Identity and Access Management Final Report

Monday, February 18, 2008

Table of Contents

Executive Summary 2

Introduction 3

Identity and Access Management Concepts and Processes 4

Reasons for an Identity and Access Management Strategy 6

Strategic Goals and Recommendations for Identity & Access Management at Penn State 7

Next Steps 12

Conclusion 13

Appendix A – Real Life Cases Where Identity & Access Management is Needed to Address Current University Challenges 14

Appendix B – Glossary of Terms 19

Appendix C – Identity & Access Management Committee and Sub-Committee Team Members 20

Executive Summary

The University is facing the challenge of simultaneously providing greater security for our digital assets and related computer systems, while at the same time becoming more open—encouraging collaboration, facilitating online learning, and engaging new types of customers. This dilemma presents a complex challenge in that many University business processes and automated applications currently in place were originally designed for a world that is radically different than the one we face today.

Although daunting, these challenges can be faced by a comprehensive approach to Identity & Access Management. An implementation successfully embracing the strategic recommendations outlined in this document would not be simple and would require significant human and financial resources, as well as a cultural change in how we manage identities and provide access to online resources. However, a successful implementation would also have significant returns. Not only would the security of our digital assets be increased and risk of breach mitigated, but we could also achieve significant efficiencies in operations, improve customer service, and provide a solid foundation for the delivery of new online services in the future.

Core Concepts - Identity & Access Management concepts and processes can be broadly broken down into the following three categories:

- **People and Relationships –** The myriad of individuals who need to interact with the University's online resources and the related life-cycles of these interactions.
- **Creation and Maintenance of Identities** – The management of the assignment of identity records and issuance of identity credentials (IDs, passwords, and other tokens) to individuals.
- **Access to Data and Applications** – The management of access rights to online resources—ensuring they are appropriately and efficiently granted when needed, auditable, and updated or removed when circumstances change.

Foundational Goals - Four overarching goals provide the foundation for a comprehensive strategy toward the implementation of Identity & Access Management at Penn State:

- Increase collaboration and innovation
- Improve customer service
- Increase efficiency, productivity, and cost containment
- Improve security of digital assets and mitigate risks

Strategic Recommendations - The following eight recommendations are offered to advance these goals.

1. **Create a Comprehensive Policy for Identity & Access Management** – A comprehensive policy, covering all aspects of Identity & Access Management, does not exist today and needs to be developed. This policy framework is crucial for the project's success.
2. **Develop a Plan for Formal Risk Assessment** – A systematic risk management process is needed to evaluate the technology and information systems that are critical to the University's mission.

3. **Create a Central Person Registry** – A single centralized person registry is needed to combine identity data records from disparate systems, ensuring the integrity and availability of person records.
4. **Add Level of Assurance Component to Accounts and Access Decisions** – A more granular approach to account creation and access decisions is needed. A Level of Assurance component will provide this flexibility and is also being required by federal agencies.
5. **Promote Single Sign-on, Federated Identities, and Better Control of University Digital Credentials –** Better control of Penn State digital credentials is needed—especially in regards to the use of these credentials with outside agencies, hosted vendor solutions, and other institutions of higher education. Single sign-on and federated identities will provide this control.
6. **Streamline Vetting, Proofing, and Issuance of Digital Credentials** – Significant gains in efficiency could be realized by overhauling the current processes for creating accounts and issuing credentials.
7. **Automate the Provisioning (and De-provisioning) of Access Rights** – Customer service and security could both be significantly increased by automating the provision of access based on affiliation, roles, and attributes.
8. **Promote Awareness and Education of the Importance of Identity & Access Management** – Initial awareness and on-going education is needed to promote understanding of the importance of Identity & Access Management and achieve buy-in from stakeholders.

Introduction

Resources like ANGEL, eLion, IBIS, and hundreds of other online services are flourishing at Penn State today because they offer convenience, increased levels of service, and greater productivity. The growing demand for these services makes it critical for Penn State to ensure that its digital transactions are secure, by controlling who has access to digital services and how that access is managed. Identity and Access Management (IAM) accomplishes this objective by establishing the processes used to identify users, and by deploying the technologies that control access to online resources. IAM is indispensable to all operational aspects at Penn State today because it allows the University to manage the process of connecting people directly with the digital services they need.

With demands for IAM paralleling the explosive growth in online interactions, it is imperative that Penn State's existing business systems, infrastructure, planning, and technologies evolve to keep pace with the access needs of the future. Recognizing the importance of developing a comprehensive, forward-looking strategy to deal with this issue, Kevin Morooney, Vice Provost for Information Technology Services, formed the IAM Initiative in April of 2007. The primary committee and related sub-groups is comprised of forty individuals who span many administrative areas at the University (see listing in appendix C). The group is co-chaired by Renee Shuey, Information Technology Services (ITS), and Joel Weidner, Auxiliary and Business Services.

The group's primary charge was to create an identity and access management road map (or strategy) for Penn State. A secondary goal was to establish a community of people and organizations from across the University who understand each other's pressures, needs, and desires for developing an IAM infrastructure that will support and enhance academic, research, business, and collaborative processes.

These efforts will ensure that Penn State not only complies with newly developing federal requirements, but also remains a recognized leader in the delivery of online services.
The purpose of this report is to both educate the Penn State community on the IAM challenges that we face as well as to present broad strategic recommendations for meeting those challenges.

Identity and Access Management Concepts and Processes

IAM concepts and processes can be broadly broken down into the following three categories:

- **People and Relationships**
- **Creation and Maintenance of Identities**
- **Access to Data and Applications**

Concept of People and Relationships – Identity and Access Management begins with people and their relationships (or affiliations) with the University. Many types of individuals have relationships with the University and the subsequent need to access online resources. Some of these relationships are obvious, such as student, faculty, and staff, but others are less so, such as patient, volunteer, supplier, and independent contractor. Some relationships tend to be formal, while others are more casual. For example, a student who is enrolled in the University has a more formal and complex relationship than a prospective student who ultimately may not attend the University.

It is also important to note that the University has digital relationships with individuals who may never physically set foot on a Penn State campus. Students enrolled at other universities take Penn State classes; World Campus students connect to the University from other countries; researchers collaborate with Penn State colleagues from other institutions; and University vendors and suppliers are based all over the country and the world. The boundaries of Penn State stretch far beyond the physical confines of the Commonwealth of Pennsylvania.

In addition, the University environment is a dynamic one, where relationships, responsibilities, and the rules of engagement are constantly evolving. Prospective students become enrolled, may withdraw, or eventually graduate. Enrolled students may change their respective campus locations or majors. Prospective faculty and staff apply for positions, are hired, and eventually change job responsibilities, terminate their employment, or retire. Other individuals may have multiple affiliations with the University, serving as students, faculty, staff, suppliers, or alumni concurrently. As circumstances change over time, the need for access to specific online resources can change as well. Managing appropriate access to resources in this dynamic environment is critical to the success of the University. Not only does service and productivity suffer when systems do not keep pace with changing affiliations and responsibilities, but the University's valuable digital assets can be put at risk.

Concept of Creation and Maintenance of Identities – A critical first step in establishing an individual's digital relationship with the University is the careful creation of that person's "identity" and the issuance of his or her digital credentials (most commonly a user ID and password). An individual's identity has many components and includes such things as name, address, past academic or employment history, and credentials issued by other agencies, such as social security numbers, passports, birth certificates, and driver's licenses. Two processes are typically employed in establishing an individual's digital credentials:

Vetting: Vetting is the process of collecting and validating information about an individual's identity for the purpose of issuing digital credentials that will grant him/her access to University resources. During this process, a registration authority, such as the Office of the University Registrar or the ITS Accounts Services Office, has the authority to verify the data and issue credentials on behalf of the University. In addition, the amount and type of data that is collected and validated will directly impact the level of confidence (or level of assurance) that the University places on the identity.

Proofing: Proofing is the act of aligning an individual's previously recorded data to the actual person—most notably at the time when credentials are issued. In order to achieve a high level of assurance (and confidence that individuals are who they say they are), some type of "in-person" (or face-to-face) proofing must occur. Credentials can be issued without in-person proofing, but the level of identity assurance will be lower than for those where in-person proofing is conducted. It is important to note that in-person proofing can also occur remotely (away from the University). In this scenario, a remotely located individual would be able to present proof of in-person verification via a notary or other authorized official.

Re-credentialing, the process by which new credentials need to be issued, could be another circumstance in which in-person verification may be required. The most common situation would be when a password is forgotten and needs to be reset. To ensure that the new password is issued to the correct individual some type of re-proofing must occur.

In most cases, the credentials that are issued in each of these processes consist of a user ID and password pair. However, for cases where a higher level of assurance is required, a 2nd factor credential can be issued as well. Currently, the University uses RSA's SecurID token, for applications where greater security and a higher level of assurance is needed. For these applications, the user is required to enter his or her user ID and password, as well as the SecurID's six-digit number (which is generated in a pseudo random fashion every sixty seconds). Without the token, a stolen user ID and password cannot be used to gain illicit access to the application and data.

Concept of Access to Data and Applications – The end purpose of IAM is to connect individuals with the appropriate online resources in a timely and convenient fashion; however, the provisioning of specific kinds of "access" can be a complex process. Access to online resources depends on a multitude of factors, including the individual's affiliation, affiliation status, the specific context and attributes for the relationship, as well as the level of assurance assigned to the digital identity. For example, employees generally have access to different resources than students and students in one college or class section have access to different resources than students in a different college or section. Access to resources changes throughout the life cycle of an affiliation. The access granted to prospective employees is different than to current employees, as well as retirees. Access can also be impacted by the protocol used when someone is connecting to a specific online resource (i.e., access to some resources may require an encrypted data stream or the use of 2nd factor authentication).

The appropriate balance of security and openness can be obtained by examining a level of assurance prior to providing access to data and applications. A cultural shift needs to occur in how the University grants access. Access can no longer be granted based only on authentication, but instead on some combination of authentication, affiliation, attributes, and

level of assurance. If IAM is implemented and managed successfully, much of the provisioning (and de-provisioning) of access can happen automatically based on normal business practices that already occur each day, such as the enrollment and scheduling of students, the hiring of employees, and the awarding of research grants.

Reasons for an Identity and Access Management Strategy

Given the issues described above, there are numerous motivating forces for creating a well-integrated and unified identity and access management infrastructure across the University. Some of these forces, which are both internal and external to Penn State, are described below.

- Federal government legislation and industry regulation have increased over the last few years, increasing the need for audit and compliance. The University is responding to requirements of HIPAA, FERPA, CALEA, the Payment Card Industry, and eDiscovery. A good example of this type of regulation is the new standards imposed by the Department of Education for the signing of Master Promissory Notes. The failure to meet these standards could result in losing Title IV funds, causing a loss of $500 million per year at Penn State. In addition, federal agencies plan to begin allowing access to their services via non-governmental "identities," such as the Penn State Access Account. In order to provide this type of connection capability for our community members, Penn State's policies must meet federal requirements for identity proofing, the issuing and distribution of credentials, and documentation of policies and practices.

- A well executed Identity and Access Management strategy would help to solve some real-life challenges that are faced daily at Penn State. Three brief examples are provided with more details and examples in appendix A.

    - New faculty and staff hires face an unmet need to access University systems, to choose benefit options, setup syllabi, and prepare for classes--before they set foot on a Penn State campus.

    - Patients and family members at the Hershey Medical Center need access to network resources while onsite for treatments and visits, but current policies and processes for provisioning access are cumbersome and resource intensive.

    - Distance education students across Pennsylvania, and around the world, face significant challenges in gaining access to the required online University resources needed for their education.

- Penn State is facing internal pressures to offer a wider assortment of online services to broader, geographically dispersed audiences. These services include the provision of accounts for distance-education students and contracting with third-party hosted services, such as online music providers, external course management systems, and outsourced purchasing services. IAM also provides the foundation for collaboration with other higher education and research institutions. Penn State shares course material, faculty, and students with higher education institutions all around the world. A comprehensive IAM implementation will facilitate virtual inter-institutional student exchanges and curriculum development, while minimizing redundant course offerings. The ability to identify students and faculty to peer institutions greatly contributes to the success of inter-institutional and international sharing of curricula and students. Penn State's identity and access management system will need to address the issues related to the identification of our community not only on Penn State campuses but around the world.

- Current Penn State initiatives such as Information Privacy and Security (IPAS) and Workflow have been created in response to continued increase of legislation, the need to mitigate risk, and the increased necessity and desire for collaboration in the higher education community. Identity and Access Management is critical to the support and success of these initiatives, providing the foundation for identifying individuals on our network and the assignment of roles to these individuals.

Strategic Goals and Recommendations for Identity & Access Management at Penn State

Four overarching goals provide the foundation for a comprehensive strategy toward the implementation of IAM at Penn State:

- **Increase collaboration and innovation** – furthering the vision of the University as the finest in the integration of teaching, research, and service.

- **Improve customer service** – resulting in higher satisfaction for students, employees, and other affiliates who are granted appropriate access, in a timely manner, with a minimum of effort.

- **Increase efficiency and productivity** – reducing administrative effort and related costs faced by units in managing identities and provisioning access.

- **Improve security of digital assets** – allowing for more tightly controlled credential issuance, increased granularity, timely provisioning of access, and greater protection of our digital assets.

The following recommendations are offered to advance these goals:

1. Create a Comprehensive Policy for Identity & Access Management – Develop a comprehensive overarching policy for IAM. As IAM requirements change, both internally and externally, Penn State must respond through adjustments and updates to its IAM policy, standards, and procedures. An advisory structure needs to be created to guide policy and resolve disputes and discrepancies as well as facilitate the integration of new requirements.

There is currently no comprehensive IAM policy at Penn State. While various policies exist that address specific aspects of IAM–such as network security, ID cards, or Access Accounts--there are inconsistencies between existing policies and related procedures. An initial analysis was recently completed to identify these gaps and inconsistencies.

An advisory structure will need to be created to determine the strength of policy in each area. Current practices at Penn State will need to be reviewed in light of industry best practices. Ultimately, standards and requirements will need to be formed that meet the business needs of the University for both our internal and external business processes. Clear articulation of the scope, boundaries, and balance among different roles within IAM will also be critical to building a successful implementation model.

The following is recommended:

- Create a collaborative group representing University-wide interests and needs, serving as an advisory group for IAM. Individuals participating in this group would be expected to understand related business needs, general principles of person management, and identity management concepts, and should be selected based on skills and potential contributions rather than title. This group would provide advice and counsel in the development, interpretation, and modification of policy in the area of IAM, and would evaluate and respond to newly identified needs.

- Create an office or department responsible for all day-to-day operations related to IAM, which would follow established policies, procedures, and standards. This office would likely reside in Information Technology Services (ITS).

- Create a new position with a strategic perspective and the authority to move quickly to resolve issues. This person would be charged with interpreting IAM policy and facilitating prudent and responsible requests. As appropriate, this individual will bring unanticipated needs to the attention of the IAM advisory group. The individual would additionally be responsible for assuring that policy is developed at the granular level as required by the decentralized departments needing such guidance and building awareness and education campaigns. The key consideration is to find an individual who has the authority, passion, and interest to take on the leadership of an effort that is crucial to advancing Penn State's identity and access management mission.

2. Develop a Plan for a Formal Risk Assessment – Design and implement a systematic risk management process for information systems that are critical to the University's mission. Implement comprehensive assessment methodology to manage potential IAM-related risk at Penn State. We recommend these assessments be conducted via the following:

- Categorize the data, based on its sensitivity.
- Measure the negative impact of unauthorized access to a given category of data based on factors such as reputation, financial, operations, confidentiality, personal safety, and legal compliance obligations.
- Map the potential impact score with the level of assurance required to protect the data.
- Use the level of assurance required to choose an appropriate technology for E-authentication as recommended by the National Institute for Standards and Technology 800-63 document, or use a similar methodology to assess the risk of a specific E-authentication method.
- Employ physical and electronic controls to support a systematic risk assessment process.

3. Create a Central Person Registry – Create a single centralized person registry that would combine and consolidate identity information currently stored in separate and non-integrated sources throughout the University. A person registry is a directory or database whose primary function is identity management. Currently much of Penn State's critical identity information is stored in multiple systems such as ISIS, IBIS, OHR, CIDR, ID Card System, LDAP (Lightweight Directory Access Protocol), and CACTUS. LDAP, the standardized directory infrastructure that supports Penn State's Online Directory Services, is the closest approximation to a central person registry at the University. However, LDAP is not complete and updates from other sources are not always consistent and timely. The new central person registry would combine

identity data records from these disparate University systems. Integrity rules would be applied that would ensure the validity of the identity data—resulting in a complete and up-to-date person record for each individual University member or affiliate.

Full implementation of a single person registry at Penn State is crucial to enabling the efficient creation and maintenance of digital identities, as well as the accurate provision of access. Central registry services could be available to those offices that have a role in establishing identities and issuing credentials, as well as to application providers for the real-time provisioning of access.

4. Add Level of Assurance Component to Accounts and Access Decisions - Create five levels of assurance to support access to current and future business and academic processes, applications, and data. “Level of Assurance” is a term used to describe the degree of certainty that an individual is who he/she claims to be when he/she present a digital credential. *Level of Assurance* is necessary for IAM at Penn State to support the balance of security with an open environment. It is important for the *Levels of Assurance* at the University to align closely with the National Institute of Standards and Technology guidelines and the federal government's Office of Management and Budget's Memorandum. This alignment will allow the University to federate--asserting University identities with peer institutions, business partners, and the federal government.

The IAM group recommends that the degrees of certainty, or *Levels of Assurance*, be defined as 0 through 4, with 0 being the lowest degree of certainty and 4 representing the highest. There are a number of factors that will affect the degree of certainty related to an individual’s digital identity. The assertion of the digital credential and determination of the current *Level of Assurance* will take place as the individual requests access to specific online services. Vetting, proofing, authentication type, protocols, and credentialing/re-credentialing all will impact the *Level of Assurance* that will ultimately be assigned to a specific digital credential through this process.

In addition, Registration Authorities, individuals, and applications or services will need to meet specific requirements to determine *Levels of Assurance*. Registration Authorities, including both the central and authorized delegates, will be assigned a maximum *Level of Assurance* that they are able to grant to an individual’s digital identity. The *Level of Assurance* that each Registration Authority is eligible to issue will be determined by an advisory group and University policy.

5. Promote Single Sign-On, Federated Identities, and Control of University Digital Credentials – Simplify and protect Penn State digital credentials by promoting Single Sign-On (SSO) capabilities both within the University environment as well as external agencies. Multiple digital credentials (IDs and passwords) are confusing for users, difficult to manage for both users and application providers, and create significant security risks. The University should continue to reduce the number of credentials for any given individual and promote single sign-on based services. Although progress has been made, there are still many silos of identity within the University that force users to create and maintain multiple IDs and passwords. In some cases, IDs are common, but passwords are not integrated. For example, IBIS/ISIS, the Data Warehouse, and the Access Account all use the same user ID, but do not share passwords.

Penn State should also federate identities with external application providers. A federation is an association of organizations that come together to exchange information (as appropriate) about their respective users and resources in order to enable collaborations and transactions.

Federating identities allows users to access resources outside of the University using Penn State credentials. With an emphasis on privacy within university communities and a need for collaboration, the capability to federate identities becomes critical for day-to-day business. Federations allow users to share resources within an agreed-upon trust fabric.

The successful federation of identities has been accomplished at the University with some external providers, but there are other contexts where this is not the case. In some cases, when departments outsource applications, the decision is made to use non-federated authentication, but the Access Account user ID is still used on the remote system. In these cases there is a strong possibility that users are also entering the same password, on these out-sourced systems, as they use in the Penn State domain—effectively forfeiting control of the credentials to an external provider. The successful federation of identities, around established standards, would reduce this risk, keeping the control of Penn State credentials within the University.

6. Streamline Vetting, Proofing, and the Issuance of Digital Credentials - Conduct a careful review of the processes currently in place to establish and validate identity and issue credentials with the goal of significantly reducing the amount of time and effort between the initial request for a digital account and the activation of that account.

In some cases the current process has become too cumbersome. For example, for a new faculty or staff member to obtain a Penn State Access Account, it most likely involves a trip to the ITS Accounts Services Office to complete a paper form and an additional visit to the id+ Card office with yet another paper form. The employee must then wait 24-72 hours while various systems are updated and then make a final physical visit to a signature station to activate the account. Even then (when the account is already technically active) it may take weeks until the account is fully provisioned and appropriate access granted to various applications. This non-integrated process results in poor customer service, excessive administrative overhead, and loss of productivity.

The following sub-recommendations have been identified to improve the efficiency of these processes:

A. Review current signature station process - The current signature station process should be reviewed in light of Penn State's overall IAM strategy. The role of the technology employed and intent of each step in the process should be evaluated, including:

- Remove elements of the process that are not directly related to IAM.
- Determine if the capture of signatures via a signature pad/tablet is still required.
- Consider the role of the id+ Card in the process and if the id+ Card issuance and credential issuance should be more tightly coupled.

B. Review of account Registration Authorities – Conduct a review of who currently has responsibility for proofing, vetting, and the issuing accounts to ensure that responsibility and authority rests in a single, centralized office. Create clear policy regarding the delegation of registration authority responsibilities, including the proper training and certification of delegated Registration Authorities. Conduct regular audits of Registration Authorities (and related practices) for compliance.

C. Leverage existing vetting and proofing activities – Identify the areas where information is currently being collected by multiple offices (and in some cases multiple times) for the same individuals. The collection and verification of identity information—regardless of the purpose—should be leveraged and made accessible to the registration authorities responsible for issuing credentials so that the pertinent information would be collected only once. The information collected would then be stored as part of the central person registry (see goal 3).

D. Consider opportunities to integrate the issuing of credentials with in-person proofing that is already taking place, increasing efficiency and customer service.

E. Consider a method for self-service re-credentialing – Password resets are the most common form of re-credentialing and the University is currently inconsistent in the application of procedures related to password resets. A self-service password reset would allow users to reset their passwords online, accompanied by a reduction in the Level of Assurance associated with the account. Some type of in-person re-proofing could then follow (for example, confirmation from the department) that would allow the Level of Assurance to be increased to the original level.

F. Consider the merging of Access Accounts and Friends of Penn State accounts (FPS) into a single type of account undistinguishable by the end-user. Ideally, the types of accounts issued to users should only be distinguished by the assigned Level of Assurance and the access provisioned to those accounts. All accounts should be authenticated via the same processes with no apparent difference to the application provider or end-user.

G. Review current second factor authentication (RSA SecurID) infrastructure. The University's existing second factor credentials are limited primarily to faculty and staff. It is conceivable that in the future the use of second factor tokens will need to be expanded and issued to other affiliates. The cost of significantly expanding the use of the current RSA SecurID tokens would be very expensive and difficult to manage. Alternatives to the current technology need to be explored, taking into consideration the cost and manageability integration of the infrastructure. Consideration should also be given to moving the control and administration for the second factor tokens to the account registration authority—centralizing the administration of identity credentials within a single office.

7. Streamline and Automate the Provisioning (and De-provisioning) of Access – Automate the provisioning of access to resources and applications to reduce the time it takes for new users to gain access to appropriate resources. Basic access could be provisioned (granted) in initial broad strokes based on an individual's affiliation (or, in other words, specific relationship to the University). As the affiliation is further defined through the use of directory-enabled roles and attributes, additional more finely-tuned access can be automatically granted as well. The timely updating of the central person registration, described above, and related directory services, will be critical to the success of timely and automated provisioning (and de-provisioning) of access.

This new model for affiliations, related statuses, and attributes will give the University the ability to define relationships (that may include certain inherent rights for access) in a way that did not exist before. Assigned roles in the new Web Role Assignment Tool database (WebRAT), as well as the new departmental identity attributes, could dovetail with a new affiliations matrix, and other current data sources, to clearly describe an individual's relationship with the University in a

very specific context—creating an identity profile or view of each person. Access could then be automatically provisioned and de-provisioned as that profile changes.

It is important to note that this is a new model for provisioning access. It is significantly different from our current model where Area Security Representatives (ASRs) complete forms requesting access from data stewards who are responsible for certain data elements. This proposed level of automation will also require the real-time integration of many of Penn State's existing administrative systems (and the related business logic) that currently govern access. However, not all provisioning will occur automatically even under this new system. There will always be certain scenarios, resources, or applications that will need to be provisioned manually based on a request to a data steward or application provider. Yet, even when these cases are taken into account, automatic provisioning, if successfully implemented, will provide increased productivity, a higher level of customer satisfaction, and greater security.

8. Promote Awareness and Education of the Importance of Identity & Access Management – Initial awareness and on-going education is needed to promote understanding of the importance of Identity & Access Management and achieve buy-in from stakeholders. This education will need to occur at many levels including individuals, service providers, and advisory boards.

Next Steps

The following steps will provide the foundation for reaching the eight IAM recommendations critical to Penn State's future in this online world.

Initiate Awareness – The committee is In the process of scheduling informational meetings with each of the University executives who have provided resources for this IAM initiative. To aid in this communication a brief video is being developed providing a high level overview of IAM and its importance to Penn State. The co-chairs will be presenting at the next Network of People meeting as well as strategic planning sessions of various departments. Recognizing that awareness needs to come from all directions and levels, handouts and presentation materials will be created with common points of interests.

Implement a Pilot of Level of Assurance – Create a team to identify requirements to provide access to online services using a Level of Assurance model, advancing the cultural shift in the way resource providers think about granting access. This pilot, will tackle an existing problem--leveraging our membership in the InCommon Federation--to partner with National Institutes for Health (NIH), providing researchers access to NIH applications assessed as level 2.

Create an IAM Model and High Level Implementation Plan – Create a team to begin development of a more detailed conceptual model for IAM and a high level implementation plan. The scope of this project is significant—impacting the entire Penn State population. However parts of the plan could be implemented in phases. It is likely that incremental changes could also be identified that would improve existing business processes and further the goals of IAM. These incremental changes would have the benefit of increasing productivity and security, without significant disruptions to existing business processes.

Conclusion

The current Penn State Access Accounts and Friends of Penn State accounts have served the University well and have allowed the successful delivery of critical online services. The University's implementation of Kerberos and related WebAccess authentication services have contributed to this success by providing single sign-on capability for many core applications at Penn State. However, there is growing evidence that we have become the victims of our own success. Now that online services have become ubiquitous, the challenges of managing identities and access properly are critical to Penn State's success. Ensuring that the right individuals have access to the right services and data, when they need it, has become a challenge that in some cases is hampering the delivery of services, frustrating customers and service providers alike, and placing the University and related digital assets at risk. In addition, new requirements from external agencies and partners like the federal government and other institutions of higher education, as well as changes in privacy laws, are requiring the University to re-evaluate its current practices and re-think the way in which digital identities are created and managed.

The challenge of implementing a comprehensive identity and access management environment at Penn State is complex and daunting, one that will cross departmental boundaries and impact many current business applications and practices. The change will require a cultural shift in how the Penn State community thinks about identity management, and a collaborative effort is called for in facing this challenge. A successful implementation, however, will strategically position the University for future success, allowing online services that support the mission of the institution to flourish, while at the same time containing costs and mitigating risk.

Appendix A – Real Life Cases Where Identity & Access Management is Needed to Address Current University Challenges

A new approach to Identity & Access Management at Penn State will increase efficiencies and provide better service to the many different types of customers the University serves each day. The new environment needs to be flexible and have the ability to provide access on a more granular level—allowing the level of trust and access to change over the life of the relationship. The policy and related identity systems need to be structured into an infrastructure that can provide prompt service, with minimal administrative overhead, all the while protecting the digital assets of the University.

The following scenarios provide examples of real situations, occurring within the University, that demonstrate the need for improvement and a more comprehensive approach to Identity & Access Management.

Continuing Education/Adult Students - School teachers from the Philadelphia area are enrolled in a continuing education program at the Abington campus. They are required to obtain a fully provisioned access account to participate in the course. To obtain the access account they are required to drive up to an hour from their home or work locations to perform in-person proofing and activate their account at a signature station—a cumbersome requirement for a teacher working full time in addition to taking a class. Alternatives were considered to make the activation of accounts easier, but our current Identity & Access Management environment does not provide the flexibility to provide the level of service needed for these customers.

New Students Applying for Admissions and On-campus Housing - A new student applies for admissions online using their newly created Friends of Penn State (FPS) account in the early spring. The University's WebAccess single sign-on infrastructure allows them to request their housing contract and follow the status of their housing offer online in eLiving. As their summer FTCAP session draws near, their new Access Account is provisioned, but because they have not yet attended FTCAP, where they will receive their ID card and fully activate their Access Account, the use of the FPS account on WebAccess begins to fail and they are unable to access eLiving until FTCAP has been completed. A more integrated approach to Identity & Access Management would allow for a seamless transition and the use of a single account for the student's entire lifetime of interaction with Penn State.

Prospective Students Visiting Penn State New Kensington - New Kensington invites high school guidance counselors and students to visit campus and complete an online application while staff are available to help answer questions. Access to the appropriate online resources in the computer labs is only available via a fully provisioned Access Account and poses challenges to accommodate the needs of these prospective students. A new approach to Identity & Access Management that better manages visitor access would help solve this problem.

New Faculty and Access to Angel and Other Class Resources - A new faculty member is hired at Penn State York. Her official appointment begins in August but she needs access to Angel and other online resources before that time to prepare for the class she is about to teach. She does not need the full access that she will eventually have as a full-time employee but because of the date of the appointment, her access account cannot be activated ahead of time. A more granular approach to granting access that is not available with Penn State's current Identity & Access Management environment would help to solve this problem.

Adjunct Faculty Activating Access Account - A new adjunct faculty member is hired to teach a single class. Prior to arriving he is sent some forms to complete, including his request for an Access Account. Upon on arriving on-campus he is sent to the ID office to obtain an ID card (required to activate his access account). Because his appointment in IBIS has not yet been entered into the system, he is given another paper form to take to the ID office. After obtaining his ID, he goes to a signatures station, only to become frustrated because his request for an account has not yet been processed. After walking to the Accounts office in the Computer building to check on his account, the form is located, but it will be another day until the required systems are updated so the signature station can be used. The following day he returns the signature station and successfully activates his Access Account. He immediately tries to access Angel to setup his course syllabus, only to realize, his access to Angel resources has not yet been provisioned—causing more frustration and delay. A new approach to Identity & Access Management that would streamline account creation and automate the provisioning of access would greatly improve customer service.

New Faculty & Staff Selecting Benefits - Many employees make a commitment to work for Penn State several weeks or months before their actual start/hire date. Some of these employees are staff and faculty from elsewhere in the United States or even from other countries. Latency issues with departments processing and approving the appropriate employment forms can cause delays in fully activating the employee's Access Account. The need exists for these "pending employees" to be able to make their online benefits selections for medical coverage, life insurance, retirement, etc.--prior to arriving at Penn State or having an active Access Account. A more flexible approach to Identity & Access Management could give these employees limited access, early on in the hiring process, to allow for the election of benefits and for expeditious processing for Penn State and our benefits administrators (Highmark Blue Shield, SERS, TIAA-CREF, etc.)

Terminated Faculty Member Maintains Access - A faculty member leaves the University, but her Access Account continues to be active for several months after her employment has been terminated. Local system administrators are not notified of her departure and because her Access Account is active, she continues to have access to sensitive University data for a significant period of time—even though she is no longer working for her department. Maintaining identity information, and related status changes, in an integrated central person registry would allow for the automated de-provisioning of access as soon as the employee was terminated.

Physicians at the Hershey Medical Center and Access to Library Resources - Doctors at the Hershey Medical Center Cancer Institute would benefit from access to the electronic databases provided through University Libraries. These doctors are not Penn State University faculty, staff, or students—even thought they are working with Penn State researchers. They are denied access because providing this service would require full-fledged Access Accounts that would grant them access to other resources--in violation of some of our content licenses. This "all or nothing" approach to access in the Libraries is not meeting the needs of our diverse constituents. A more flexible approach to Identity & Access Management--one that takes into account many different types of affiliates, and their related needs for online resources, could address this issue.

Patients, Family Members, and Visitors at the Penn State Hershey Medical Center – People of all ages and backgrounds depend upon the public internet as critical means of communication. While someone suffering from a debilitating illness and/or injury may have much on their mind, it is not unreasonable to think that they have needs to stay in touch with friends, colleagues, classmates and/or employers via the internet. Particularly where prolonged or repeated stays are involved, HMC/COM guest access to the public internet is pivotal to staying informed and keeping others informed. Today's processes, for provisioning access for these customers and accommodating their needs, are manual and resource intensive.

Parents and guardians of young children are integral to the care and well-being of the patient. Having to choose between leaving the bedside of a loved one, even momentarily, to stay in touch with others (including employers) is a heart wrenching decision. Staff members in the Penn State Children's Hospital and Penn State Cancer know first hand that guest access to the internet (for family members of acutely ill patients) is of paramount importance.

Long-term patients, who are also students, are entitled to special education accommodations in order to maintain and grow their knowledge. Increasingly school districts are relying upon electronic information and systems to enrich and facilitate student's education, to maintain documentation, and report grades. Consequently, Intermediate Unit staff request HMC/COM guest internet access privileges to service their students.

In the near future guest access needs will arise in areas such as: Kidney Dialysis, Chemotherapy and other day-long procedure suites. Looking ahead to the future of healthcare, one can foresee the day where patients and/or loved one's play an increasingly important role in the delivery of care; perhaps even to the extent of having limited, real time, access to the patients electronic medical record. A comprehensive strategy for Identity and Access Management will help meet these current and future needs and reduce current administrative burdens for providing access.

Alumni Donors - A few key alumni donors have been granted Access Accounts in order to better serve in key volunteer roles for the Alumni Society. Recently, standard account notification processes, have sent out email notices requiring them to pay for the accounts to keep them active--despite the fact they have donated millions of dollars to Penn State. These are all major donors to the university and have supported the university with scholarships and endowments. These donors are among key volunteer structure and will likely be making additional major gifts to Penn State in the future. Identity and Access Management is needed to more seamlessly incorporate alumni into the Penn State community providing key donor volunteers with the access they need and deserve.

Alumni Association - The Alumni Association has an online directory and offers services such as email forwarding, career services, and access to library resources. Currently each service requires a separate user id and password, with no ability to maintain a single account. A comprehensive Identity and Access Management solution will reduce administrative efforts and costs related to multiple identifiers, as well as improve the online experiences for our alumni.

Local Community Member and Short Term Access Accounts - A local community member comes into the Accounts Office and asks for a Short Term Access Account (STA) for forty-five days to do research. Forty-six days later, they come in and get another (STA). This cycle can repeat again and again with the University, in essence, becoming their Internet Service Provider. Current policy does not prohibit this from happening.

Registrar Relationships - Students need to authorize others to have access to their educational records for various purposes. For example, a parent may be granted access to the student's bill and/or bursar account for payment purposes. In addition, a student may grant the parent access to their enrollment verification and/or grade report. Parents need authenticated but limited access to Penn State secure services as they relate to their student.

Student Lifecycle - Students represent the largest percent of our user community and the largest number of consumers of University online services. Currently Penn State provides services to and creates a relationship with prospective students before they make the decision to become a registered Penn State student. An individual who subsequently applies to the University and is accepted becomes a student and receives a Penn State Access Account which then provides them access to many services. The Access Account is deactivated six months after the student graduates or leaves the university making, it difficult to maintain a relationship with the student. The need to provide authenticated and authorized access to services extends beyond the current lifetime of the Penn State Access Account, with the need to allow former students to request transcripts, acquire career services, and repay student loans.

New Students Applying for Admissions - A new student applies for admissions online using an Access Account granted while taking a course as a non-degree student. After course completion the Access Account is deactivated and the student can no longer access MyPennState to check the status of the application, receive the decision, or accept the offer of admission. This citation would often result in the student creating an FPS account and cumbersome intervention by staff to allow proper access to services. A more integrated approach to Identity & Access Management would allow for a more seamless transition and the use of a single account for the student's entire lifetime of interaction with Penn State.

Provision of Access to Course Work For Students at a Distance - Currently, it can take a distance learner anywhere from 7 to 10 days to get his Access Account activated, and to become fully authorized for other required electronic services to access his Penn State coursework. This is especially problematic for new students during the latter phase of the start of a semester, when changes to course scheduling may require student access to additional courses/resources which may already be underway, putting that student at a disadvantage. While resident students may be able to sit in on class lectures as they are awaiting the "red-tape" to catch up, the distance student cannot join in class participation because he cannot access the ANGEL course information until all of the system provisioning processes are completed. This lengthy setup process shows how various systems within the University will benefit from an improved identity and access management system, which will shorten the timeframe of granting full access to systems. We cannot sustain the current process which starts with obtaining the student's enrollment request (a touchpoint for creation of identity

records), proceeds to verification of student credentials, and continues with receipt of signed signature forms from the distance student, which will then be processed using resident student mechanisms. The mail service is part of the distance process, and is used to return the digital id and password to the student, all the while awaiting various overnight batch processing to create student records and class roster information for ANGEL. In the reality of today's world, where a purchase generally buys a consumer immediate access to their new electronic "goods", Penn State must seek to improve this experience for our distance students and for the staff and faculty who serve them.

Library Resources - The library currently provides access to over 10 million dollars worth of electronic journals, books, and databases. Penn State students, faculty and staff can access these resources if they have an Access Account. No Access Account means no access. But what about the researcher who is working with a Penn State Faculty member? He or she may need access for a short period of time while they're working on an article together or checking citations. Currently, we have no way of accommodating that need; it's all or nothing. Or what about the doctor that is being flown in to work on a case and wants to double check something that was in a medical resource that is provided through the library. Since the physician doesn't work for Penn State and doesn't have an access account, he or she would not have access to journals provided by the library. Our current system is not granular enough to allow for these types of situations.

Appendix B – Glossary of Terms

Affiliation - is defined as the combination of: A relationship with Penn State (that could allow access to electronic services) and some form of TRUSTED (might not be PSU) identity

- - Are relationships with Penn State + Some form of trusted identity. - Are not roles. - Never are deleted. - Can have zero, one or many active relationships. Zero occurs if all relationships have been deactivated. - Are active if they have one or more active relationships. - Have a single “dominant” relationship when the affiliation is active.

Identity and Access Management (IAM) - is defined as an administrative process coupled with a technological solution which validates the identity of individuals and allows owners of data, applications, and systems to either maintain centrally or distribute responsibility for granting access to their respective resources to anyone participating within the IAM framework.

Information Owner - Defined, as it pertains to PSU, as the organizational unit responsible for making classification and control decisions regarding use of information. These Information Owners would assign the trust levels based on the sensitivity of the information and nature of the transactions performed on the information.

Level of Assurance (LoA) - The degree of confidence in the vetting and proofing processes used to establish the identity of the individual to who the credential was issued. As well as the degree of confidence that the individual who uses the credential is the individual to who the credential was issued.

Relationships - Identify how an entity touches (the context) the University.

- Not roles but establish the context in which the roles “operate.” - Can be deactivated and reactivated. - Are like tags from a controlled vocabulary. - Have attributes to further define context. For instance, where the relationship touches the University, as in (but not limited to) a college, department or administrative unit. Attributes derive from a controlled vocabulary.

Reasons to create a relationship

- Distinguish between groups that have significant difference in access rights. - Try to eliminate relationships with few members.

Trust level classification - Process by which the Information Owner assesses the risks, potential impacts and required trust level to adequately maintain the privacy and security of the information and reduce risk inherent in the transaction.

Vetting - The process of the acquisition of data about someone. To the extent that we get second party validation of the information is now being viewed as proofing. So our working definitions have evolved such that Vetting and Proofing are not distinct or separable processes.

Appendix C – Identity & Access Management Committee and Sub-Committee Team Members

Renee Shuey, Information Technology Services (ITS)
co-committee chair and chair of Levels of Assurance sub-committee
rshuey@psu.edu

Joel Weidner, Auxiliary and Business Services
co-committee chair
jlw2@psu.edu

Masume Assaf, International Programs
Vetting, Proofing, and Registration Authorities sub-committee
Levels of Assurance sub-committee
mxa3@psu.edu

Jackie Babcock, Office of the University Bursar
Levels of Assurance sub-committee
jkg1@psu.edu

Scott Bitner, Office of the University Bursar
Levels of Assurance sub-committee
smb5@psu.edu

Chris Brown, The Graduate School
Life Cycles & Affiliations sub-committee
cab4@psu.edu

Jeff Campbell, Penn State Milton S. Hershey Medical Center
Risk Assessment sub-committee
jcampbell3@hmc.psu.edu

Sean Costella, Auxiliary & Business Services
Life Cycles & Affiliations sub-committee
spc1@psu.edu

Ken Forstmeier, Office of Sponsored Programs
Leader of Life Cycles & Affiliations sub-committee
kgf1@psu.edu

Lisa German, University Libraries
Governance & Policy sub-committee
lbg10@psu.edu

John Gorman, Penn State Great Valley
Governance & Policy sub-committee
Risk Assessment sub-committee
jxg32@psu.edu

Gary Grgurich, Internal Audit
Risk Assessment sub-committee
gig13@psu.edu

Tom Irwin, Commonwealth Campus
Vetting, Proofing, and Registration Authorities sub-committee
tri2@psu.edu

Cindy Kellerman, Auxiliary & Business Services
Vetting, Proofing, and Registration Authorities sub-committee
cqk2@psu.edu

Steve Kellogg, Information Technology Services (ITS)
Leader of Vetting, Proofing, and Registration Authorities sub-committee
Levels of Assurance sub-committee
kellogg@psu.edu

Kathy Kimball, Information Technology Services (ITS)
Governance & Policy sub-committee
Risk Assessment group
krk5@psu.edu

Linda Klimczyk, University Libraries
Vetting, Proofing, and Registration Authorities sub-committeel
lgk1@psu.edu

David Lindstrom, Office of the Corporate Controller
Leader of Risk Assessment sub-committee
djl6@psu.edu

Deb Meder, Office of the Corporate Controller
Leader of Governance & Policy sub-committee
dmm4@psu.edu

Marta Miguel, Information Technology Services (ITS)
Life Cycles & Affiliations sub-committee
Levels of Assurance sub-committee
mam58@psu.edu

Jerry Mihaly, Information Technology Services (ITS)
Vetting, Proofing, and Registration Authorities sub-committee
jsm@psu.edu

Lorraina Miles, Office of the Corporate Controller
Risk Assessment sub-committee
lxh8@ **psu.edu**

Frank Miller, Office of the University Registrar Penn State York
Life Cycles & Affiliations sub-committee
fpm1@psu.edu

Tom Moore, Development and Alumni Relations
Life Cycles & Affiliations sub-committee
tam1@psu.edu

Greg Myford, Intercollegiate Athletics
gjm14@psu.edu

Donna Neideigh, Office of the Corporate Controller
djn1@psu.edu

Janice Pearce, Office of the Corporate Controller
Governance & Policy sub-committee
jaw2@psu.edu

Bob Quinn, Office of Student Aid
Risk Assessment sub-committee
req1@psu.edu

Karen Schultz, Office of the University Registrar
Governance & Policy sub-committee
kls2@psu.edu

Steve Selfe, Office of Human Resources
Vetting, Proofing, and Registration Authorities sub-committee
srs1@psu.edu

Cheryl Seybold, Outreach and Cooperative Extension
Life Cycles & Affiliations sub-committee
Levels of Assurance sub-committee
cys1@psu.edu

Steve Shala, College of Agricultural Sciences
Risk Assessment sub-committee
sas127@psu.edu

Steve Shelow, University Police Services
shelow@police.psu.edu

Jim Smith, Office of the Physical Plant
Vetting, Proofing, and Registration Authorities sub-committee
jas4@psu.edu

Vince Timbers, Undergraduate Admissions Office
Life Cycles & Affiliations sub-committee
Levels of Assurance sub-committee
vlt@psu.edu

Neal Vines, College of Agricultural Sciences
Vetting, Proofing, and Registration Authorities sub-committee
ntv1@psu.edu

Jim Vuccolo, Information Technology Services (ITS)
Life Cycles & Affiliations sub-committee
jvuccolo@psu.edu

Michelle Weaver, Materials Research Institute
Life Cycles & Affiliations sub-committee
mzw4@psu.edu

Matt Weber, Penn State Milton S. Hershey Medical Center
Governance & Policy sub-committee
mweber@hmc.psu.edu

Eric White, Undergraduate Education
erw2@psu.edu