP Standard 8: Malware Prevention

...

8.1 UTEP Network Infrastructure and other Information Resources must be continuously protected from threats posed by Malware.

(a) Virus protection software must not be disabled or bypassed;

(b) Settings on the virus protection software must not be altered in a manner that will reduce the effectiveness of the software;

(c) Automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates;

(d) Email gateways must utilize properly maintained email virus protection software that is UTEP-approved;

(e) Any server attached to UTEP Information Resources must utilize UTEP-approved virus protection software and must be set up to detect and clean viruses that may infect the server or files shares; and

(f) Any system identified as a security risk due to lack of virus protection may be disconnected from the network or the respective network account may be disabled until adequate protection is in place.

8.2 All computing devices owned, leased, or under the control of UTEP must, to the extent technology permits, execute and keep up to date all required protection software and adhere to any other protective measures as required by applicable Policies and Procedures;

8.3 Any personally owned Computing Device that contains Confidential University Data must be configured to comply with required University security controls while holding such Data;

8.4 Any system identified as a security risk due to a lack of virus protection may be disconnected from the network or the respective network account may be disabled until adequate protection is in place;

8.5 Submit exceptions to the UTEP CISO for approval by completing a Security Exception Request Form. ...

UTEP Standard 9: Data Classification

UTEP Standard 11: Safeguarding Data

11.5 Protecting Data in Transit. Data Owners shall implement appropriate administrative, physical, and technical safeguards to adequately protect the security of Data during transport, including electronic transmission. The following shall all be addressed:

(a) Identification and Transmission of the least amount of Confidential Data required to achieve the intended business objective;

(b) All Confidential Data transmitted over the Internet must be appropriately encrypted;

(c) Confidential Data transmitted between Institutions and Shared Data Centers must be appropriately encrypted;

(d) Confidential Data transmitted or received must be deleted upon completion of the intended business objective unless otherwise subject to records retention, in which case it must be encrypted or password protected.

UTEP Standard 14: Information Services (IS) Privacy

UTEP Standard 19: Server and Device Configuration and Management.

19.2 Server Hardening. To protect against malicious attack, all Servers and Devices on UTEP networks will be security hardened based on Risk and must be administered according to UTEP Policies, Standards, Guidelines, and Procedures prescribed by UTEP and U.T. System, as applicable, and incorporates the following procedures: (a) identify and assign appropriately trained administrators for all Mission Critical Devices, or Servers supporting Information Systems containing Confidential Data;

(b) Minimum Security Standards for Systems as well as other UTEP Guidelines provide the detailed information required to harden a Server or computing Device and must be implemented for UTEP Information Security Office (ISO) accreditation; and

(c) manage the test and installation of service packs, hot fixes, and security patches for equipment under their responsibility.

UT SYSTEM

UTS165 Standard 1: Information Resources Security Responsibilities and Accountability

UTS165 Standard 4: Access Management

UTS165 Standard 5: Administrative/Special Access Accounts

UTS165 Standard 8: Malware Prevention

UTS165 Standard 9: Data Classification

UTS165 Standard 11: Safeguarding Data

UTS165 Standard 14: Information Services (IS) Privacy

UTS165 Standard 19: Server and Device Configuration and Management.