IDENTITY MANAGEMENT AND COMMON SYSTEM ACCESS

SYSTEMWIDE

Audit Report 12-44
June 11, 2013

Members, Committee on Audit

Lupe C. Garcia, Chair
Rebecca D. Eisen  Steven M. Glazer
William Hauck  Hugo N. Morales

Staff

University Auditor: Larry Mandel
Senior Director: Michael Caldera
IT Audit Manager: Greg Dove
Senior Auditor: Gordon Eng

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
CONTENTS

Executive Summary ...................................................................................................................................... 1

Introduction ................................................................................................................................................... 2
  Background ............................................................................................................................................... 2
  Purpose ...................................................................................................................................................... 4
  Scope and Methodology ........................................................................................................................... 6

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Governance ................................................................................................................................................... 7

Student Identity Validation ........................................................................................................................... 8

Deprovisioning Application Access ........................................................................................................... 8
APPENDICES

APPENDIX A: Personnel Contacted
APPENDIX B: Management Response
APPENDIX C: Chancellor’s Acceptance

ABBREVIATIONS

CIO       Chief Information Officer
CO        Chancellor’s Office
CSU       California State University
ICSUAM    Integrated California State University Administrative Manual
I&IT      Instructional and Information Technology
IAM       Identity Access Management
OUA       Office of the University Auditor
EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of the University Auditor (OUA) during the last quarter of 2011, the Board of Trustees, at its January 2012 meeting, directed that Identity Management and Common System Access be reviewed. The OUA had previously reviewed some aspects of identity management and common system access in the 2008 and 2009 audits of Information Security and in the 2011 audits of Sensitive Data Security and Protection.

We visited five campuses from June 25, 2012, through December 13, 2012, and audited the procedures in effect at that time. Campus-specific findings and recommendations have been discussed and reported individually.

In our opinion, the fiscal, operational, and administrative controls for identity management and common system access as of December 13, 2012, taken as a whole, were sufficient to meet the objectives stated above and in the “Purpose” section of this report.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls changes over time. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to, resource constraints, faulty judgments, unintentional errors, circumvention by collusion, and management overrides. Establishing controls that would prevent all these limitations would not be cost-effective; moreover, an audit may not always detect these limitations.

Our audit of identity management and common system access did not examine controls over all common system authentication techniques, but was designed to assess management control and oversight, consistency of controls on a sample basis, and compliance with California State University guidance.

The following summary provides management with an overview of conditions requiring attention. Areas of review not mentioned in this section were found to be satisfactory. Numbers in brackets [ ] refer to page numbers in the report.

GOVERNANCE [7]

Campuses had not developed written policies and procedures for overall governance and definition of roles and responsibilities in operating, using, and monitoring the identity access management (IAM) system.

STUDENT IDENTITY VALIDATION [8]

The campus IAM systems did not require identity validation for all registered students.

DEPROVISIONING APPLICATION ACCESS [8]

Campus did not have an adequate process to ensure that changes in access privileges were performed consistently and in a timely manner, or to ensure that privileges within the application systems had been removed.
INTRODUCTION

BACKGROUND

Identity management is a method to provide common access and authentication to systems and data through adherence to a common set of standards, identity attributes, data and data definitions, and identity management practices.

Each California State University (CSU) campus has implemented some form of identity management technology to govern access to their local systems and data. In addition, the CSU, through its identity and access management initiative, has implemented common identity management standards and practices to support a unified identity and access management infrastructure across the CSU system. This includes efforts at the campuses and the chancellor’s office to establish the identity authentication and authorization processes necessary to allow students, faculty, and staff to easily access courses, share resources, and conduct research across networked information systems.

Identity and access management technology enables authorized campus individuals to use their local campus digital identity credentials to gain access, as appropriate, to systemwide CSU resources and services. It will also enable secure transactions between education, business, and government partners.

Integrated California State University Administrative Manual (ICSUAM) §8000.0, Information Security Policy, dated April 19, 2010, represents the most recent and specific guidance to campuses regarding the security and protection over access to systems and data. It provides direction for managing and protecting the confidentiality, integrity, and availability of CSU information assets and defines the organizational scope of information security throughout the system.

The policy states that the Board of Trustees is responsible for protecting the confidentiality, integrity, and availability of CSU information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the mission of the CSU, violate individual privacy rights, and possibly constitute a criminal act.

According to ICSUAM §8000.0, it is the collective responsibility of all users to ensure the confidentiality of information that the CSU must protect from unauthorized access, the integrity and availability of information stored on or processed by CSU information systems, and compliance with applicable laws, regulations, and CSU or campus policies governing information security and privacy protection. The policy further states that auxiliary organizations, external businesses, and organizations that use campus information assets must also follow the CSU Information Security Policy.

State Administrative Manual §5300 defines information security as the protection of information and information systems and equipment from a wide spectrum of threats and risks. Implementing appropriate security measures and controls to provide for the confidentiality, integrity, and availability of information regardless of its form (electronic, print, or other media) is critical to ensure business continuity and protection against unauthorized access, use, disclosure, disruption, modification, or destruction. Pursuant to Government Code §11549.3, every state agency, department, and office shall comply with the information security and privacy policies, standards, procedures, and filing requirements issued by the Office of Information Security and Privacy Protection in the California Office of Information Security.
State Administrative Manual §5320 states that each agency must provide for the integrity and security of its information assets by identifying all automated files and databases for which the agency has ownership responsibility and ensuring that responsibility for each automated file or database is defined with respect to owners of the information within the agency, custodians of the information, users of the information, and classification of the information to ensure that each automated file or database is identified in accordance with law and administrative policy.
PURPOSE

Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to the administration and control of identity management and common system access; to determine the adequacy of controls over the related processes; and to ensure compliance with relevant governmental regulations, Trustee policy, Office of the Chancellor directives, and campus procedures.

The objective of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, without the need for redundant user administration. Use of identity federation standards can increase security and lower risk by enabling the CSU to identify and authenticate a user once, and then use that identity information across multiple systems. It can improve privacy compliance by allowing the user to control what information is shared, or by limiting the amount of information shared. Moreover, it can drastically improve the end-user experience by eliminating the need to login to multiple systems.

Within the overall audit objective, specific goals included determining whether:

- Cross-departmental administrative and managerial internal controls are in place, including delegations of authority and responsibility, oversight committees, executive-level reporting, and documented policies and procedures.
- A management framework is established to initiate and control the implementation of identity management within the organization, and management direction and support for identity management is communicated in accordance with business requirements and relevant laws and regulations.
- CSU campuses are participating in the federated model, which defines specific identity validation techniques, process controls, and monitoring.
- Responsibility for definitive identification of individuals is defined, and processes address acceptable forms of photo identification required prior to the assignment of user accounts.
- Responsibilities and procedures for the management of information processing and identity management architecture are defined, and technical security controls are integrated within systems and networks to ensure consistency of user account and password controls for all systems connected to this centralized authentication process.
- Individual user access rights to systems, applications, and business processes are appropriately controlled through user identification and authentication techniques that are based on business and security requirements.
- Formal monitoring and event reporting procedures are in place to identify information security events and weaknesses within the supporting servers and technologies, and communication of such security events is consistent and effective, allowing for timely corrective action.
The overall integration of information systems design, configuration, operation, use, and management are in conformance with statutory, regulatory, and contractual security requirements governing privacy and protected data; and the entire process is regularly reviewed for compliance with associated regulations.
The proposed scope of the audit, as presented in Action Item, Agenda Item 2 of the January 24 and 25, 2012, meeting of the Committee on Audit, stated that Identity Management and Common System Access would include review and compliance with Trustee policy, federal and state directives, systemwide guidance, and campus policies and procedures surrounding system authentication; procedures for technical specifications; program access considerations; technical architecture; and access provisioning and deprovisioning requirements.

Our study and evaluation were conducted in accordance with the International Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors and included the audit tests we considered necessary in determining that operational and administrative controls are in place and operative. This review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor and campus policies, letters, and directives. The audit review focused on procedures currently in effect.

We focused primarily upon the administrative, compliance, operational, and technical controls over authorization processes used to validate the identity of users and ensure that users are appropriate, including security of the server hosting the directory services, the authentication process, and procedures used to create and maintain the user credentials. Specifically, we reviewed and tested:

- Information security policies and procedures.
- Identity management organizational structure and management framework.
- Directory architecture and administrative and technical procedures.
- Access and configuration controls over networks, systems, applications, business processes, and data.
- Authentication methodologies and technologies.
- Procedures to create and maintain user credentials.
- Support and maintenance of the servers used to support identity management systems.

Our testing and methodology was designed to provide a managerial level review of key practices over identity management and common system access. Our review did not examine all systems with independent authentication, but focused on those authentication techniques that were shared by multiple application systems. Our testing approach was designed to provide a view of the system security used to provide access to key networks and applications and to assess the associated identity validation methods.

During the course of the audit, we visited five campuses: Humboldt, Pomona, Monterey Bay, San Diego, and San Marcos. We interviewed campus personnel and audited procedures in effect at the time of the audit.
GOVERNANCE

Campuses had not developed written policies and procedures for overall governance and definition of roles and responsibilities in operating, using, and monitoring the identity access management (IAM) system.

Integrated California State University Administrative Manual (ICSUAM) §8015, Organizing Information Security, dated April 19, 2010, states that each campus must develop, implement, and document the organizational structure that supports the campus’ information security program. The organizational structure must define the functions, relationships, responsibilities, and authorities of individuals or committees that support the campus information security program.

ICSUAM §8030, Personnel Information Security, dated April 19, 2010, states that campuses must implement procedures to revoke access to information resources upon termination of employment, or when job duties no longer provide a legitimate business reason for access, except where specifically permitted by campus policy and by the data owner. Unless otherwise authorized, when an employee voluntarily or involuntarily separates from the campus, information system privileges, including all internal, physical, and remote access, must be promptly revoked.

The campus chief information officers (CIO) stated that campuses had not formally prepared various policies and procedures for the IAM system and overall governance because they thought that meetings between stakeholders and end users provided sufficient oversight and governance of assignment of roles and responsibilities.

A lack of sufficient policies and procedures for IAM may lead to undetected system breakdowns and data misappropriations and misuse, and lack of access monitoring tools could lead to undetected attempts to circumvent system security.

Recommendation 1

We recommend that the chancellor’s office (CO) develop and implement written policies outlining overall governance and definition of roles and responsibilities in operating, using, and monitoring the IAM system.

Management Response

Management concurs. The CO will work with the campuses to develop written systemwide policies to guide the creation, governance, operation, and use of identity management systems in the California State University. These policies will be completed by February 28, 2014.
STUDENT IDENTITY VALIDATION

The campus IAM systems did not require identity validation for all registered students.

ICSUAM §8025, Privacy of Personal Information, dated April 19, 2010, states that campuses acknowledge their obligation to respect and protect private information about individuals stored on campus information systems and network resources. It further states that, except as noted elsewhere in California State University policy, information about individuals stored on campus information systems may only be accessed by the individual to whom the stored information applies or his/her designated representative(s).

The campus CIOs stated that a lack of identity validation for all students and applicants presented little or no risk to the campuses because the students and applicants were provided with only limited access to non-critical systems and data. They also stated that student identity validation was a campuswide issue and was not unique to identity management systems.

Incomplete identity validation increases potential security risk and internal network exposure to security compromises and increases the risk that security over student records may not be adequate.

Recommendation 2

We recommend that the CO evaluate the systemwide implications of campus identity management systems that have not adequately validated student accounts and issue guidance on validation of students requesting access to records.

Management Response

Management concurs. The CO will evaluate the implications of campus identity management systems that have not adequately validated student accounts, and issue guidance on validation of students requesting access to records. This evaluation will be completed by December 31, 2013.

DEPROVISIONING APPLICATION ACCESS

Campuses did not have an adequate process to ensure that changes in access privileges were performed consistently and in a timely manner, or to ensure that privileges within the application systems had been removed.

ICSUAM §8015, Organizing Information Security, dated April 19, 2010, states that each campus must develop, implement, and document the organizational structure that supports the campus’ information security program. The organizational structure must define the functions, relationships, responsibilities, and authorities of individuals or committees that support the campus information security program.
ICSUAM §8030, *Personnel Information Security*, dated April 19, 2010, states that campuses must implement procedures to revoke access to information resources upon termination of employment, or when job duties no longer provide a legitimate business reason for access, except where specifically permitted by campus policy and by the data owner. Unless otherwise authorized, when an employee voluntarily or involuntarily separates from the campus, information system privileges, including all internal, physical, and remote access, must be promptly revoked.

The campus CIOs stated that they had relied on the systemwide IAM working committee to resolve issues regarding the collection and maintenance of attribute identifiers, and that the campuses were waiting for the CO to provide additional guidance on the scope and minimum requirements of an IAM policy. They further stated that the decentralized nature of the information technology functions on campuses had made it difficult to gain consensus on identity management across the enterprise. They also stated the campuses had recognized that the manual processes used to deprovision accounts were subject to human error and delays based on existing processes.

Insufficient policies and procedures for IAM may lead to undetected system breakdowns and data misappropriations and misuse.

**Recommendation 3**

We recommend that the CO notify campus CIOs that weaknesses have been identified in access privilege change processes and in the manual processes that remove privileges within applications, and remind them of the obligation to maintain accurate identity authentication processes.

**Management Response**

Management concurs. The CO will notify the campus that weaknesses have been identified in access privilege change processes and in the manual processes that remove privileges within applications, and remind them of the obligation to maintain accurate identity authentication processes. This notification will take place not later than September 31, 2013.
### APPENDIX A:

**PERSONNEL CONTACTED**

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chancellor’s Office</td>
<td></td>
</tr>
<tr>
<td>Benjamin F. Quillian</td>
<td>Executive Vice Chancellor and Chief Financial Officer</td>
</tr>
<tr>
<td>Bruce Briggs</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Mark Crase</td>
<td>Senior Director, Technology Infrastructure Services</td>
</tr>
<tr>
<td>Ed Hudson</td>
<td>Information Security Director</td>
</tr>
<tr>
<td>William Perry</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>Michael Redmond</td>
<td>Senior Director, Chancellor's Office Fiscal Control and Special Initiatives</td>
</tr>
<tr>
<td>Humboldt State University</td>
<td></td>
</tr>
<tr>
<td>Rollin C. Richmond</td>
<td>President</td>
</tr>
<tr>
<td>Patricia Ambrosini</td>
<td>Payroll Officer</td>
</tr>
<tr>
<td>Dave Bugbee</td>
<td>Associate Vice President, Human Resources</td>
</tr>
<tr>
<td>Josh Callahan</td>
<td>Director, Enterprise Technology</td>
</tr>
<tr>
<td>Dana Deason</td>
<td>Assistant Director, Academic and Career Advising</td>
</tr>
<tr>
<td>Denise Glitzow</td>
<td>Office Manager, Human Resources</td>
</tr>
<tr>
<td>Scott Haag</td>
<td>Director, Admissions and Financial Aid</td>
</tr>
<tr>
<td>Carl Hansen</td>
<td>Dean, Office of Distance and Extended Education</td>
</tr>
<tr>
<td>Mark Hendricks</td>
<td>Information Security Analyst</td>
</tr>
<tr>
<td>Ben Hylton</td>
<td>Accounting Manager</td>
</tr>
<tr>
<td>Anna Kircher</td>
<td>Chief Information Officer/Information Security Officer</td>
</tr>
<tr>
<td>Melissa Koval</td>
<td>Coordinator, Academic Personnel Services</td>
</tr>
<tr>
<td>Emily Kupec</td>
<td>Financial Analyst</td>
</tr>
<tr>
<td>Joyce Lopes</td>
<td>Vice President of Administrative Affairs</td>
</tr>
<tr>
<td>Carol Lorentzen</td>
<td>Associate Vice President, Business Services</td>
</tr>
<tr>
<td>Mary Ann McCulloch</td>
<td>Director, Information Technology Studies</td>
</tr>
<tr>
<td></td>
<td>Administrative Support</td>
</tr>
<tr>
<td>Burt Nordstrom</td>
<td>Vice President, Administrative Affairs (At time of review)</td>
</tr>
<tr>
<td>Clint Rebik</td>
<td>Interim Registrar</td>
</tr>
<tr>
<td>Ken Rocha</td>
<td>Analyst/Programmer</td>
</tr>
<tr>
<td>Lynne Sandstrom</td>
<td>Director, Financial Services</td>
</tr>
<tr>
<td>John Taloff</td>
<td>Library Supervisor</td>
</tr>
<tr>
<td>Ken Thrift</td>
<td>Lead Analyst/Programmer</td>
</tr>
<tr>
<td>Cade Webb</td>
<td>Director, Specialized Application Support</td>
</tr>
<tr>
<td>California State University, Monterey Bay</td>
<td></td>
</tr>
<tr>
<td>Eduardo M. Ochoa</td>
<td>President</td>
</tr>
<tr>
<td>Terry Ashley</td>
<td>Payroll Services Supervisor</td>
</tr>
<tr>
<td>Hayley Azevedo</td>
<td>Academic Personnel Coordinator</td>
</tr>
<tr>
<td>Rachelle Bass</td>
<td>Assistant Director of Student Services</td>
</tr>
<tr>
<td>Diana Cockerham</td>
<td>Administrative Support Coordinator</td>
</tr>
<tr>
<td>Art Evjen</td>
<td>Director of Business and Support Services</td>
</tr>
<tr>
<td>Peter Fernandez</td>
<td>Lead Analyst, Student Information Systems</td>
</tr>
<tr>
<td>John Fitzgibbon</td>
<td>Associate Vice President for Finance</td>
</tr>
<tr>
<td>Veronica Flores</td>
<td>Director of Student Information Systems</td>
</tr>
</tbody>
</table>
APPENDIX A: PERSONNEL CONTACTED

California State University, Monterey Bay (cont.)

Mike Green  Analyst Programmer, Administration and Finance
Grace Cardenas Leal  Director, Academic and Career Advising
Chip Lenno  Chief Information Officer/Information Security Officer
Steve Mann  Associate Director of Network Services
Mary Mauro  Director, Information Technology Compliance and Planning
William Musselman  Director of Accounting
Venkata Paruchuru  Lead Administrative Analyst
Kevin Saunders  Vice President of Administration and Finance
Karen Sellick  Program Coordinator/Analyst, Extended Education
Eric Simoni  Associate Director of Information Systems
Henry Simpson  Director of Technology Support Services
Laura Tantillo  Diversity, Equity, and Employee Development Analyst
Chris Villanueva  Credential Analyst II, Calstate TEACH Program

California State Polytechnic University, Pomona

J. Michael Ortiz  President
Al Arboleda  Associate Chief Information Officer (CIO) of Operations, Instructional and Information Technology (I&IT)
Edwin Barnes III  Vice President and Chief Financial Officer, Administrative Affairs
Deborah Brandon  Executive Director, Office of Admissions and Outreach
David Drivdahl  Interim Director of System Administration, I&IT
Paul Henson  Operating System Analyst, I&IT
Rose Kukla  Director, Student Affairs Information and Technology Services
Darwin Labordo  Associate Vice President, Finance and Administrative Services
Lee Anne Ma  Student Administration Security Coordinator
Candie McDougall  Lead Support Help Desk, I&IT
John McGuthry  Chief Information Officer, I&IT
Dennis Miller  Chief Employment Officer and Managing Director, Foundation
Gary Pierce  Information Security Analyst, I&IT
Tim Raymond  Director of Central Applications, I&IT
Jane Self  Director of Payroll, Employment and Compensation Services, Human Resource Services
Randall Townsend  Management Information Systems Manager, Foundation
May Tang  Systems Administrator, Administrative Affairs Information Systems
Glendy Yeh  Executive Director, Administrative Affairs Information Systems and Interim Associate CIO Enterprise Applications, I&IT
Joice Xiong  Director of Internal Audit, Administrative Affairs

San Diego State University

Elliot Hirshman  President
Scott Burns  Associate Vice President, Financial Operations (at time of review)
Mikhail Burstein  Director, Student Information Management System
Valerie Carter  Director, Audit and Tax
Tony Chung  Director, Information Systems Management, Student Affairs
Bob Hilchey  Staff College of Sciences
San Diego State University (cont.)
Darrell Irwin                Staff College of Engineering
Loretta Leavitt             Associate Vice President, Financial Operations
Gene LeDuc                  Information Technology Security Officer
Tom McCarron                Vice President, Business and Financial Affairs
Diana Osborn                Operating Systems Analyst, Expert, College of Sciences
Rich Pickett                Senior Director and Chief Information Officer, Enterprise Technology Services
Michael Pietrzak            System Administrator
Kimberlee Reilly            Assistant Controller
John Ross                   Academic Information Technology Coordinator/
                           Information Technology Interim Director
Sally Roush                 Vice President, Business and Financial Affairs (At time of review)
Jim Varnell                 Staff, College of Sciences
Felecia Vlahos              Information Security Officer
Rayanne Williams            Registrar

California State University, San Marcos
Karen S. Haynes             President
Candice Bebee               Assistant to the Vice President
Jane Cross                  Director Payroll Services
Wayne Dilly                 Operating Systems Analyst
April Grommo                Director, CMS Program
Randi Hall                  Program Coordinator, IT Project Office
Linda Hawk                  Vice President Finance and Administrative Services
Chris Lambert               Manager, Accounting and Systems Operations and Development
Penny Lanese                Information Technology Consultant
Teresa Macklin              Information Security Officer/Director, Enterprise Systems Group
Carol McAllister            Director Admissions and Outreach
Lisa McLean                 Human Resources Manager
Diane Petersen              Analyst/Programmer, Database Group
Katy Rees                   Assistant Vice President of Administration
Thomas Swanger              Registrar
Susan Thompson              Library Systems Coordinator
Wayne Veres                 Dean and Chief Information Officer, Instructional and
                           Informational Technology Services
Sarah Villarreal            Associate Dean Extended Learning
Deirdre Wallace             Faculty Personnel Generalist
MEMORANDUM

DATE: July 19, 2013

TO: Larry Mandel
   University Auditor

FROM: Benjamin F. Quillian
      Executive Vice Chancellor and
      Chief Financial Officer

SUBJECT: Audit Report # 12-44 Identity Management and Common System
         Access Audit

In response to the “Incomplete Draft” report dated June 11, 2013, we are providing the
enclosed management responses.

Should you have any questions, please feel free to contact us.

BFQ:mpr

Attachment

cc: Bruce Briggs, AVC/CIO Information Technology
    Mark Crase, Chief Technology Officer
    William Perry, Chief Info Management & Security Officer
    Michael Redmond, Sr. Dir. CO Budget and Special Initiatives
IDENTITY MANAGEMENT AND COMMON SYSTEM ACCESS

SYSTEMWIDE

Audit Report 12-44

GOVERNANCE

Recommendation 1

We recommend that the chancellor’s office (CO) develop and implement written policies outlining overall governance and definition of roles and responsibilities in operating, using, and monitoring the IAM system.

Management Response

Management concurs. The CO will work with the campuses to develop written System-wide policies to guide the creation, governance, operation and use of identity management systems in the CSU. These policies will be completed by February 28, 2014.

STUDENT IDENTITY VALIDATION

Recommendation 2

We recommend that the CO evaluate the systemwide implications of campus identity management systems that have not adequately validated student accounts and issue guidance on validation of students requesting access to records.

Management Response

Management concurs. The CO will evaluate the implications of campus identity management systems that have not adequately validated student accounts, and issue guidance on validation of students requesting access to records. This evaluation will be completed by December 31, 2013.

DEPROVISIONING APPLICATION ACCESS

Recommendation 3

We recommend that the CO notify campus CIOs that weaknesses have been identified in access privilege change processes and in the manual processes that remove privileges within applications, and remind them of the obligation to maintain accurate identity authentication processes.
Management Response

Management concurs. The CO will notify the campus that weaknesses have been identified in access privilege change processes and in the manual processes that remove privileges within applications, and remind them of the obligation to maintain accurate identity authentication processes. This notification will take place not later than September 31, 2013.
September 4, 2013

MEMORANDUM

TO: Mr. Larry Mandel
   University Auditor

FROM: Timothy P. White
      Chancellor

SUBJECT: Draft Final Report 12-44 on
         Identity Management and Common System Access, Systemwide

In response to your memorandum of September 4, 2013, I accept the response as submitted with the draft final report on Identity Management and Common System Access, Systemwide.

TPW/amd