Identity and Access Management At Northwestern University

Working Group Report

August 29, 2014

Working Group Membership

James Rich	Kellogg School of Management
Michael Satut	The Graduate School
Ken Woo	School of Continuing Studies
Kirsten Yehl	Feinberg School of Medicine
Stu Baker	Northwestern University Library
Serena Christian	Finance, Facilities, and Research Administration
Kristin McLean	Human Resources
Jody Reeme	Student Enterprise Systems
Tom Board	NUIT
David Keown	NUIT
Phil Tracy	NUIT

Executive Summary

The Context

The Northwestern University NetID management system was launched in 1993 to support electronic mail services. This marked the beginning of our Identity and Access Management (IAM) system as we have come to know it. (An IAM system is a set of applications, policies, and processes by which electronic identities and credentials are managed over their lifecycles, and the mechanisms by which business applications utilize that system to make decisions about permitting (or denying) access to their online services and resources.) Over the past twenty years, the majority of the electronic services within the University have adopted the NetID as their user identifier and authentication credential. This level of adoption has clearly benefited the University's ability to introduce new services in a relatively coordinated fashion.

During this time, the University's IAM infrastructure has grown organically without ever having benefitted from a systematic review of its functionality or how it aligns with the business needs of Northwestern. The decision to pause for a comprehensive review of this evolving and increasingly critical area was driven by multiple factors:

- the product "end of life" for the core Identity Management application (NUValidate)
- the growing importance of IAM functionality
- the frustration by the IT@NU community with the functional short-comings in this area
- the difficulty in maintaining the current, fragmented suite of systems

The University's IAM system is the primary hub of our ever-growing portfolio of online services that support a changing Northwestern community, and the context for this set of functionalities has changed qualitatively, particularly in the last 5-10 years. The community for which these identities are managed, and access decisions are made, is very different:

1. the University is entering into more partnership and affiliate agreements with external institutions;
2. the geographic scope of Northwestern is becoming increasingly distributed;
3. collaboration with people outside of the traditional boundaries of Northwestern is "the new normal";
4. there is an increasing interest in expanding the range of years during which the University maintains a relationship with "members of the Northwestern community", e.g., with talented and interested youth well in advance of the time they might apply to Northwestern, to people well past their young-adult student or even working days.

Concurrently, there has been a qualitative shift in technology. With the growth of online services and the rise of cloud computing, transactions and services need to happen online on a real-time basis, and the interaction of systems and the management of identities needs to happen "at scale" on a "hands off" basis.

The Path Forward

A cross-organizational working group (whose members are listed on the cover page) was formed in the fall of 2012 to compile a broad sampling of the IAM needs across the Northwestern community, and to recommend a path forward. One clear conclusion of this information gathering is that a reliance on episodic, just-in-time responses to changing circumstances has left the IAM system undervalued, and thus underinvested in, leaving it insufficient for the University's current and future needs. This insufficiency does not manifest itself in a big-bang, highly noticeable manner; the effects are felt repeatedly throughout the enterprise in user frustration, delays in getting new systems integrated and online, and staff time routinely wasted working around the system's deficiencies. Our IAM system is perhaps our most valuable enterprise system, enabling all of our online services, and it needs to be restructured and repositioned.

The degree of change that is needed to accommodate the trends listed above goes beyond isolated adjustments to one part of the system or another. The vision laid out in this document is designed to lead to an IAM system that will return much higher value for the University by being more integrated within itself, more integrated on a real-time basis with the applications that surround and depend on it, more secure where it needs to be, and more extensible and flexible via federated identities.

The report's recommendations are organized into three sections, each of which includes suggested changes based on key architectural cornerstones:

- The Identity Management System's (IdM) integration within itself needs to be improved via simplification and consolidation. Some of this work needs to be done as part of the process of replacing NUValidate. Areas connected to this replacement in which change is recommended include the processes for manual NetIDs and WildCARD procurement, the distributed Active Directory structure, and the practice of embedding access management logic within the IdM system.

- The Access Management system needs to be more integrated on a real-time basis with the Identity Management system, moving from a "heads down, internal to each system" process for authorizing access, to a process where online systems are more integrated with the IdM system on a real-time basis, "expose" information outside of their system about individuals' access status within their system so it can be used by other systems, and are "smarter" in the sense that they can make use of a new central registry (much of which will likely be virtual) when making their decisions about authorizing access. The University's new web services infrastructure (Service-Oriented Architecture (SOA)) and a commitment to enterprise web Single Sign-on (SSO) will be key to making these changes.

- The way our IAM system incorporates Identity assurance (the level of confidence that the credential is accurately associated with a real person, and the correct person) and trust (how do we know the person presenting the credential is really the person to whom it was issued) into its processes needs to be optimized vis a vis the resource/service being accessed. In some situations, this will mean the NetID is supplemented by multi-factor authentication during the login process, and in other situations it will mean there will be a reduced reliance on NetIDs via such techniques as Identity federation.

To achieve these goals, the entire IT@NU community will need to be involved. NUIT, distributed IT units, enterprise system development teams, and business application owners will need to be involved. The scope of the technological work should not be underestimated, but these technological changes cannot happen in a vacuum. New business rules and standard processes will have to be envisioned, refined, and adopted in order for the new technology to be selected, implemented, and work effectively.

NUIT's Identity Services team will be a pinch point in this initiative, and the Next Steps section (page 51) highlights work that will involve this team that is recommended for consideration for initial prioritization. Due to NUValidate's end of life status, preliminary envisioning of a new IAM model leads the list in order to know the functionality needed for its replacement. Also included for consideration are other sets of work that are more easily outsourced than the envisioning work is.

This is a long report that attempts to cover a very complicated topic with a lot of misunderstanding attached to it. Several of the Appendices are included to help its digestion, e.g., Appendix B (page 58) is a quick reference guide to the report, Appendix C (page 62) details the work called out or implied in the report, and Appendix D (page 67) includes annotated workflows on how the IAM system at Northwestern functions.

We hope we have articulated the need for change and have provided not only a beginning point for that change, but also a roadmap to be pursued over time in order to take advantage of different technological possibilities and keep pace with the University's changing environment and business aspirations.

I. Introduction

What is Identity and Access Management?

Two very similar acronyms will be used in this report: **IdM** and **IAM**. IdM stands for Identity Management, which is a subset of IAM, or Identity *and Access* Management. The two sets of functionality – the management of identities and the management of access - are obviously very tightly connected, and they are often mistakenly conflated.

Identity Management (IdM) encompasses the maintenance tasks associated with the lifecycle of electronic identities: provisioning, de-provisioning, and handling changes in between. The IdM system also makes those identities, and a set of attributes for each identity, available via published directories, which can be used by surrounding applications to *authenticate* a person's credentials at the time of requested access and receive attributes about that person in return.

Access Management (the **"AM"** in **IAM**) encompasses the tasks associated with providing access to resources once a person's credentials have been authenticated. The identity management system makes no decisions about access to surrounding applications, only about the verification of credentials. The applications are, or should be, responsible for defining the business rules that *authorize* people's access to resources (e.g., read/create/update/delete data, gain access to a building) and implementing those rules based on personal attributes associated with an electronic identity. Together, these two sets of functionality – authentication and authorization - comprise **IAM – Identity and Access Management**.

(See Appendix A on page 56 for a Glossary of Terms used in this report.)

Context for the IAM Working Group and the Following Report

Northwestern's Identity and Access Management infrastructure has grown organically over the last twenty years without ever having benefitted from a systematic review of its functionality or how it aligns with the business needs of Northwestern. The decision to pause for a comprehensive review of this evolving and increasingly critical area was driven by multiple factors:

1. the difficulty in maintaining the current, fragmented suite of systems;
2. the frustration expressed by the IT@NU community with the functional short-comings in this area;
3. the growing importance of IAM functionality;
4. the product "end of life" for the hub of the IAM system: NUValidate.

A special note is due regarding the status of NUValidate. In 2011, following Oracle's purchase of SUN, the identity management product was declared "end of life" and is no longer fully supported. We still retain a perpetual license to run the software, but there is some risk to this situation. The risk level is thought to be "low" to "medium low" because the software has been running for years without an incident, it is not widely deployed, and steps have been taken to reduce or eliminate storage of sensitive data in the system wherever possible. However, the status quo is not where we want to be, and the lack of ongoing vendor support is ultimately not tenable. Knowing that a system must be replaced makes it much less attractive to do further development and customization, which (a) will have to be re-done when the system is replaced and (b) reduces resources available for the replacement. This limits what can be done in the system to support other initiatives important to the University.

A cross-organizational working group (whose members are listed on the cover page) was formed in the fall of 2012 to compile a broad sampling of the IAM needs across the Northwestern community. That work was completed in the late spring of 2013, and work was begun on a summary report. The completion of this report

has been delayed by other studies which now inform this report: the working group reports on “Enterprise Content and Business Process Management”, and “A New Vision for Research Administrative Systems”.

Because the topic, and the research undertaken by the group is so broad, there are undoubtedly some omissions, oversights, and probably even some misstatements in the paper. For these we apologize in advance. Similarly, the focus groups were completed between November 2012 and April 2013. Time has passed since then, and some important work has taken place in the interim, e.g., iBuyNU is now enabled with the enterprise web Single Sign-on environment and very important work has been on-going at the Feinberg School of Medicine and Northwestern Medicine, and the authors of the report have not tried to cycle back with people to fully incorporate these developments.

Despite these caveats, we firmly believe we have captured the important details and the essence of IAM across the University, and there is no intent to make this into a living document. Instead, the intent is to grow the awareness of this critical area within the institution, and to engage the community in a discussion about repositioning this system in our IT portfolio.

Finally, it should be noted that once the focus groups were completed, the tasks of reviewing, congealing, and presenting the raw data necessarily had to narrow down to a smaller set of people, and these tasks became the responsibility of the NUIT representatives on the committee. Once a version of the report that was close to its publishable form was completed, the full working group was asked to provide feedback on the report. The members of the working group outside of NUIT dedicated many hours of effort and insight to this project, and the report has benefitted greatly for their commitment. Whatever the shortcomings there are in the report, the primary authors within NUIT take full responsibility for them.

Organization of the Report

The first half of the report is its main body, which covers three general areas:

- **Section II** provides a brief historical perspective on IAM at Northwestern
- **Sections III, IV, and V** provide reviews of our current situation. Section III focuses on IAM within the University. Sections IV and V look at approaches to IAM outside of Northwestern, e.g. Big 10 schools, vendors, industry analysts.
- **Sections VI and VII** look at the recommended path forward. Section VI describes the path, and section VII has a brief synopsis of the work to be done.

The second half of the report is a series of Appendices, that provide reference material or more detailed versions of material summarized in the report:

- A: A Glossary of Terms used in the report.
- B: A “Quick Reference Guide” summarizing the key points of the report.
- C: A Summary Listing of the sets of work included in the IAM Report.
- D: Overviews on The Northwestern IAM System, including two annotated flowcharts: one showing how data flows to and within the University’s IdM system, and the other showing “IAM in Action”, i.e. the role that each part of the system plays when someone tries to log in to a Northwestern University system.
- E: Overviews of the On-boarding and Off-boarding Processes
- F: The details from the 24 focus groups that were held, including a summary of the 23 themes distilled from the focus group results, and the notes from each focus group that gave rise to those themes).

Because of the report's length, it's recommended that you start with the Appendix B "Quick Reference Guide" to help guide you through the report.

II. The Changing Context for IAM

The Evolution of IAM at Northwestern

The first identity and access management (IAM) system at Northwestern was developed internally in 1993 to save labor in establishing email accounts and to support authentication through the University's modem pools. The SNAP system (Simple Network Account Program) received feeds from the HR and Student systems to create a combined census of who had rights to the services, and allowed administrators to "activate" the service for a requester. These credentials were removed from the services when the person was no longer presented in either of the incoming data feeds.

Relative to the requirements today, the problem solved by the original deployment of SNAP was quite limited in scope, the community served was relatively small, and the application required only the most primitive expressions of the relationship between the person and the University. Since then, the use of NetIDs has expanded greatly to include the core "systems of record" (SES, FASIS, and NUFinancials), scores of other University applications (Blackboard, InfoEd, FAMIS, etc.), and many local applications in the schools.

As the growth of administrative systems increased, and the NetID spread to become the primary online identity credential, the variety of different situations requiring different ways of deciding whether or not to provide access to a person was growing as well. Rather than changing the role of the applications in this IAM relationship, the relation was left unchanged:

- the business applications still only expected a Y/N response to the authorization query about whether the NetID was active;
- the applications still only made a Y/N access decision on the result of that response;
- business rules within the SNAP system, previously coded for the relatively simple original email application space, kept getting built out.

As a result, the SNAP system became crisscrossed with special-cases, becoming increasingly difficult to modify to incorporate the next case presented. Replacing the homegrown SNAP system with a commercial product in 2010, now called NUValidate, improved certain support efficiencies and addressed certain IAM system usability problems, but it did not address this tangled web of business logic.

The growth of the number of online systems, their increasing complexity, and their need to manage access to their functionality were reflected in changes to the IAM environment beyond just the increasingly tangled web of business logic within NUValidate. For instance, the increasing use of online services across the University led to the need to provide access to people who were not included, or not yet included, in the HR and Student systems. To address this need, the ability to create "manual" NetIDs outside the normal matriculation/hiring processes was introduced along with the ability for a set of designated people in each school and administrative division to create these "manually-asserted" NetIDs. Also, despite the central University's decision to not actively participate in the provisioning of Microsoft's IAM product, Active Directory, schools and other business units began investing in more and more Microsoft products that assumed its existence, and as a result, a solution was devised to replicate NetIDs to these independent Active Directory "domains".

Today's IAM "System"

The IAM "system" at Northwestern today is not a single system, as, for example, one might think of an admissions system. Rather, it is a collection of applications:

1. **a core Identity Management (IdM) system** (NUValidate), which stores identities based on NetIDs that are in turn based on data fed primarily from authoritative identity sources such as the Faculty and Staff Information System (FASIS) and the Student Enterprise System (SES), allows people to manage those identities, and updates Northwestern's identity directories;

2. **identity directories** (e.g., LDAP, Active Directory, and Kerberos), which surrounding business applications use to authenticate users requesting access to their system;

3. **a physical identity system** (the WildCARD system), which provides proof of identity for access to buildings, events, etc.;

4. **a directory synchronization utility** (Radiant Logic), which keeps data in multiple active directory domains synchronized;

5. **a web Single Sign-on system** (SSO), which reduces the need to keep logging in with the same credentials for each Northwestern University application that is used;

6. **federation services** (e.g., Shibboleth), which allow people at trusted affiliate, partner, or peer institutions to use their home institution's credentials to gain access to Northwestern systems and services;

7. **a multi-factor authentication service**, which provides an extra layer of password protection using an application on a registered smart phone or answering a phone call to reduce the risk that personal information can be easily compromised should someone learn a NetID password;

8. **an "Identity Provider" bridge service** (currently being run by the Alumni and Development Enterprise Applications team for the OurNorthwestern system), which enables alumni to log in with either an active Northwestern identity or with one of their own external social accounts (Gmail, Yahoo, Microsoft).

See the section on "IAM in Action" in Appendix D (page 71) for a diagram and description of how these parts work together to provide IAM functionality when a person tries to log in to a Northwestern application. Appendix D also has an annotated diagram that shows how data flows within the IAM system (page 68).

The Increasing Importance of IAM in Today's World

These changes in the parts and complexity of the IAM system, and the surrounding web of applications it enables, reflect the changing nature of the world in which we live, which has obviously changed greatly since the time when the vexing problems to be solved were facilitating access to University email and the modem pool.

- Online services offered by the University are qualitatively greater in both number and complexity, and more parts of the daily activities on the University community are premised on easy access to these services.

- More and more services are increasingly being offered off-campus from the cloud, and maintaining control over identity-related information/attributes is increasingly important in the face of increasing security threats and the increased regulations they engender.

- As services become available outside of proprietary systems and through web services, services and data are expected to be available for self-service in real-time, and integrated with one another.

- The "Northwestern community" is growing and becoming more complex as:

    - the University enters into more partnership and affiliate agreements with external institutions;

    - the geographic scope of Northwestern becomes increasingly distributed geographically (e.g., other cities in the U.S., Qatar, partnerships with international schools around the globe, and the global spread of research engagements and student learning experiences);

    - collaboration with people outside of the traditional boundaries of "Northwestern" becomes "the new normal" (e.g., fellow researchers at other institutions, consortiums of universities offering courses, peer administrators at other institutions, practitioners outside the University, community engagement);

    - interest grows in expanding the range of years during which the University maintains a relationship with "members of the Northwestern community" (from earlier in life -- youth and young adults participating in University programs such as the Center for Talent Development or the National High School Institute program -- to later in life, via alumni programs and life-long learning).

As these trends continue, the IAM system will need to handle a wider variety of situations, offer more options, depend less on physical proximity, and be flexible enough to be deployed quickly and effectively "at scale" so it does not become the bottleneck for the deployment of new services, but also does not become an increased risk for compromise. In this sense, the IAM system has become one of the University's most important systems.

III. An Assessment of Northwestern's Current IAM Environment

A Note on Northwestern Medicine

Before beginning on this analysis, a special note on the situation at Northwestern Medicine is in order. The separate but inextricably intertwined relationship of the Feinberg School of Medicine, Northwestern Memorial Hospital, and the Northwestern Memorial Faculty Foundation has led to an IAM situation that is particularly complex. The intertwining of these institutions creates an enhanced set of IAM challenges – for example, hospitals want more stringent standards around identity and access management policies and procedures, and budgets, policies, and resources are the responsibility of three mostly independent organizations, yet the doctors, researchers, and the administrators need to work fluidly across the organizational silos and resource redundancies -- and undoubtedly, there are places in this report where those challenges could have been better highlighted.

In the intervening time between the publication of this report and its beginning in 2012, significant work has been engaged on these fronts within Northwestern Medicine and with the University as a whole. Suffice it to say, that being a part of that work is a high priority of any plan for making progress within IAM at the University.

Attributes of a Highly-functioning IAM System

A highly functioning identity and access management system is typified by these nine characteristics:

1. Each person has a single electronic identity. There may be multiple credentials attached to that identity, but there is only one electronic identity.

2. The IdM infrastructure is integrated within itself, so that data about identities and personal attributes flows smoothly throughout the system.

3. Identities and access to resources are provisioned and de-provisioned rapidly in alignment with the need for their actual usage, with easily auditable trails.

4. Authorization is appropriately granular and based on robust identity information.

5. Surrounding business applications are integrated with the enterprise IdM system.

6. The level of rigor employed in identity proofing and authentication at the time of access is based on the risk and value of the transactions to be done.

7. Identities are protected and secure.

8. Each part of the IAM system is relatively easy to maintain and to replace.

9. Business applications and the IAM infrastructure are flexible and easily modified to take advantage of new IAM technologies as they emerge and become stable.

The following section gives an assessment of the Northwestern IAM system for each of these characteristics.

An Assessment of the Northwestern IAM System

As already mentioned, Northwestern's IAM system provides a wide range of functionality, and for the most part, it handles basic IAM functionality across the identity lifecycle for the traditional core constituencies of on-campus faculty, staff, and students. But there are stress points in each of the characteristics listed above, many of which are being aggravated as the world changes around us.

1. Each person has a single electronic identity. There may be multiple credentials attached to that identity, but there should be only one electronic identity.

One of the core tenets of Identity Management was a fundamental premise of multiple focus groups: individuals should have one electronic identity at Northwestern. The first aspect of being able to provide the correct information about a person, and being able to accurately provide access to resources, is being able to correctly match an identity with a person and their attribute data. To do this effectively, there has to be a unique identifier for each person. Duplicate IDs or separate IDs for access to different sets of services were each seen in the focus groups as barriers to many important goals: customer service, administrative efficiency, foundational information security, and integrated reporting. There is great value to be realized by applying effort on the front end of the identity management lifecycle to avoid issues in these areas later on.

At Northwestern, there is a basic adherence to this premise. There is widespread adoption of the NetID as the primary electronic identity at the University. These identities are rarely reused -- the only exceptions are NetIDs that were assigned to organizations (e.g., "chemistry department") for email and directory-listing purposes, and NetIDs used as 1-day library walk-in patron NetIDs – but all others are kept forever and are never re-used, and they are propagated across the enterprise's large number of Active Directory "domains". (A "domain" is a logical container within a directory that allows for the management of a set of accounts -- i.e., people -- and devices -- e.g., printers, computers -- via a single directory service.)

However, the NetID is not the only enterprise identifier at Northwestern. There are also WildCARD barcodes, and EMPLIDs in FASIS and SES. (An "EMPLID" is an "employee ID", which is the unique key for a person in both FASIS and SES. If a person is both an employee and a student, their EMPLID in each system should match.)

Although any one person should never have more than one of each of these, duplicates do creep into the system in multiple ways as shown in the next section.

In addition, there are some system-specific identities at Northwestern. While the NetID, with its associated password credential, has been widely adopted as the default means of authenticating to a Northwestern system, there are still multiple systems that do not utilize the University's identity management system. Examples mentioned during the focus groups include: iBuyNU (since corrected), the I-9 Service Center, Galter Library, multiple systems for alumni that are not tied together, McCormick systems that grant students access to Microsoft products for their classwork, Quest login (UNIX ID), HR Benefit Systems (e.g. FSA), Vista, ProCard, FundDriver, CBORD (cashless card system utilized by University Services for "Munch Money"). All of these identities have different username and password conventions, and different frequencies for password changes.

Northwestern's online alumni community system used to be by far the largest system using its own unique, non-NetID Northwestern identity. Now, however, the use of Google IDs for most students in the University has almost entirely eliminated this issue for recent graduates because very few of them choose to switch at graduation to a new Google account with "alumni" in the address, and Our Northwestern's current ability to accept social identities, e.g., Facebook, or a non-Northwestern Google account – has further eroded the need for a system-specific Northwestern identity for alumni.

Interestingly, one of the "exceptions" to a standardization on the NetID is the management of identities with "elevated privileges" within FASIS and SES (but not for NUFinancials). Administrators whose job involves doing more in these systems than simply managing their own information via self-service must apply for a special ID to be used specifically for these purposes. This separate set of IDs is maintained outside the NetID process, by administrators tied to SES or FASIS. Premised on the need for additional external controls on these access permissions, and a concern that the NUIT Help Desk is populated by temporary employees, this practice is unable to take advantage of the benefits afforded by integration with the normal IAM system (e.g., users only having to know one ID/PW, the management of identity lifecycles being less dependent on weekly reports and manual processing), and because it is paper-based, there is no way to easily monitor the process of requesting permissions be added to, or deleted from, an identity. (See also Optimizing Authorization, page 22.)

2. The IdM infrastructure is integrated within itself, so that data about identities and personal attributes flows smoothly throughout the system.

There are many "moving parts" to the IdM system at Northwestern, and data moves between all of them but not without glitches. (See Appendix D, page 68 for a diagram and description of how data flows within Northwestern's IdM system.)

One of the most vexing problems associated with areas of disconnection within the IdM system is the creation of duplicate IDs (NetIDs and/or EMPLIDs). When duplicate IDs are created, they cause all manner of problems downstream with WildCARD, Course Management, payroll, etc. Some duplicates are easier to resolve than others, but most duplicates seem to have their own set of idiosyncrasies, and they often require hours (if not days) of analysis and untangling from a variety of resources on multiple teams - business users, business analysts, developers, etc.

Disconnects Due to Failed Matching with Existing People in FASIS/SES

There are multiple ways duplicate identity credentials/identifiers can be created at Northwestern due to limitations in the identity-creation processes within the two systems of record – FASIS and SES – and within the Manual NetID process. Logically speaking, there are six ways a duplicate NetID can be created. Three of these

are related to manually-asserted NetIDs, which are discussed in the next section. The other three situations that can lead to duplicate credentials/identifiers occur within FASIS and SES:

1. *Failure by FASIS to match a newly-employed person with their existing student record in SES (duplicate EMPLIDs and NetIDs created)*
2. *Failure by SES or Admissions systems to match newly-applied/enrolled persons with their existing employment records in FASIS (duplicate EMPLIDs and NetIDs created)*

FASIS and SES have algorithms, run as part of the creation of a record for a new person, which check against other existing records in their own system to guard against duplicate EMPLIDs or NetIDs being created. In order to verify a pre-existing record, the following fields are used in varying combinations that have varying levels of certainty attached to them: name, gender, DOB, SSN, citizenship, address, email. Missing information, typos, name changes, non-domestic names reversed by mistake, dates of birth entered incorrectly because of international differences in the order of m/d/y, multiple passport IDs, and gender changes can all cause a match to be overlooked, as can the "dummy SSNs" that are created for international students who do not yet have a SSN.

Clearly, one area where these mistakes can lead to missed matches is with international students. One focus group, for instance, talked about the relatively recent administrative access that had been given to the International Office so they could directly correct personal attribute errors in international student SES records, and how that had made such a difference in keeping this demographic data accurate. The risk of missed matches also goes up when a person has an intermittent relationship with the University – e.g., CTD students, lifelong learners, adjunct faculty, etc.

SES gets a nightly feed of bio/demographical data from faculty and staff in FASIS. However, once a person's data is sent over, only the faculty data is subsequently updated with changes from FASIS. So, for instance, if a staff member comes over in the feed initially with a dummy SSN, if that person decides to take a course later after they have received a real SSN, their SSNs will not match. Payroll, on the other hand, only has access to the Names file in SES, which does not include indicative attributes such as date of birth, SSN, or citizenship, and any additional analysis on their part would require the support of someone.

3. *Failure to internally match "new" students or employees within either SES, Admissions or FASIS systems (duplicate EMPLIDs and NetIDs created*)

This scenario is not uncommon during the admissions process, with either former students applying to grad/professional school, an affiliate becoming a student, or a prospect submitting multiple applications. People also apply for full-time undergrad status after being in Continuing Studies for a while. Duplicates can be created "within" SES in these cases, especially if there has been a significant change in the person's name, citizenship, birth date, or gender. Additionally, students do not need to provide a legal name or SSN, unless they get financial aid. The result is that SES will have two student records, with two different EMPLIDs for the same person.

Duplicates can also occur within FASIS when hiring an affiliate, re-hiring former employees, or giving a current employee a second job. However, because FASIS must collect SSNs and do I-9 verification, finding duplicate records in FASIS is much less common than it is with SES.

Disconnects Due to Extensions of the IdM System

Since its nascent SNAP days, Northwestern's IAM system has been "extended" multiple times to provide valuable new functionality. However, several of these key extensions have been added with limited functionality and integration, which has resulted in a fragmented IAM infrastructure. Three of these

extensions – Manual NetIDs, the WildCARD system, and Microsoft Active Directories – were the genesis of many requests for change in the focus groups.

Manual NetIDs

As stated earlier, because the SNAP system (and its successor, NUValidate) was informed only by FASIS and SES information, a sizable set of people did not have a way to gain access to file shares, the internet, or online resources such as the Library, BlackBoard, or Alumni Relations applications. People who needed a different path to these resources included people with temporary relationships with Northwestern, and people whose relationship with the University fell outside the normal HR employment or student matriculation processes: e.g., affiliates, contractors, Sodexo and Aramark employees, volunteers, summer enrichment program attendees, CTD students, NMFF, NMH, and other medical center staff who work closely with Northwestern, especially with the Feinberg School of Medicine.

The Manual NetID (thus named because these IDs were "manually asserted" by distributed administrators rather than being created as part of the normal hiring/matriculation processes that have multiple identity assertions – e.g., I-9 data, passport numbers, SAT scores, transcripts, recommendation letters -- built into them) was created to provide this alternative path to a Northwestern electronic identity. Unfortunately, the lack of controls placed around this process, and its lack of integration with the rest of the IdM process, can give rise to a set of nagging problems further down the road.

The last three ways duplicate NetIDs can be created are related to the limitations of the Manual NetID process:

4. *Creation of manually-asserted NetIDs for persons with existing FAIS- or SES-asserted identities (duplicate NetIDs created)*

   NUValidate's Manual NetID creation functionality has limited search/match features. You can search for an existing NetID or EMPLID and add a manual assertion to keep it alive beyond termination of employment/enrollment, but when creating a new NetID, none of the standard search/matching is available (e.g., by name), either within the IdM system itself or with SES/FASIS.

5. *Hiring an employee, or enrolling a student, who already has a manually-asserted NetID (duplicate NetIDs created)*

   There is no protection against this because the batch processing of FASIS/SES data matches only on EMPLIDs and SSNs, and manually asserted NetIDs have neither of these.

6. *Creation of multiple manually-asserted NetIDs (duplicate NetIDs created)*

   This is often a case of poor recordkeeping or lack of coordination within a school or business unit. Because the Manual NetID functionality has such limited search/match capability, the ability to avoid creating a second manually-asserted NetID is dependent on the information that is available to the person creating the NetID. The creation process can match on EMPLID or NetID if the person's current EMPLID/NetID is known and used by the NetID administrator. If they don't have this information, for whatever reason, a duplicate NetID will be created for someone who already has one.

Each pathway to duplicate NetIDs presents its own challenges. For example, if a student is hired as an employee and a set of duplicate NetIDs / EMPLIDs is created, she will have to use one NetID for all of her coursework, and the other for entering her time in Kronos. That creates obvious confusion for the end user herself, and for other people who depend on that person being represented by one identity (uncorrelated data in reports, two Online Directory listings with different info, official notices going to two separate email accounts, etc.). It also creates a burden on the administrators who need to remediate these duplicates because it's difficult to "move" privileges or resources from the old NetID to the new NetID. There are no tools

to merge records in the enterprise systems or the Identity Management system, so most, if not all, things need to be moved manually, and there is no one-stop shopping; each system must be handled individually, e.g., Exchange mailbox, email address, NU Financials privileges, Blackboard courses, etc. The fifth use case – hiring an employee or enrolling a student who already has a manually-asserted NetID is probably the most difficult case to address, requiring coordinating multiple manual operations within the same business day.

The Manual NetID is also problematic because there is so little contextual information captured when it is created (about the person, the reason for the identity creation, or the person responsible for the identity), it is hard to manage it during its lifecycle. This lack of contextual information makes these identities more likely to linger past the time the access is needed and appropriate, and makes troubleshooting any identity and access problems difficult.

Over the years, these problems have been compounded as the Manual NetID process has come to be seen, despite the problems it created for the identity-owner or the administrators having to sort it out later, as an expeditious tool to give people who go through the normal HR hiring or student matriculation processes access to online resources before or after the access provided by the normal processes. For example:

1. Faculty and graduate students sometimes need early access to systems in order to support grant applications or work in Blackboard. (New hires can now be entered up to 90 days in advance of their actual hire date, and adjunct faculty can be hired on an annual basis but only activated for the quarters in which they actually teach, but not everyone knows about these processes.)

2. Contract/temporary employees are issued affiliate NetIDs. If they are "converted" to a full-time NU position, they are then issued a new NetID.

3. Staff at NMFF/NMH who need access to NUFinancials and other systems.

In other words, the creation of the Manual NetID system addressed an acute problem, but in the process of doing so, it turned the acute pain into a less noticeable aggravation, and the diffusion of the pain took the urgency away from the need to remediate the root problems.

The WildCARD provisioning system

While the NetID is the primary electronic identity at Northwestern, the WildCARD system represents a second separate identity management environment that issues a physical credential with attributes recorded upon it. The WildCARD system is similar to NUValidate in that it receives its own data from both FASIS and SES to create most WildCARDs, and then that data is supplemented by the ability to create "manual" WildCARDs for people not within the primary "systems of record" (e.g., for alumni or spouses wishing library privileges, or spouses who would like to be able to get WildCARD discounts).

The separation of WildCARD from NUValidate causes ongoing confusion. More frequently, community interest is expressed in why there is not more integration between these systems. For instance, WildCARDs do not store NetID information in their onboard data cache, and while WildCARDs are used to record attendance at an event or permit access to a building, the systems that store identity information have not contained the WildCARD barcode number. (NOTE: The WildCARD barcode information has recently been added to the attributes stored in LDAP, which makes it retrievable for these purposes along with the already stored NetID and EMPLID.)

Microsoft Active Directories

The main online registry of identities for the University has historically been LDAP, but with the rise of client-server technology in the mid-1990s, and the attendant growth in popularity of Microsoft applications, Microsoft environments ("domains", built around their own independent and proprietary directory, "Active Directory") began to spread through schools and business units across the University. These Microsoft

environments fueled great value across the enterprise as schools and some business units began offering more and more services that were previously unavailable to them, but their implementation introduced a third disconnect within the University's IdM system.

In order to address the need for these two independent identity environments to coexist, two steps were taken. A provisioning process was set up to replicate NetIDs (created in SNAP -- now NUValidate -- and made available to applications via LDAP) out to the Active Directory (AD) domains via a Radiant Logics server that acted as a synchronization utility. In addition, a central University AD domain was created (ADS) but it was a very bare bones directory, and there was no integration with the domains distributed around campus. (There are now twenty Active Directory domains at Northwestern.)

This dilemma of how to deal with two "competing" IdM systems played itself out in enterprises everywhere, with central IT groups making a variety of choices. In many universities, the University would not provide a central Active Directory domain at all until much later. In many cases, if they did provide an AD domain at this point, there was often a complete disconnect between the identities provided by the distributed domains and the identities provided by the University. Faculty, staff, and students in the schools would then have to remember two identities – the University's and the school's – and two passwords, and remember when to use which one.

Northwestern's solution, which was far better than having two distinct identities, is not without its flaws:

1. The Radiant Logic synchronization solution was innovative, but it does not always work properly for this functionality. While NetIDs and their passwords are successfully synchronized across these domains on a daily basis, this infrastructure introduces glitches in the IdM system that have proven impossible to rectify. For instance, people in multiple focus groups referenced the frustration associated with the need for users to change their NetID password as the only known way to fix access permissions that get lost when a person's identity status changes or for a transferred employee to get access to the AD domain in her new department. An upgrade to Radiant Logic is underway, which may address some of these issues, but a tighter integration directly with the IdM system is a better long term strategy.

2. Group memberships and other data are core to providing access to online resources, and this data does not flow easily between the LDAP registry and the AD domains, or between the distributed domains and the central University domain.

    a. Some attributes (e.g. group membership data) are captured in NUValidate and passed to the LDAP directories but do not automatically flow to Active Directory domains, which are the primary directories for managing access to collaboration resources (in which group membership information is so important);

    b. Each unit owning an AD domain implements its own local policies, group definitions, and organizational structures. The unit may also choose to update certain attributes manually, or automatically by connecting to their own internal systems. While this information is sometimes only useful at the local level, at other times the information would be useful at the University level – but the information does not flow back "upstream" to the IdM system, FASIS or anywhere else. Basic demographic and organizational information created and/or stored in local systems can also lead to inconsistencies (e.g., different job titles or addresses in the central vs. school-based AD), uncertainty as to what data is authoritative, and additional work to resolve the inconsistencies.

3. The bulk duplication of NetIDs, passwords and data across multiple AD domains presents added security risks compared to a single, centralized infrastructure; data replicated to twenty different

environments presents twenty opportunities for accidental or intentional security breaches. From a University-wide perspective, duplicate AD infrastructures also have other costs: staff time devoted to replicating AD for each school could be invested in other areas, both within the central identity management team and the distributed IT units who support the distributed AD domains, each AD infrastructure requires redundant infrastructure, and people in schools or business units that have their own AD domain, have to remember to preface their login credential with a different (and often strangely foreign) domain name when trying to use a centralized shared service.

In the early years of this architecture, the limitations associated with it were, if not ideal, at least acceptable. As more services that assume Microsoft's AD environment have been deployed at the University level, this arrangement has become more problematic. The fragmentation of the AD directory infrastructure, its limited integration with the rest of the IdM system, and the relatively undifferentiated group structure in the University level ADS domain limit and complicate deployment of global services that depend on the Microsoft AD infrastructure, e.g. the Microsoft collaboration suite, OnBase or ImageNow, or support tools utilized by IT organizations.

3. Identities and access to resources are provisioned and de-provisioned rapidly in alignment with the need for their actual usage, with easily auditable trails.

In order for online services to fully realize their potential, identities and access permissions need to be provisioned and de-provisioned rapidly to allow "as needed" access to online resources within the defined business process. The speed of provisioning and de-provisioning identities, and the ability to turn access on and off as a result, was flagged repeatedly in the focus groups as being in need of improvement, as was the problems associated with people needing access to resources either before or after their NetIDs were active.

One of the issues related to the speed of provisioning and de-provisioning is that each piece of the IdM system, and each of the surrounding business applications that depend on the IdM system, are like independent islands, connected only by periodic batch shipments of data to update the identity and personal attribute data they store independently. The impact, by definition, is that the currency of identities and identity attributes (and the access that is provisioned on the basis of that data) is always "delayed", resulting for example in lags in gaining access to library privileges, online course materials, or the ability to get your WildCARD.

The speed of the onboarding process, where access to a resource may be dependent on a series of consecutive export/import data transfers was flagged in multiple focus groups as being in need of improvement, particularly at times when normal processing cycles need to be compressed, e.g. late admits right before school starts who need to review financial aid packages, make payments, and get access to course materials very quickly. (The one exception to this approach, which is not without its problems associated with students ending up with multiple NetIDs, was put in place for the School of Continuing Studies due to the nature of their online business. People who want to enroll for a School of Continuing Studies non-degree online course can register and get a NetID in real time, rather than applying and waiting for the process wheels to turn via periodic batch exports/imports.)

The on-boarding process of staff needing access permissions and training in order to use enterprise systems was also flagged as being in need of improvement. One group said it could take weeks for a new employee to get properly positioned to do their job, and it could take weeks for a director level person to get all of their permissions and training. The lack of a "smart" online workflow, which could offer default suggestions for access permissions based on a person's job and could show where the requests stand in the workflow, was also flagged multiple times.

Speed is also a concern when identities and/or access need to be de-provisioned, particularly when access to financial systems or sensitive research is involved; however, the qualifying phrase that was used in this

section's first paragraph – "rapidly … within the defined business process" – is very important. Identities can linger today for what some would term "too long" in order to accommodate the indeterminacies within the off-boarding business process. For example, even the current system could completely and automatically deactivate/de-provision NetIDs for terminated employees within a day or two, and in fact, the SES system has a deactivation routine that runs nightly, removing SES access from any employee who has been terminated.

But the process is not set up to move that quickly because employees who are actually leaving may have a lot of back-and-forth in their actual departure date, and annual or academic year appointments often have delays in getting renewed. To avoid the error of deactivating a NetID prematurely or mistakenly, the system is intentionally slow with email notifications built into it to avoid these situations. And in some situations – e.g., sponsored research needs to have the NetID stay on when a researcher leaves —"leaving" is not an all or nothing situation. The researcher may continue working on the project after leaving NU and moving to another institution, or resources may be tied to the NetID that are most expediently preserved by also preserving the NetID.

This, then, leads into another part of the same qualifying phrase – "rapidly *in* alignment with the need for their actual usage" – reflects another recurring theme in the focus groups: the current process is not fine-tuned enough to provide access to resources for all entering or departing members of the community. Examples cited included: students needing to get to housing or financial aid packages before they enter, or pay bills, request transcripts, or see credit balances or account history long after they graduate. (One comment was that it was like we disown the students after they graduate.) Faculty often need access to Blackboard, research file shares, or research proposals prior to getting their NetIDs.

The final part of the tenet - "easily auditable trails" -- has not been a past requirement. However, auditing both the management of a NetID and its use in accessing systems is becoming more important. Auditing (e.g., being able to log/review activities by a NetID) is a current compliance requirement of HIPAA/HITECH, and it is expected that more regulations requiring similar logging will be forthcoming. Additionally, NUIT's Security and Compliance team receives requests regarding "where/when" a NetID was last used. Auditing of the management of a NetID is necessary to ensure an ongoing level of confidence that the real person remains in control of the associated credentials and the credentials are not being used maliciously. An example of this concern within the current IdM structure is the possibility that a NetID administrator could create a manual NetID and use it to approve transactions entered by him with his real NetID. Financial Operations wants to minimize the chance that a single person can create and approve transactions – and one way to do that is to more aggressively audit and track what NetID admins are doing and confirm periodically they really do need those privileges to do their jobs.

This confidence may also become necessary for certain security applications (e.g. laboratory entry, computer access to human-subject data, etc.). The IAM system should provide audit trails for any NetIDs with a required level of confidence.

By comparison, auditing the use of a NetID to access systems is most often implemented within the applications themselves; however, which NetIDs to audit may be determined by either local (application) or global (IAM) attributes. For example, a NetID with the ability to approve purchases above $1M might always be audited within a financial application. In another instance, a NetID assigned to a contractor working on a human-subject database project might be audited at a network level to confirm that the NetID is being used in keeping with required security agreements.

Another side of this is auditing the people who create NetIDs. University auditors have shown increasing interest in the manual NetID process, and as a result there has been an interest in reducing the use of manual NetIDs. Every six months, NUIT contacts a designated person in each school or department asking them to review all of the school's NetID administrators (anyone who can create NetIDs or reset passwords). The

designated reviewer must contact NUIT and indicate that each administrator still requires those privileges. If this attestation is not done, the privileges are automatically removed.

4. Authorization is appropriately granular and based on robust identity information.

Assuming that a person's appropriate identifier can be found and is authenticated, the next step in the IAM process is for the application to make an informed decision about providing access to services/resources. With the manifold and ever-expanding set of electronic services now available, a rich set of data should be made available to a wide variety of business applications. For example, an entering graduate student should be represented by a standing (graduate student) in a given program (Mechanical Engineering) with a given initial start date (September 1, 2015). This information can allow services such as SPAC to decide in real-time if this person is allowed services. If SPAC policy is to allow access as early as June 1 before initial start date for graduate students, then the SPAC software can make that determination. Similarly, even though the general policy is to offer service to full-time students, part-time students from some schools allowed access and undergraduates might be offered service over the summer, despite not being enrolled in classes for that term.

Northwestern's access logic situation is far from this ideal. The information is limited on both sides of the IAM relationship: by what the identity management sources make available, and how the applications are set up to process that information. Today, access control has little subtlety: the IdM system essentially says whether the NetID is active or inactive, and then access to the desired system is either on or off.

Participants in the focus groups recurringly expressed interest in correcting this situation by changing the information that is being retained and made available for access decision-making on several important dimensions: the persistency of information (i.e. historical data is important to keep and have available), and the ability to have information about a person's full set of relationships with the University, not just their primary one.

Persistent Information

It is not unusual for a person to come and go from the University, sometimes with relatively long periods of time away, and sometimes with relatively short periods in between. Examples of these situations - where a person suspends their relationship to the University then returns later (either to that relationship or a new one), or where a person becomes known to the University, then fades from view only to reappear later - include:

1. Intermittent instructors (SCS, adjuncts, CTD) who teach for a part, or parts, of a year, year after year, and any delays in getting access to Blackboard can have a significant impact on their classes;

2. Retired learners (OLLI – Osher Lifelong Learning Institute) who need access to Blackboard on a recurring but often episodic basis, and often register with a very short turnaround time);

3. Students in part-time programs where continual enrollment is not required, or students who take a year off for a variety of reasons;

4. Consultants, contractors, or volunteers who may become students, staff, or faculty, and vice versa.

5. Students in the continuing professional education courses offered by multiple schools at Northwestern, whose identity is not retained from one session to the next.

As stated at the outset (See the section on The Increasing Importance of IAM in Today's World, on page 9.), we heard from many focus groups that they anticipated their communities-of-interest will change in ways that will increase the need to handle episodic relationships (and multiple relationships as well) as part of our IAM system's core competency. For instance:

- With shifting demographics, improved technology for remote learning, and a greater interest in lifelong learning, episodic students will likely increase in number.

- Competition for the best students continues to intensify, leading to an increased desire to begin prospecting for the best students even earlier, and particularly when potential students have a relationship with the University already via one of the growing number of programs the University has with bright and talented youth.

The relationships of most of these people to the University are different from the traditional relationships of students, faculty, and staff, and the expanding interest in maintaining a connection to, or an awareness of, people across a longer span of time will make the need to maintain persistent information even more important.

At this time, the IdM system does not retain this kind of information, i.e. that a person has a known-but-interrupted relationship with the University. The result is that, at the very least, the same amount of effort is required to provision and de-provision their ID each time they come and then leave. At worst, duplicate NetIDs can be provisioned.

Another facet of "persistency" that was mentioned in the feedback was the importance of not recycling NetIDs. Some systems, such as the Integrated Safety Information System (ISIS) (which tracks research-related training and compliance requirements) tracks people by NetIDs, some of which are Manual NetIDs, and if a NetID is recycled, important data records can be mistakenly mashed together. Currently, some NetIDs are re-used – NetIDs that were assigned to organizations (e.g., "chemistry department") for email and directory-listing purposes, and also those used as 1-day library walk-in patron NetIDs – but all others are kept forever and are never re-used.

Information about Multiple Relationships

Another instance in which personal attribute data is missing is when a person has multiple relationships with the University. In this common scenario, each of these relationships has a different set of services, or different levels of the same services, tied to it, and the IAM process should be able to handle these situations as part of its core competency.

There are limitations, however, that constrain this desired state. Some are technical, on both sides of the IAM relationship. For instance, some LDAP attributes (e.g., 'mail', 'displayName', 'postalAddress' and 'eduPersonPrimaryAffiliation') are defined by the LDAP protocol specs as "single-value" attributes that force limiting the choice of values to those attached to the primary role. There are other LDAP attributes that store the values from other sources, but many applications can't be configured to look anywhere besides the default LDAP attribute, or cannot parse a list of multiple values and pick the one they want.

This makes handling the following situations very difficult:

1. *Joint appointments for faculty* - While these may be proportionately small in number, they are often done for high-profile faculty, and they can be very frustrating for the faculty member and the administrative staff who are responsible for the services s/he wants/needs. For example, the "non-primary" school does not have access to the person in some systems, which makes it difficult to do things like granting security permissions for them.

2. *Students in dual degree programs across schools* - The same problem exists for students in joint degree programs, e.g. JD/MBA. The school that admits the student first "owns" him or her, and as the student moves between schools, access to resources becomes problematic, e.g. email addresses if the two schools have branded email addresses, access to collaboration tools/resources, and assistance with NetID problems.

3. *Multiple roles crossing constituency types* – A staff member might become a student or be an alumnus, too; an undergraduate student might be an applicant for graduate school; a grad student might be an instructor, sometimes for only a quarter; a faculty member can be a parent of a student, etc. When one role is added, dropped, or changed, the other role(s) often remains unchanged, and unless that remaining role is known and factored into the provisioning or de-provisioning process, services can be inadvertently affected. For example, an employee who also becomes an undergraduate student might not be recognized as having free access to certain athletic facilities or events because of the "primary" employee relationship. Similarly, a graduate student has different library privileges than a faculty member, but what if a person is both (and what happens when they go back to being "just" a graduate student)?

These situations elicited recurring requests in the focus groups to:

- be able to know about the multiple relationships of a person,
- be able to manage access to services for all roles, not just a primary role,
- not have a change in one relationship affect services provided to the other role(s).

As we have seen, being able to fulfill these requests involves not only having this information available, but having the applications that control access to their own resources be capable of acting appropriately on the more complex information.

Information that is Globally Contextual

A growth in the international nature of our community also puts strains on basic data elements in our systems that are identity attributes. For instance, international students/employees often have multiple visas and renewed passports sometimes get new numbers, but there is only one data element for a visa number (and the federal government only allows one within the U.S.). Similarly, personal names are different in number and order around the world, which can also create confusion and visa verification issues. These situations, which are at root "systems of record" data issues that then become IAM issues, can cause confusion in international campuses such as Qatar, can cause confusion for international citizens at domestic campuses, and can lead to the mistaken issuance of multiple credentials or conjoined records, which combine two distinct students under one record.

Information about Group Membership

Access to most services, including basic communications, is based on memberships in different "groups", and the need for a finer granularity in available group information for provisioning and de-provisioning is important not only at the enterprise system level, but also at the local school level where many services are delivered and controlled. The availability of basic role and organizational information (e.g., staff, tenure-track faculty, chemistry major, works within WCAS, member of Central HR, member of Medill IT, etc.) needs to be generally available (i.e. not just in LDAP but in Active Directory too), the ability to create and manage many of these groups needs to be available locally, with the data, in many cases, stored or replicated in central directories given the emergence of centrally-managed shared collaboration services.

To cite only a couple of examples from the focus groups, the Library needs to create custom groups all the time (e.g., all Music faculty, a professor and her graduate students, thesis and dissertation committees) for providing access to a custom set of library resources, and if WCAS had better access to this information, they could maintain email lists dynamically rather than manually as they do now.

5. Surrounding business applications are integrated with the enterprise IdM system.

Even if the IdM system provided access to robust identity information and it was available as it was created or as it was needed, the overall IAM system would only function at a high level if the surrounding applications are

tuned in to the IdM system and use it fully for their authorization/access decision-making. Neither of these aspects is currently optimized.

Optimizing Authentication

As stated earlier, the NetID is the accepted standard for online identities (though there are notable exceptions to this rule, see page 12). Most University systems, and most local systems, use NetIDs for authorization decisions. Appreciation of the productivity benefits afforded by this standardization were repeated in multiple focus groups, however it was always coupled with frustration because the expectation is not only that there will be a single electronic identity used for access to University services, but that this single identity should give access to an integrated suite of services via web Single Sign-on (SSO).

The need to log in to multiple systems, repeating entry of the same NetID and password, or the need to supply different credentials for different systems, were seen as unnecessary barriers to productivity. A single authentication event in a browser session should suffice for multiple system log-ins.

By the same token, administrators who had to use more than one enterprise system at a time also expressed frustration that the current implementations of web Single Sign-on causes these sessions to conflict with one another, forcing the user to either use two separate browsers or to log out of one system and clear their browser's cache in order to log into the second system.

Optimizing Authorization

As we have seen, while the NetID is the accepted standard for online identities, the integration of surrounding business applications to the University IdM system is quite loose. There are several downsides to this situation.

On the provisioning side, identity and personal attribute data is available via periodic batch data export/import sequences instead of being real-time processes, applications often look internally for the data that has been stored from these export/import routines, and the applications do not handle any "special case" access logic on their own. In short, most applications at Northwestern use a very limited set of outputs from the IdM system, and by far the most widely used output is basic NetID authentication, which triggers a basic On/Off access decision. As the sections on Manual NetIDs and the need for more robust information have shown, access mechanisms at Northwestern need refinement to get past this binary mode of operation.

On the de-provisioning side, there are situations that arise from time to time where access permissions are not always taken away when they should be due to the "loose" connections between the applications and the IdM system. For instance, when a person who is a student and a staff member stops being a staff member, but their NetID remains active due to their continued status as a student. Some of their permissions connected to being a staff member might persist, and because there is not an automated connection between identity status changes and the access permissions in the surrounding applications, those authorizations might not get removed when the NetID gets turned off. In the latter case, should the person return in a different role, those authorizations could still be in effect.

Another area in which business applications could benefit from better integration with the enterprise IdM system is in the handling of identities for people with elevated access permissions in administrative systems, i.e., administrators that can change grades, do salary or budget planning, authorize large expenditures, etc. These privileges in the FASIS and SES systems are currently tied to second IDs, not regular NetIDs and not Manual NetIDs. This process, which exists completely outside the enterprise IdM system, gives total control over access to these system owners, but moves all the IdM functionality outside the enterprise IdM system, which increases the risk that this elevated access could be left intact when a person changes jobs within the University or leaves it entirely, and makes it difficult for other workflows to be tied to this status. (See the discussion on the use of secondary attributes, page 38.)

[*Side Note*: There are three types of users of enterprise administrative systems:

1. the general population which gets access to their own individual records by definition (e.g., individual faculty and staff self-service access to their records in FASIS),
2. administrators with higher level rights who can see, and sometimes change, data for groups of people other than themselves,
3. IT personnel (programmers, database administrators, and system administrators) who have system-wide access.

The first group is handled via the regular NetID process, the last group is handled specially via a separate server (CyberArk). It is the middle group of users that is being discussed here.]

6. The level of rigor employed in identity proofing and authentication at the time of access is based on the risk and value of the transactions to be done.

In today's world, one size cannot fit all when it comes to security. As the nature of our business, the world in which we live, and the definition of our community all change, there are increasing requirements for greater confidence and security, AND an increasing need for lower barriers to access.

The Need for More Confidence and Security

On the need for greater confidence and security side, multiple types of credentials for a single authentication can create greater confidence in identification and appropriate authorization to access high-value functions or high-value information. Interest in multi-factor authentication (MFA) (e.g. key fob and biometrics) was mentioned more than once in the focus groups, as was interest in out-of-band challenge-response methods for certain functions (e.g., such as banks use today – perhaps sending a text message with an authorizing code to a person's cell phone for entry when completing a transaction). The common interest in these approaches is to increase trust in credentials at the moment of authorizing access. This interest has coalesced into a pilot project on multi-factor authentication using a product called DUO.

There is also growing interest in insuring confidence in identities themselves during their lifetimes. With the growth in regulations surrounding student records, personal information, and health information, the heightened sensitivity of protecting valuable research data, the growing role of online education, identity assurance (the confidence that a person is who he or she claims to be) has become increasingly important to research and academic functions. Granting agencies are beginning to require improvements in this area, and external auditors are paying more attention to this area.

At Northwestern, employees who go through the basic hiring process have fairly robust identity vetting as part of the federal I-9 employment eligibility process, as do TGS students in order to receive stipend funds. Students may never present a photo ID between the time they take the ACT/SAT and when they want to pick up an official transcript at graduation. Manually asserted NetIDs are created with little or no identity vetting.

The Need to Lower Barriers to Authentication and Access

Aside from the manual NetID process (which, as implemented, has multiple downsides), getting and using a NetID is a "heavy" process, with administrative checkpoints built into it to insure high levels of Trust and Assurance are connected to the credential. If using your NetID and password to access resources is not a normal part of your daily routine, remembering your ID/PW can be a challenge, and requirements to be physically present to get your password reset if you can't remember the answers to your security questions can be problematic if you are not on-campus anyway. As the nature of the Northwestern community expands and evolves, the number of people who fall into this category will grow – the number of affiliated partner institutions continues to grow; wholly online programs are growing; experiential learning and community-

involvement projects and initiatives are expanding as is lifelong learning, and short-duration programs offered for the larger public are increasing – and being able to maintain appropriately high levels of security becomes much more problematic in these cases.

Lightening the process by "lowering the barriers" can come in different ways for different combinations of people and resources. Sometimes resources don't require the higher confidence and security provided by the core NetID processes. Some resources only need a much lower level of confidence and security, and in other situations, the levels of assurance and trust can be set sufficiently high without using a NetID. For instance, access to the University's wireless network used to be available via NetID authentication. This always caused problems for people temporarily on campus – e.g., contractors, consultants, guest lecturers, recruiters, parents, prospective students, or visitors – and with the growth in mobile devices – laptops, smartphones, tablets – and the spread of wireless networks everywhere else, the problem only became worse. Today, we have a guest network that only requires a user to self-enter a name and email address in order to gain access.

Similarly, Northwestern alumni used to be able to access the online alumni community application only via a Northwestern-issued alumni account. But it was difficult for alumni to remember their ID and password, which created a barrier to participation and placed a support burden on the University alumni staff. By contrast, the new OurNorthwestern alumni application has an Identity Provider module that allows alumni to log in with their Facebook or Google account, thereby removing participation barriers, allowing the University to get updated personal information stored in those external applications, all while lowering support burdens. This approach could be used in multiple other situations around the University where the services are less sensitive and the users are more removed from the everyday life on campus. For example, other schools are using this approach to provide access for library patrons (e.g., the person who comes in off the street to read *The Chicago Tribune* for two hours, or the graduate student who needs to come for a week to research African art), parents to look at their children's grades and financial records, people taking non-credit courses, students to share their portfolios with potential employers and friends outside the University, recommendation letters.

Progress has also been made in the last year on the University's ability to federate our IdM system with systems at other institutions. Shibboleth, the University's primary federation application, has been brought to the most current release and allows the Northwestern community to use their credentials at other federated institutions and vendors, and vice versa. About 40 cloud-hosted applications are now being accessed with NetID and password. Examples include TeraGrid (research computing), Student Conduct (Student Affairs), CareerCat (Career Services), Qualtrics (surveys for Feinberg, Weinberg), Orbitz (Travel Services), Primo, Illiad and Ares (University Library) and the Canvas pilot (Provost, NUIT). Planned deployments include the Box.net file sharing system, several University Library systems and purchasing from SciQuest via NU Financials.

7. Identities are protected and secure.

The University has an obligation to protect individual identities for legal and regulatory reasons (e.g., HIPAA, FERPA) as well as strategic reasons (e.g., institutional reputation, faculty/student/staff recruiting). Protection of individual identities also protects the institution; compromised individual credentials can lead to further breaches and unauthorized data disclosures.

Confidentiality, Availability & Privacy

Information should be disclosed in an intentional manner, according to defined policies and practices. Some information, such as basic directory information as defined by FERPA, can be disclosed to the general public, or at least to anyone within the institution. Other data (SSNs, credit card numbers) should be more carefully guarded. Northwestern's IAM systems must not only safeguard information they store internally, but must also provide data that allows other systems to make appropriate access decisions.

One tactic is limiting the spread of sensitive information. For instance, the IAM ecosystem makes use of SSNs only in matching data between FASIS and SES, stores them in encrypted form in its internal database, and does

not provision them into directories where they might be visible to applications or end users. IAM systems do not use credit card or other financial information at all. Most of Northwestern's enterprise and other systems still rely on bulk data replication. Moving to real-time access to information only when needed offers a much smaller target for intentional misuse or accidental disclosure than making multiple copies of the data. Even aggregation of data into AD or LDAP directories represents added risk compared with simply querying the source (authoritative) system for that data.

Local and cloud-based applications that access data in directory-type repositories (AD, LDAP) or via federation protocols (Shibboleth/SAML) go through an approval process whereby data stewards explicitly approve each such data release. The new Service-Oriented Architecture infrastructure can make additional data available from more sources, both for direct consumption and for access control decisions, provided applications are prepared to communicate with that infrastructure.

Integrity, Non-Repudiation & Auditability

Maintaining accurate and consistent data over time is a key component of securing identities. Our IAM infrastructure and most other applications already use standard cryptographic techniques to protect data in transit (SSL/HTTPS, SSH/SFTP). Good security policies exist, but are not adopted or enforced evenly across the University.

Strong password management policies contribute to identity security by making passwords more difficult to guess or discover by other means. Our current policies regarding minimum password length, frequency of change and complexity are roughly in line with peers, but are weaker than desired for high-value or high-risk transactions conducted with HIPAA and other sensitive data. Security experts are also increasingly skeptical that *any* password scheme can, by itself, provide adequate security.

Use of the Web SSO system allows secure authentication of the user without the added risk of exposing credentials directly to applications during authentication operations. Applications that require users to type in passwords must hold that password in memory at least briefly in order to authenticate the user against Active Directory or LDAP servers. This exposes the password to additional risk. Applications using Web SSO don't ever need to see passwords and thus provide less exposure.

A multi-factor authentication (MFA) pilot is underway with the FASIS system to increase the level of confidence in authentication sessions. This technology protects identities by requiring physical possession of a device (smart phone, office telephone or other device) in addition to knowing the NetID password. Broad adoption of this technology would reduce our vulnerability to phishing and other attacks involving the compromise of passwords. Ideally, MFA should be integrated with the SSO environment, and/or directly with applications, so the applications can decide whether to allow certain transactions based on their confidence (or lack thereof) in the strength and validity of the original authentication.

8. Each part of the IAM system is relatively easy to maintain and to replace.

Most of the applications within the IAM system are provided by 3rd-party vendors with regular upgrade and maintenance paths. The oldest and most complicated homegrown system – SNAP – was retired six years ago.

Today's IAM system has three pieces that require inordinate effort to maintain: NU Validate, the plethora of independent Active Directory domains, and the system that provisions data into the WildCARD system.

NU Validate has had a great deal of customized logic added to it in order to handle differing business needs. The logic for these special cases has been built directly into the system instead of being handled on a decentralized basis in the surrounding applications. The centralization of this logic, and the centralization inside of the identity management system itself, increases the overall system's complexity. This makes the

system difficult to troubleshoot and hard to extend due to the lengthy testing cycles required to prevent changes from breaking other portions of the system.

The proliferation of independent Active Directory (AD) domains creates a second area of increased effort. The software used to replicate data to the various AD domains requires a great deal of maintenance and customization to handle the requirements of each individual domain being synchronized (e.g., who is included in the domain – all temporary employees look like they're employed by HR, not a school or business unit, sometimes students connected with one school are taking a class in a second school which requires that they have access to the second school's online resources, sometimes special group attributes need to be pulled in and put in a unique place in the receiving unit's Active Directory, etc.). This increased complexity necessitates extra effort to troubleshoot the replication of identities, and irritating workarounds are required to fix problems created by basic IdM tasks, e.g. a password change is required when an employee switches jobs and needs to be added into a different AD domain, and sometimes a person's access permissions get lost when their identity's status changes and a password reset is the only known way to bring them back.

The third area that requires inordinate effort to maintain is the system that provisions data into the WildCARD Office card printing system, University Library, Athletics and the Henry Crown sports & recreation facility. This system essentially duplicates the functionality of the NU Validate system in order to produce and manage the physical Northwestern identity credential, the WildCARD: it assembles data from two authoritative systems (FASIS, SES), performs customized data transformation logic for downstream systems unable to do so, and transmits that data to other systems for use. The current incarnation of this system was created within an urgent, fixed-deadline project three years ago when it had to be moved off the University's mainframe computer so another year of software licensing fees for the mainframe could be avoided. Because it mirrors NUValidate's process, it has much the same set of convoluted "special case" business logic built into it, plus it has code in between it and the authoritative systems (FASIS and SES) that convert attribute codes back and forth between the codes used in the authoritative systems and the codes use in the legacy mainframe system.

9. Business applications and the IAM infrastructure are flexible and easily modified to take advantage of new IAM technologies as they emerge and become stable.

The wave of the future is being able to connect to, and integrate, 3rd-party systems hosted in the cloud by someone else. We need to be able to connect to these seamlessly and have our clients (faculty, students, staff, etc.) use an approved credential to authenticate. We need to be able to make this work for all sizes of 3rd party solution providers. Some can do federation via Shibboleth, but many just want to authenticate straight to our AD / LDAP. We need to provide a set of tools that can be used across all of these situations.

We have made positive strides in this area in the past year plus, with a growing usage of federation via Shibboleth and SAML, but there are no well documented best practices to follow, we do not prioritize this capability when new applications are being vetted, and we do not offer a wide range of standardized capabilities to enable this type of connectivity.

IV. Opportunities and Threats

Introduction

Parts of the IAM marketplace -- e.g., internal (i.e. on-site) identity management, provisioning, directories and authentication systems -- are made up of mature software, standards and vendors. There is still some fluidity even in these areas as vendors compete, merge with, and acquire one another but these are essentially commodity services. Innovation is largely concentrated in the area of federation, which is rapidly changing. Enabling people, devices and applications to operate smoothly across institutional boundaries is the key challenge for many organizations as they look to deploy applications in more locations (data center, public cloud, private cloud), more rapidly, and make them available to more users (beyond traditional employees or students) than in the past. Thoughtful decisions about IAM standards, vendors, purchasing policies and the use

of external resources offer Northwestern the opportunity to improve end user experience with IAM, reduce costs and decrease deployment time for new services.

The IT marketplace varies widely in product and standards maturity.

Some IAM-related standards are mature and widely implemented at Northwestern and by vendors, both in IAM products and business systems that use IAM infrastructure. Making use of systems that support these standards makes obvious sense and should be encouraged. However, when building infrastructure on less mature or less widely-implemented standards and products, Northwestern will need to balance the short-term benefits with the longer-term risk that a product, standard or vendor could change or disappear entirely, requiring a potentially costly adaptation.

Nearly all applications in use today can externalize basic user authentication and attribute lookups to some degree. This allows a baseline of integration – NetID/password authentication and some degree of on- and off-boarding. Standards in this category include lightweight directory access protocol (LDAP) for authentication and directory lookups, Kerberos for authentication, and several Microsoft-specific standards for applications relying on Active Directory (AD).

Other standards are mature but unevenly implemented by vendors, or by Northwestern. When both Northwestern and vendors have implemented software supporting the same standards, integration with University systems is relatively quick and inexpensive. When vendors have chosen different standards or proprietary methods, integrations are difficult, expensive or impossible. Standards in this category include security assertions markup language (SAML) for federation with external partners (cloud-based vendors, other universities); simple object access protocol (SOAP) and representational state transfer (REST), commonly used in Service-Oriented Architecture (SOA) deployments that use web services as the fundamental method for integrating applications and making functionality available; and some of the "WS-*" collection of web services standards.

A third category consists of standards that are not fully mature, or are mature but have not achieved wide adoption. These standards largely represent future opportunities, though they may be useful in the near term under the right conditions. Some will succeed, while others are simply lingering until something better comes along. Such standards include OpenID Connect/OAUTH2, another federation standard; service provisioning markup language (SPML); some of the WS-* standards; system for cross-domain identity management AKA simple cloud identity management (SCIM); and others.

Many cloud-hosted applications use SAML, which makes for relatively easy integration for basic authentication and first-access user provisioning. Other applications expect that users will use a different ID/password for access, an insecure initial password (e.g., SSN), have access to our AD/LDAP directories (not allowed by policy for security reasons) or use a proprietary federation method. A growing minority support REST or SOAP web services for provisioning user data, but many still expect either bulk feeds of flat files or another proprietary method.

Identity and credential assurance has long been a concern, but has been slow to gain traction.

When identities from one organization are used to access sensitive resources at another, it may be necessary to communicate the identity provider's (IdP) level of confidence (sometimes called level of assurance, or LOA) that the person initiating a transaction is actually that person. Technical solutions such as multi-factor authentication are available, as well as frameworks for evaluating an IdP's policies and procedures (e.g., InCommon[1] Bronze/Silver). The biggest challenges to implementing the InCommon Bronze/Silver standards are

[1] InCommon is a federation of institutions, with connections to the Internet2 organization, that is dedicated to creating and supporting a "common trust framework for U.S. education and research". As such, InCommon

in areas not obviously related to IAM – policies about network encryption, configuration of encryption used in web and authentication protocols, operation of data centers, etc. LOA is likely to be increasingly important within Northwestern as well; applications may wish to restrict certain transactions or limit access to data depending on the characteristics of the user and/or session.

The open source IAM ecosystem, led mainly by higher education institutions, is vibrant.
Internet2, InCommon, Shibboleth Consortium, JASIG and Kuali are some of the organizations playing a role in this area. Many are interrelated and fall under the Internet2 umbrella in one way or another. There are active development efforts in many areas - federation (Shibboleth, Cirrus Identity's social/SAML gateway), group/privilege management (Grouper), core identity management/provisioning (Penn State's "Person Registry"), policy & standards (MACE/Middleware Architecture Committee for Education), SSO (OpenAM, CAS). Commercial vendors (ForgeRock, Unicon, 9Star) are offering support for these systems as well, making it more attractive for institutions (such as Northwestern) with smaller commitments to in-house IAM development. Work is underway to collect many of the aforementioned systems into an open source IAM suite called CIFER.

Vendors for some IAM systems are small and could easily be acquired or fail financially; other vendors are large corporations for whom Northwestern is one customer among thousands or millions in a global market.
IAM systems such as Web SSO, Radiant Logic (AD synchronization) and CyberArk (privileged account management) have been licensed from very small companies. This can give us leverage with product features and (sometimes) good financial terms. The products developed by these companies are often innovative, even leaders in the market. As with any small company, they are also at elevated risk of financial failure or being acquired by a larger company. Expertise can also be difficult to find due to the small market presence.

Other IAM systems, such as NU Validate, LDAP and Active Directory are licensed from large companies (Oracle, Microsoft). Northwestern has little direct influence over product features and direction. Products are also relatively expensive, but expertise is widely available.

Professional services and contract labor resources are available to speed deployments, but can be scarce and expensive for the most specific needs.
Even the most widely deployed IAM standards and applications remain niche markets compared to more common line-of-business systems (financials, HR, etc.) and as a result talent is harder to find. This is true for both contract workers and permanent staff. Not only is IAM in general a niche market, it is also fragmented across several vendors. Even when candidates with good IAM experience are identified, that experience may well be with a different vendor or technology.

Cloud-based systems hold the promise of filling needs quickly and cheaply, yet they can unreasonably raise end-user and business expectations.
Applications hosted in the cloud are often partially or fully targeted at consumers and are therefore: easy to begin using; have a clean and modern user interface; do not require customers to do maintenance, monitoring or upgrades; and offer popular services for low (or no) cost. Traditional applications hosted in the data center often suffer from deficiencies in some or all of those areas. On the other hand, cloud-hosted applications also present all of the same authentication, provisioning and integration challenges that we face with traditional applications hosted in the data centers. Under ideal conditions (vendor supports SAML, is a member of the InCommon federation, application automatically provisions user profile at first login) new cloud applications have been deployed at Northwestern in hours. Under other conditions, it can take days or weeks.

---

defines Identity Management standards that define different levels of identity assurance (Bronze, Silver, and Gold), and issues software certificates to institutions based on their ability to implement the requirements.

a. Allowing clear-text access to NetID passwords outside of the University data centers, even briefly, is a serious security risk, so current policy & practice prevent the direct use of LDAP, AD or Kerberos authentication (because the vendor would have access to NetIDs/passwords in clear text, even if only for an instant). Alternatives such as SAML (see above) exist, but have not been adopted by all vendors. A few vendors have alternate means of authentication (OpenID Connect/OAUTH) which we do not yet support. Many vendors suggest various proprietary methods which are costly to implement and sometimes of dubious security. Rough estimates of the vendors we are likely to deal with are that 20% are able to use SAML, 10-15% prefer OAUTH2, and 65-70% are either not yet prepared to do any sort of federation, or else they use a custom built technique. SAML adoption has been rapid, especially in higher education and the vendors that serve higher education; adoption outside that sector is also growing but may not become pervasive. OAUTH2 is newer, widely viewed as simpler, and rapidly growing; however, the technology is too new to accurately predict its ultimate adoption rate.

b. Some vendors support first-access provisioning, where user profiles are provisioned during the first successful login. Other systems require flat file feeds or other basic mechanisms. A few systems are starting to become web-services capable.

c. Vendors who support RESTful or SOAP web services (inbound and outbound) present the greatest opportunities for quick and secure integration with other University systems, regardless of location (cloud or data center). Applications still requiring proprietary development work or nightly bulk data transfers to integrate with other systems are more expensive and time-consuming to implement. The integration points are also more brittle and can easily break during upgrades, patching, corporate mergers & acquisitions and network re-configurations.

Alternate identities are widely available and every consumer-based internet user in the world has at least one.

There are hundreds of external identity providers (Microsoft, Yahoo, Facebook, LinkedIn, Google, other universities, governments, etc.) who collectively manage millions of identities and provide authentication services to anyone who wants to use them. Technologies exist to build bridges between our IAM infrastructure and others. This presents a huge opportunity for Northwestern to offer authenticated access to services and resources beyond what would be practical (or even possible) if everyone needed a NetID issued and maintained by Northwestern.

The intent here is not to supplant the NetID as the core Northwestern credential for the Northwestern portfolio of services. Rather, the idea is to augment the NetID with these credentials when appropriate. (See below, page 47.) In cases where the people involved are more loosely connected to the University, and the transactions have a lower risk or lower value attached to them, these external credentials provide IAM opportunities that did not exist in earlier times. With appropriate integration points developed within the IAM infrastructure, federated authentication can be used to large sets of people for which trying to scale the NetID would be impractical.

V. What Others are Doing

The IAM Marketplace – Gartner's Perspective[2]

Gartner sees certain IAM technologies as mature, and now considered to be basic infrastructure. These include Web SSO, virtual and physical directories, and basic identity management & provisioning software.

[2] http://www.gartner.com/document/2008315?ref=lib
http://www.gartner.com/document/2556016?ref=lib

Northwestern's experience is generally in line with that assessment, though we lag in some areas (Web SSO has not yet been adopted by most enterprise systems, for instance). Other IAM technologies, mostly related to federation, are changing more rapidly and present additional challenges for organizations. These include many of the things Northwestern has recently begun to take interest in as well – SCIM, OpenID Connect, OAUTH, social identities in general).

Regardless of maturity level, Gartner sees many organizations still struggling to fit IAM into existing governance structures in a well-integrated fashion. IAM governance is recognized as a critical area at Northwestern as well, and is being folded into the developing IT@NU governance structure. IAM remains poorly understood outside of IT organizations both at Northwestern and in the world at large.

Gartner has focused much research on federation and cloud-based applications in their "Identity Management" practice area. This area includes Identity and Access Governance, Identity Data Services, Identity Policy Admin, Provisioning and Web Access Management. Gartner observes that not only applications, but also user identities, devices, and IAM itself are moving outside traditional institutional boundaries. Northwestern and other universities have long dealt with external devices, e.g., student laptops, so users bringing their own devices to work/school to access services has not presented the same types of challenges as in the corporate world. Northwestern has deployed many applications in the cloud, and has also begun to accept external identities for access to a small number of systems (e.g., "OurNorthwestern"). As preliminary conversations at Northwestern have shown, organizations often struggle with whether and how much to trust external identities, applications and data storage services. Gartner research indicates this is a common set of issues that nearly all types of organizations are trying to address. There are few proven best practices in this area.

Regardless of how policy and governance development plays out, a concept Gartner calls "adaptive access control" is emerging to guide implementations. While traditional role-based access control depends on having local identities with a rich set of information about each user's job responsibilities, adaptive access control ties authorization to a variety of factors (whether the identity is internally-provisioned or external, the type and location of end user device, time of day). The level of access granted will vary based on many factors. For instance, a system might allow purchases up to $10,000 when an internal identity is used from a local IP address during business hours; but it would restrict expenditures to $100 after hours, when the user is not physically present, or is using a federated identity rather than a credential issued by the organization. Gartner believes this approach will prove easier to implement than role-based access control and will be better suited to a federated environment where less complete data about some users is available.

Institutions purchasing cloud-based services face the same IAM challenges as with locally-hosted applications – rapid and secure provisioning, managing access rights, auditing, etc. While many traditional IAM vendors (on-premise and in the cloud) are starting to include federation features, consultants and vendors are meeting a significant integration need by selling connector software and integration services to help organizations manage the integration of cloud-based systems with local resources. Northwestern could potentially realize significant benefits (reduced cost, quicker deployment, development of local expertise) by purchasing software and services from this new and thriving marketplace.

---

http://www.gartner.com/document/2676617?ref=lib
http://www.gartner.com/document/2630035?ref=lib
http://www.gartner.com/document/2618915?ref=lib

CIC – Committee on Institutional Cooperation[3]

IAM has been a recurring and growing subject of attention within the higher education IT community: in the CIC, RUCC (the Research University CIO Conclave, an informal self-organized group of approximately 50 CIOs of North American "research intensive - high" Carnegie class universities), and Internet2 (a community of leaders from research, academia (over 250 universities are members), industry, and government who create and collaborate around technological issues, topics, and needs). Building on a shared understanding of the importance of this area, Internet2 has commissioned a quick review and recommendation in the area of IAM, and some are even suggesting that IAM will require significant support and investment (some say equivalent to what it took to start Internet2) in the very near term.

The following observations come from a recent survey on IAM within the CIC:

a. **General IAM Environment.** Most CIC schools have had active IAM environments for many years, beginning in the 1990s or earlier. As at Northwestern, CIC schools are maintaining complex IAM environments that are a mixture of home-grown, commercial and open source systems. Nearly all CIC schools run an enterprise LDAP directory. Most schools also have long established Active Directory environments, either centrally run, de-centralized, or a hybrid. For identity management products, a 2009 survey indicated there is no clear trend; two schools were running homegrown systems, two were using open source, three used commercial systems, and a plurality (five) used a blend of two or more types. A survey from several years ago revealed that three schools had already integrated physical identity card systems with IdM systems. Eight did not, but six of those had plans to do so (presumably some have been completed in the intervening years). Ten out of eleven also handled guests, alumni, hospital employees and other affiliates in their IdM systems, as Northwestern does with manually asserted affiliate NetIDs (see the discussion of Manual NetIDs on page 14).

b. **Federation.** Most CIC schools (9) use the open source Shibboleth software to support federated authentication, as does Northwestern. At least seven CIC schools (excluding Northwestern) are releasing at least some user attributes by default to other InCommon members to support quick integration with partners. Without this automatic (prior) approval, each proposed federation partnership must be presented to data stewards for review and approval. Northwestern does, however, automatically release data to partners who have been certified as “Research & Scholarship” service providers, as do most other CIC schools. Only one school required InCommon membership for all vendors, but (anecdotally) IT staff at several other schools are leaning in this direction.

c. **Level of Assurance.** Only two universities in the country have qualified for InCommon Bronze assurance (Virginia Polytechnic, University of Nebraska Medical Center). Only Virginia Polytechnic has qualified for Silver. Individual projects are underway at several CIC schools to explore Bronze/Silver certificate, as well as joint projects such as a “cookbook” for bringing Active Directory networks into compliance.

---

[3] https://cicme.cic.net/sites/cicit/idmgmt/Documents/Meetings/2009/August%204-5%20Face%20to%20Face/OSU%20Status%20Updates/CIC%20Survey%20Results.docx

https://spaces.internet2.edu/display/InCFederation/Research+and+Scholarship+Category

https://incommon.org/federation/info/all-idps-certified.html

https://cicme.cic.net/sites/cicit/idmgmt/Documents/Resources/Shib%20Version%20Survey.xlsx

EDUCAUSE[4]

A 2011 survey of EDUCASE members revealed the following national trends in higher education:

- Doctoral institutions commonly join inter-institutional identity federations; other categories of higher education institutions (e.g. four-year liberal arts colleges, community and junior colleges) do this less often but they do use federation technologies to enable on-campus web Single Sign-on.
- A majority of respondents agreed that demand for cloud computing in the coming year would increase their need for federated ID solutions.
- Between 2005 and 2010, use of strong passwords rose 25% and banning use of unencrypted passwords doubled.
- Institutions engaged in automated role-based authorization projects grew by half; those with fully operational implementations reported better IdM outcomes.

Northwestern's experiences are mostly in line with these overall conclusions, though we have not significantly strengthened password policies because those currently in effect are believed to be a reasonable compromise between convenience and security. Our efforts to implement enterprise role definitions have been modest, limited by difficulties in defining actual business roles that are consistent across the entire institution.

VI. The Path Forward

Clearly there are many areas where the University's situation can, and needs to, be improved given the changing nature of the Northwestern community and the changing landscape around us (technological, regulatory, security, and user expectations). Much work lies ahead if we are to leverage our Identity and Access Management infrastructure at scale, as we need to be able to do in order to optimize the delivery and support of our growing portfolio of online services and resources.

So often, the problems with "identity management" get flagged in conversations with the connotation that these shortcomings are purely technology issues, and sometimes with the implication that the topic is the sole responsibility of NUIT. To the contrary, one of the major intents of this report is stating that improving IAM at Northwestern will take the coordinated effort of the entire, and very broadly defined, IT@NU community.

Certainly, much of this work is technical, and the effort that this will require should not be underestimated, but it is important to recognize that a significant part of this work is outside of the purview of NUIT. Whether it is consolidating Active Directory domains, or reworking the applications so they integrate with the identity management systems (e.g., processing identity data and information via services instead of via batch files, making their own more finely-tuned authorization decisions based on real-time data held elsewhere), much technical work will be required outside of NUIT. And most of this technical work presupposes that existing business processes and needs have been documented and compared, and new processes, definitions, and policies have been articulated. This business analysis effort that must accompany the technological changes is undoubtedly complicated and time-consuming, and is central to the implementation of the new architecture being envisioned.

As stated at the outset of this paper, Identity and Access Management (IAM) is a relationship, with a set of systems/applications in the center that manage identities and enable a surrounding portfolio of systems/applications to make intelligent, real-time decisions that authorize access to their resources/services.

[4] http://www.educause.edu/library/resources/identity-management-higher-education-2011-report

The following subsections break this relationship down into three areas, with brief overviews of how we recommend moving forward in each area:

1. Restructuring Identity Management
2. Integrating Access Management with Identity Management
3. Optimizing Levels of Assurance and Trust

Restructuring Identity Management

IAM Characteristics addressed in this section:

1. Each person has a single electronic identity. There may be multiple credentials attached to that identity, but there is only one electronic identity.
2. The IdM infrastructure is integrated within itself, and data about identities and personal attributes flows smoothly throughout the system.
4. Authorization is appropriately granular and based on robust identity information.
8. Each part of the IAM system is relatively easy to maintain and to replace.

This section is largely about reducing complexity in the identity management infrastructure by altering several of the extensions that have been added to the IdM portfolio of systems/application over the years. It also contains a proposal for a key new piece of the IAM infrastructure: a new central registry of identity and personal attribute data, which will contain a more robust set of information about all of the people with whom the University has/had a relationship, including the identity information associated with each of them.

The first set of recommendations, and part of the central registry infrastructure, are elements of the first cornerstone of the new IAM architecture being recommended:

> **IAM Architectural Cornerstone #1:**
> The identity management system needs to be consolidated at the center with delegated administrative functionality.

Reduce Complexity

There are multiple places in the IdM system where complexity can be simplified, which will free resources to focus on other tasks that have been otherwise hard to get to, allow data to flow more freely within the enterprise infrastructure, and improve customer service.

Externalize "Special Case" Logic in NUValidate and Replace the End-of-life System

The NUValidate system is at "end of life" status with Oracle (see page 6), and we need to continue moving forward with due purpose to replace it. In order for this to happen, a functional replacement needs to be chosen, configured, and integrated. Initial preliminary work has started on the selection process, but replacing the product within a restructured architecture is a complex, multi-year task, which will involve many parts of the Northwestern community and have many aspects to it.

Prior to actually replacing NUValidate, the tangled web of "special case" logic needs to be externalized from the IdM system. Software logic that is added into the identity management system itself should be restricted to functionality that is in direct service of actual identity life cycle and password management; NOT to accommodate specific needs of applications. Code related to authorization needs of applications belongs outside of the identity management system and is the responsibility of the unit owning the relevant application. Who actually writes and maintains this code for an application is, as always, open to discussion, but the business and financial responsibility for the application rules belongs with the application owners, and all work should be done in accordance with documentation provided by NUIT. Externalizing this code (and

decentralizing it as much as possible) will not only reduce the difficulty in replacing NUValidate, it will also reduce the day-to-day operational burdens (maintenance, incident troubleshooting and remediation) on the Identity Services team, so it can focus its efforts elsewhere.

Consolidate Active Directory Domains

The proliferation of Active Directory (AD) domains happened to a large extent because of the absence of a robust central Active Directory domain. In recent years, driven largely by the selection of Microsoft's Office collaboration suite for faculty and staff usage, the central AD domain (ADS) has been extended in its functionality and utilization. A number of smaller schools/units have recently given up their own AD instance and moved to the central domain, and others are expressing interest, but there are still twenty AD domains at Northwestern. As more units look to save or refocus IT resources, more services begin to be utilized across domains, and the central domain becomes more robust, more units will see this as a viable option.

This movement should be encouraged, with a goal of a single Active Directory domain, or at least at reduced number of domains that are linked via "trust". This consolidation/integration has many advantages. For example, it will:

- reduce the effort required to deploy shared services across a variety of schools, and make it easier for users of these systems to authenticate into them.
- remove the glitches that require NetID password resets to fix access permissions and gain access to new AD domains when roles change,
- reduce effort expended in both NUIT and distributed IT groups in the daily work associated with maintaining identities,
- reduce effort in the distributed units that is required to maintain their own Active Directory infrastructure,
- reduce the risks associated with holding multiple copies of sensitive information (NetIDs and passwords).

However, local AD domains are a significant business resource for schools and business units, and a considerable number of design discussions will be needed in order to determine how the distributed units are actually using their domains, and what additional tools and overall AD structure must be in place in order to rationalize the twenty remaining AD domains. For instance, the current ability to manage local groups and resources will probably need to be replaced by a different software solution (e.g., Grouper), work needs to be done to insure that currently local AD schemas have not been extended in ways that will be harmed by collapsing into one central schema, and the local applications that rely upon local domains need to be evaluated for transitioning them to the central domain.

The analysis and design work for this transition will a partnership effort between NUIT and the schools and units giving up their own AD domains. When it comes time for the actual merging of a distributed domain into the University domain, the bulk of that work will fall upon the IT groups in the units, because they will have to manage the reconfigurations of all the devices in that domain, and transition to a new way of managing groups etc.

Integrate the WildCARD with the Rest of the IdM System

The separate, parallel identity provisioning universes of the NetID and the WildCARD are a historical artifact of a time-limited transition off of the University's mainframe. These processes should be integrated as part of NUValidate's retirement.

Similarly, the WildCARD barcode has historically existed in a parallel but separate universe from the NetID. Recently, the barcode has been added to LDAP, but the NetID is still not being placed on the WildCARD's

onboard cache of information. (The EMPLID is, but the NetID is not.) Usage of the WildCARD will only increase (e.g., the addition of RFID functionality into the card will enable touchless access, it could be integrated into the parking system or Ventra), and its unification with the rest of the IdM system should be prioritized.

Continue to reduce the use of separate University identities beyond the NetID

The NetID is the default means of identity for Northwestern, but there are still notable exceptions to its usage. (See page 12 for a list of some of the systems cited in focus groups sessions for not using the NetID for authentication.) Wherever a Northwestern credential is required, we should work to make it the NetID. This is also true for handling people with elevated permissions for FASIS and SES. The process of creating special IDs for people with elevated access to FASIS and SES should be discontinued, bringing it in line with NUFinancials, and eliminating one of the blockages to integrating these systems into the University's web Single Sign-on system. The current procedures should be replaced by a process that utilizes multi-factor authentication to enhance security on these identities, leverages online workflows to improve the speed and auditability of the process, and externalizes this status outside of the relevant system so that it can be used by other workflows. (See the discussion of secondary attributes on page 38.)

Reduce Duplicate Identities

There are multiple opportunities for reducing duplicate NetIDs which cause negative experiences for members of the Northwestern community, giving them poor impressions of Northwestern and NUIT at the beginning of their relationships, and resolution of these situations has a high overhead on staff resources. Aside from their role in creating duplicate NetIDs, eliminating/reducing the use of manual NetIDs also has positive implications for auditing, security, and reducing the overall complexity of the IdM system.

Reduce duplicates created within FASIS/SES

The FASIS and SES systems are capable of creating duplicate identities on their own when existing records are not found via the matching routines they employ. In these situations, reducing inadvertent duplicates is all about improvements in data entry, data quality assurance, and searching/matching.

Reduce our Dependency on Manual NetIDs

The situations involving Manual NetIDs are also about searching and matching, but the situation is more complicated. It is hard to imagine not needing a means for managing identities for people who do not come to the University via the core hiring and matriculation paths. Theoretically, manual NetID functionality could be improved to require a more robust personal attribute set at the time of creation, and search/matching functionality could be enhanced internally within NUValidate and externally to SES/FASIS. However, this functionality is a custom module that has been built onto NUValidate, and the goal is to replace NUValidate by the end of 2016. At the very least, no effort should be invested on enhancing the existing NUValidate manual NetID functionality, and it seems unlikely that resources should be invested in recreating this functionality in whatever succeeds NUValidate. Instead, attention should be focused on two areas:

1. *Low-hanging fruit*: Improving the awareness of the problems surrounding Manual NetIDs, and the existence of alternatives to using manual NetIDs in some cases could be helpful. Improvement in the business processes in the distributed units for creating NetIDs – e.g., developing templates for keeping records, getting people to fill in all fields accurately and completely, improving communications with the person getting the NetID to see if they've ever had one before, perhaps moving the responsibilities for maintaining these identities to the HR team in the distributed unit, etc. – could all prove useful in lowering duplicate NetID issues.

2. *Transformation*: Engaging in a conversation about the possibilities of reducing, and perhaps even eliminating, the need for Manual NetIDs will give more benefit in the long run. If there are resources where there is no longer a need to require the use of an existing credential, such as was done with the guest wireless network, that transition should be done.

Where the use of a credential is still desired, a bigger push on federation (see below, page 48) can help a lot in this area. (It was stated in one focus group that 90% of the manual NetIDs that need NUFinancials access are from NMFF/NMH.) Where possible, this federation should be done with other institutions with solid identity management processes. For less sensitive situations, the federation can be done with lower levels of identity vetting (e.g. with social identities), but usage of these credentials can also be coupled with active in-person vetting of people and identities to increase the level of assurance associated with the credential. (See the section on Assurance and Trust below, page 44.)

For people who don't fall into either of these categories, and we still want to give them a NetID, these people might be required to go through an HR-or SES-like process to be entered into the official systems of record (FASIS, SES) to get NetIDs, perhaps using the existing FASIS POI ("person of interest" category. People who might fall into this category are people with a "non-employment" relationship, e.g. contractors, who need access to NetID-authenticated resources such as legally/contractually restricted data, or use of the University's Virtual Private Network (VPN). To be clear, however: if the FASIS POI process came to have a role, it would not be simply to give them an identity. It would be because they need access to resources that are restricted to NetID access.

Create a Central Registry Service

In order to move into a world in which we're interested in more types of people over a longer period of time, and in which we want to provide access on a more granular basis to a larger set of online resources, one of the things we need to do is change the way we store and make personal attribute data available.

Identity attributes are useful for three functions:

a. influencing access decisions at run-time,
b. structuring the association of entities within organizational units, and
c. influencing identity lifecycle decisions.

In other words, the attributes of an identity affect both what the entity can do in all systems and how the identity management system itself handles specific changes in the status of the entity.

Today, the information that is available centrally is tied to the NetID and is a relatively narrow set of information contained in LDAP and (to a lesser extent) in the various Active Directory domains. These directory services are becoming a legacy approach to providing identity attributes. In the future, most identity and demographic attributes will be acquired through Web Service calls that retrieve data from authoritative data sources (e.g., FASIS, SES) and not just LDAP or AD.

To address the needs detailed in the rest of this section, a second architectural cornerstone is proposed: a common census of persons, accessible through a central registry:

IAM Architectural Cornerstone #2:
A central registry should be built to provide access to a more robust set of data (than is currently available via LDAP) about a broad spectrum of people with a relationship to the University (i.e., not just those with NetIDs). Each person's information should be tied to a unique identifier that is not an already existing University identity or identifier. Most of the data will be accessible virtually (rather than being replicated to a database).

This registry will be managed centrally as a service to all business functions. It will include all people who have relationships that the University wants to track (e.g., not just those with a NetID, not just alumni, not just students in degree programs, not just faculty and staff). The NetID – while still being the primary identity of

the University – would become one of multiple identities and identifiers that could be attached to a person, all of which would be accessible via this registry, which will also make available a more robust set of data (described below) than is currently available via LDAP.

In other words, there are a set of high-level principles that should define this registry:

1. a centralized clearing house for obtaining data about people;
2. a resource that relies primarily on providing access to data in authoritative systems rather than replicating that data in a central location;
3. a resource for obtaining historical as well as current information about people;
4. a way to connect, into a single location, identities and identifiers for the same person from multiple sources.

While the exact nature of this registry remains to be worked out, there are several things that it is known NOT to be. It is not:

1. a massive database containing lots of replicated data
2. a system that provides flat-file data feeds to applications
3. a newer, more complete AD domain or simply putting more data put into LDAP

The following sections flesh out the types of information that will be accessible via this new registry.

Better Data

Generally, identity attributes are assigned to, or removed from, particular entities through three types of assertions:

1. authoritative system assertions,
2. distributed processes which approve access to resources not administered centrally, or
3. formal administrative processes which approve specific access requests.

To make the widest possible use of identity attributes - regardless of source - they should all be visible or obtainable through standard means. For traditional directory services, this means all attributes would have to be present within central directory services. In the new Service-Oriented Architecture (SOA) model being deployed at the University, data could remain housed largely within authoritative systems and be retrieved via web services rather than being copied to one or more directories. Composite SOA applications could take as input a variety of identifiers (NetID, email address, EMPLID, alumni ID, etc.) and then assemble data from multiple sources for presentation back to the calling application. Composite applications could be developed and maintained centrally to meet common needs; schools and departments could use those as building blocks to create applications to meet more specialized needs. In some cases (perhaps most cases), this would eliminate the need for local Active Directory instances and mass replication of data to LDAP. The ability of schools and business units to create and maintain local identities on their own will need to be preserved, possibly through utilities such as Grouper, which could synchronize group memberships across different directories, databases and other repositories. (See also the discussion of SOA as an architectural cornerstone in the section on Integrating Identity and Access Management, page 42.)

Currently, only the first type of assertions are available centrally, and there are relatively few of them, e.g. basic demographic information such as faculty, staff, Kellogg, Medill, etc. The set of data that is collected in this registry needs to be expanded. Included in this expanded set of data would be the "profile" information that was requested in multiple focus groups: information on a person's multiple relationships with the University, both present and past. (See the sections on the need for persistent data about multiple

relationships, page 19.)

It should be noted that this central registry is not intended to archive permissions of people when they leave. While some participants in the focus groups wanted to be able to check a box that said "give this person the same permissions that the previous person had", the risk of misapplying old permissions has a potentially dangerous downside to it, and the goal recommended here is to not do this. Instead, the recommended path is to set aside the NetID to reduce the number of mistakenly duplicated identities, and to help people "pick up where they left off" – e.g. a person who left comes back in the same role, or a new person is hired to replace them -- the ability to provision permissions quickly (via online forms and workflows, preferably with options for permissions based on definitions of basic roles) should be emphasized instead of trying to retain a person's permissions. Work of this type is beginning to happen around NUFinancials access permission processes, and to the extent these roles are able to be defined and utilized, they should exist in the central registry, outside of the application that develops them, so they can be used by other purposes when they are relevant.

Assertions of the second type are currently confined mostly to local Active Directory instances where they instantiate school or departmental group definitions and other attributes for organizing assets or controlling access to file systems. If access is to be provided more granularly by more applications, an expanded set of attributes about the person and his/her status needs to be readily available. For instance, having access to a more detailed set of organizational data about people becomes increasingly important as more shared services are deployed centrally. This is particularly true for collaboration services, which are deployed to smaller groups of people (e.g., Box.net and SharePoint), some of which are formed on an unpredictable, as-needed basis.

The third type of assertions are held separately within each system's security tables and are not visible outside those systems. If these assertions are instead promoted to what we'll call a "***secondary attribute***" within a central registry service, many business rules could be written for manipulating the access permissions and identity lifecycles of entities with access to these core systems. For instance, approved access for SES, FASIS, and NUFinancials could become attributes in this registry, e.g. OK-SES, OK-FASIS, and OK-NUFIN. Today, this status is known only to the owning system, lying buried in its internal security tables. Externalizing it as a flag within the identity management system allows other systems to incorporate it into their own business rules. For example, the identity management system could build logic into its system that says if either OK-SES or OK-FASIS is flagged, password lifetime could be shrunk from 365 days to 180 days, and if OK-NUFIN is checked, it would shrink to 90 days. Similarly, the identity management system could use this information to adjust rules on unsuccessful login's, varying the number of permitted unsuccessful attempts and the action taken once the threshold is reached (e.g. extending the wait period vs. disabling the ID) depending on the levels of access associated with an ID. In these cases, the identity management system is changing its own behavior based upon permissions granted to the entity and reflected in the assigned attributes.

New Data Structures

Making these new sets of information available should be based on a new approach to storing the data. The University's new web services infrastructure should make rethinking how data is accessible and maintained in this new context a high priority. While some attribute data may continue to be replicated into directories from authoritative sources, this is not required. In fact, this repository could be an entirely virtual database containing links to multiple different sources of data, e.g. the central identity database managed by the identity system, centrally stored organization and personal attributes, even links to distributed local attributes or attributes collected specifically for functional areas (e.g. the researcher-specific information discussed in the working group paper on A New Vision for Research Administrative Systems). The application making an access decision should not have to know where the authoritative data resides, and the data need not be replicated in this centralized registry (though the registry could be used to house additional sets of data, e.g. multiple visa numbers, if the data schemas in the authoritative systems can't incorporate these extensions).

A Different Focus for Identity Management
This single source of data should include all people who have relationships with the University that should be tracked, not just those with NetIDs. By definition, then, the unique key that identifies people in this database will not be the NetID, though there will still be the premise that there will be no more than one NetID per person, just as there should be no more than one WildCARD barcode and one EMPLID per person.

There will also be other identities stored in this database, for example, federated IDs from peer institutions or from consumer-oriented businesses such as Facebook, LinkedIn, Microsoft, Google, etc. How these identities might be used within Northwestern systems is described below, but the point here is simply that one person will have multiple identities, each of which will be stored in this central registry. (See the discussion below on Optimizing Assurance and Trust, page 44.)

As part of creating this centralized common census, the tasks of avoiding duplicate identities will grow. More people will be included in this census, they will come from more sources, and it is possible that each person will have multiple identities attached to them. This means that the task of avoiding duplicate identities will also become larger and more complex, and the value of doing it well initially, and over the lifecycle of an identity, will become even greater than it is today.

NUValidate currently does this work when requests for NetIDs are forwarded on to it from authoritative systems. In the new model, the NetID will explicitly be just another credential attached to an identity, rather than implicitly assumed to be the identity. A NetID will still need to be managed throughout its lifecycle, but the identity system will need to be a repository where additional credentials are stored and managed as well, e.g., the WildCARD, multi-factor systems, biometrics, perhaps a digital signature, and registered third-party credentials. Some people in the registry will not have a NetID at all. Theoretically, a person could use different identities and credentials in instances where different levels of trustworthiness are required. Systems could theoretically allow access with a variety of credentials, some may restrict different types of access to different types of credentials, and some systems may choose to accept only certain types of credentials (e.g. only NetIDs).

As a result of this change, this matching functionality needs to be externalized from whatever replaces NUValidate and used for more than just NetID creation. Because of its increased complexity and importance, this census of persons should be managed more closely to avoid wasting labor resolving errors and questionable practices, and where possible, tools should be available to correct mistakes.

Moving to this common census of people is obviously not a trivial task, and it does not have to happen all at once. Not only does it need to be conceptualized and built, the surrounding applications need to be retooled to make use of it. However, given the changes in the environment in which we live, we see this as a fundamental piece of the new architecture that will qualitatively change how the University's is able to do its business.

Integrating Identity and Access Management

IAM Characteristics addressed in this section:

3. Identities and access to resources are provisioned and de-provisioned rapidly in alignment with the need for their actual usage, with easily auditable trails.
4. Authorization is appropriately granular and based on robust identity information.
5. Surrounding business applications are integrated with the enterprise IdM system.

9. Business applications and the IAM infrastructure are flexible and easily modified to take advantage of new IAM technologies as they emerge and become stable.

Enabling Improved Access Responsibility

In order to optimize agility, responsiveness, and customer experience within our portfolio of online services and resources, the responsibility for making access decisions ("authorization") needs to be more fully shifted to the applications, and the applications have to be less inwardly focused and less passive about making these decisions.

The number of services offered online is already far too large to centralize all the access logic for them. Even the relatively limited set of "special access" cases that are programmed into the NUValidate system makes the identity system brittle, and hard to maintain and upgrade. Making access even more granular is not possible within this model, and the number of services that will be made available online will continue to grow.

Similarly, the larger the system – e.g. NUFInancials, InfoEd, FASIS –the smaller the likelihood that a one-size-fits-all approach to access management (is the NetID active or inactive?) will be sufficient to appropriately manage access to its own range of functionality across the entire lifecycle of our increasingly diverse set of constituents. This, then, is the third cornerstone of the new IAM architecture being recommended:

> **IAM Architectural Cornerstone #3:**
> Authorization, the permission to access resources, needs to be handled by the surrounding business applications, not by the identity management system. Applications must become identity-aware pieces of an integrated portfolio, rather than heads-down, internally focused silos, and authorization should be flexible enough to open access to individual services as needed.

In short, the Access Management side of IAM needs to do more work than simply seeing if a NetID is active or not, and the applications doing this work need to be better integrated with an improved and restructured Identity Management side of IAM. Ultimately, we need to move to the place where NetIDs are no longer turned on or off. Instead, they will be an enterprise credential, that a person does or does not have, and each person's access to online resources will be handled by the system that provides the resource, based on attributes that are available to it on a real time basis.

The following sections talk about two key factors in improving the integration between identity and access management: smarter applications and more integrated applications.

Make Applications "Smarter"

In order to change the current application access decision process based on the active/inactive status of the NetID, the following needs to happen:

1) The applications need to look outside themselves for identity and personal attribute data at the moment when the access request is made, or, next best case, when personal attribute information changes for people who use that system. Either way, the application needs to be more identity aware, on a real-time basis, of the status and attributes of the people requesting its services instead of trying to stockpile more attributes internally. (See the discussion of a Service-Oriented Architecture below, page 42.)

One example of the latter case is the Library's turnstile system, which might want to store information about who is eligible for library access locally to guard against network outages. However, rather than stockpiling that information via overnight feeds, the information should be updated on a per-individual, real-time basis. In these cases, the application must be capable of realizing a change has occurred in a person's relationship with the University, and be capable of acting upon that change. The declaration of a change may come from the IAM system, but could also easily come from an authoritative system (FASIS, SES, etc.)

2) Applications need to fully own their access decision-making process, and they need to be able to make more finely-tuned access decisions, which will be based on a more thorough understanding of exactly who is requesting access, e.g. knowing all of a person's roles, not just their primary role.

There is one important caveat to this distributed authorization model: while the limitations of a single yes/no source of access permissions are obvious, this does not mean that the enterprise infrastructure should not have this capability. In most cases, the control should be more nuanced, but there undoubtedly needs to be the capability to quickly shut off all access in some circumstances. (See the section on web Single Sign-on on page 43 below for more on this.)

The Role of Roles

When people talk about an ideal identity management system, they usually speak glowingly of a system predicated on roles (groups of attributes that, when taken together, lead to the provisioning of access to sets of resources). These roles are usually projected as enabling the automatic provisioning and de-provisioning of access in real-time. While developing roles is a key factor in the IAM environment that is envisioned here, its scope is smaller than what is often implied in casual conversations about IAM.

It is our belief that once one needs to define access permissions for many real-world resources, the need to parse the "role" of someone often quickly becomes quite complex, taking one outside of what is typically defined as a "role", and into a more complex set of "If… then … else" sets of logic. A recent example of this is related to understanding who needs what access to various RCR (Responsible Conduct for Research) training. A simplistic role-based perspective is anyone who is a researcher. However, the reality is that it is much more complicated. Even the role of "researcher" who is "NIH" or "NSF" would also fail to be granular enough for the stated business requirements of the campus. Adding a role of "School" would still not resolve this. Different departments have their own RCR training requirements and may apply them to people in different fashions (even going beyond the granting agencies requirements). In other words, this logic cannot be resolved simply by adding roles to the IAM system; it can only be resolved by building the business logic in the business system. The detail that is needed starts with commonly used roles, but in order to achieve the specificity which is often assumed when we talk about a proper system having the roles to make these determinations, using this type of complex logic to create roles would result in an unmanageable number of very granular "roles".

Similarly, to build the overarching roles that are often posited in these discussions, one would need consolidated documentation on the relationships people may have with the University, and the permissions associated with each of them. While it would be good to begin to consolidate this information, the cost/likelihood of success ratio associated with spending time up front trying to define and agree on consolidated roles is usually not favorable. In most cases, it is more important to have the required personal attributes available, to have the application do the "If… then … else" logic with the attribute values, and to look for similarities as these sets of logic get defined so smaller roles can be defined when appropriate, and then expanded as more appropriate use cases get identified.

This is not to say that the use of roles will, or should be, non-existent. Some roles can be built on higher-level attributes, and this has been done in several functional areas already. However, each of these successes has also realized that the 80-20 rule definitely applies in this area. (For example, NUFinancials has looked at their permission requests and have seen that the majority of their users request low-risk access, while the remainder of their users needs a variety of access levels.) In some cases it might even be possible to tie job categories to roles. For instance, the role of a department assistant 2 might contain OK-NUFIN because all department assistants will use that system in their work. Where it is possible to automate the association of roles to job categories, automating the work process for granting permissions can be envisioned, with necessary checkpoints and approvals built into the work flow. In other words, role-based systems could spawn access permission request workflows that start with a default set of permissions, but they would not

automatically grant access. The automation would aid by having standard sets of permissions to start with, rather than relying upon someone to launch a set of requests separately and from scratch.

Integrate Applications Better – SOA and SSO

SOA – Service-Oriented Architecture

If more is expected from the applications, they need to be better connected to the IdM system, largely through the utilization of real-time service calls that will be available through the enterprise Service-Oriented Architecture (**SOA**). While the growth of our SOA architecture will not have a great impact on the actual authentication step (which will probably continue to be via an LDAP bind, Active Directory, or Web SSO (using LDAP as a back-end data store), it will play a very important role in providing personal attribute information to the applications on a real-time basis and helping with the optimization of assurance discussed in the Optimizing Levels of Assurance and Trust section that follows this one.

Therefore, the web services that are the basis of SOA are the fourth cornerstone of the new IAM architecture being recommended:

> **IAM Architectural Cornerstone #4:**
> Identity and access management processes need to be done online utilizing web services that provide real-time and workflow functionality based on data for individuals.

As just noted, these might be service calls at the time of the access request to verify the status and attributes of the person making the request, or they might be a service that "publishes" a change in status -- e.g. that a staff member has moved from the Dean's office in McCormick to the Bursar's Office -- and then, because a system has "subscribed" to all such publications, it is coupled with a corresponding service within the subscribing system that harvests the relevant information and updates the personal attribute data and/or security tables it stores internally.

Being connected via services that pass information about individuals on a real-time basis will also enable provisioning of initial access (and de-provisioning as a result of a change in status) to be as quick as the associated business process would like it to be. Moving towards a web services architecture will enable very different processes for identity and access management, but the technology is only an enabler. Any sort of qualitative change is also very much about how business processes are defined and executed.

This puzzle has two sets of components: (a) the processes that create identities, preserve them, and eventually retire them, and (b) the timing of authorizations granted to identities (NetIDs) by applications and the workflows for establishing and removing those authorizations. For example, when an employee separates from the University, the first portion describes how long the electronic identity remains visible in directories or how long credentials remain usable. The second portion describes what business functions would be immediately suspended or would be preserved for a period of time and for what reasons.

Many focus groups expressed bewilderment at how these decisions are made and whether they are coordinated (e.g. needing to see final paycheck information conflicts with disabling the NetID). Confusion about, and misunderstanding of, policies surrounding authorization to functions and information can only be resolved by service providers taking control of those decisions based upon identity and relationship information – and then documenting them and publishing them for their customer community. Multiple focus groups said that simply knowing what services get turned on and off, for whom, and at what point would be very useful knowledge to be available, not only for the people affected by these changes in service, but also by those people who administer the services or assist the affected parties. But this information is not centrally stored or tracked. Adoption of SOA allows us to build the foundation for this sort of information, but it is only a necessary step, not a sufficient one. Creating a University-wide service catalog, complete with eligibility rules, would be a very large project. A better start might be identifying a handful (6-12) of critical systems, then documenting and publicizing the rules they use.

Migrating to integration via services is not only driven by the desire to become more "real time", it is driven by the movement of applications to "the cloud" (To mention just a few of these systems at Northwestern: admissions, student career services, student email and collaboration, survey tools, payment of student fees, alumni community, athletic ticketing, the library's central administrative system, software test environments, file storage/sharing, employee healthcare management functions.) The movement of our application portfolio off campus and into the cloud exacerbates technological strains already apparent in our ecosystem.

On the one hand, third-party cloud applications increasingly presume the existence of web services and API's (application programming interfaces) for connecting to the University's identity management system or updating data in the enterprise systems. When a vendor is equipped to use the identity services we have in place, deployment can be a matter of days. When we don't have what they use, or they require a data feed just like our on-campus applications currently do (just because an application is in the cloud, it doesn't mean that it uses the latest solutions for data transfer or identity management), integration will be much more protracted.

We need to get out of the business of doing integration via individually tailored batch data transfers. Instead, we need to prioritize our ability to integrate external vendors easily via web services and APIs to reduce the time and effort required to integrate new applications, and to reduce the risk associated with the proliferation of data via the transmissions of batch data feeds. Not only do we need to be emphasizing our ability to do this, we also need to be pushing our vendors to incorporate these standards and approaches.

Single Sign-on (SSO)

Applications also need to be better integrated with the Identity Management System via the adoption of the enterprise web Single Sign-on (**SSO**) infrastructure as the Northwestern standard. This integration provides:

- An important convenience for users of Northwestern systems: no need to login more than once or twice per day in order to gain access to many systems.
- Additional authentication factors (smart phone, hardware token) can be integrated into the SSO system rather than each individual application. Records of the use of these additional factors can be maintained in the SSO system as part of other session information, and queried by the application when needed; e.g. to require multi-factor authentication for access to certain functions or sensitive data.
- A building block for expanding the functionality, and hence the value, of NUPortal.
- Two valuable security controls: 1) should there be a need to quickly suspend access across a wide set of systems, the SSO infrastructure provides a single "choke point" on an identity, and 2) applications using SSO don't need to hold, even for an instant, clear-text usernames (NetIDs) and passwords. NetIDs/passwords would be only collected by the SSO system, which would pass out tokens where they're needed, thereby decreasing the risk that passwords could be obtained or disclosed either accidentally or by deliberate abuse.

It needs to be noted that not only should the applications change to be more integrated into the SSO infrastructure, the SSO environment needs to be more predictable and convenient. For example, entering or exiting from an application should not affect credentials already accepted by another application. If applications are not sensitive to the possibility that they might not be the only application in use during the session, then the local cookie holding the record of SSO authentication will be discarded when "logging out" of one of the applications, potentially causing unpredictable states with other applications (e.g., triggering a new authentication challenge). For instance, when a staff member logs into SES, it puts a cookie into her browser. When that staff member then logs into NUFinancials, the SSO system will see that cookie and will not require a new authentication. But if the staff member logs out of either application, how the other log-ins will be

treated depends on how the cookie is treated, i.e., do the other applications remain gracefully open, or does one or more of them get unceremoniously terminated? It needs to do the former rather than the latter.

The installation process for applications using SSO should be simplified. At present, applications must install agent software directly into the web or application server layer. This has proved difficult or impossible, sometimes for technical reasons and sometimes due to licensing restrictions. Setting up SSO on simple HTTP/S proxy servers is a likely solution, as is direct SAML integration with our federated authentication infrastructure. Other options should be investigated as well, and it would probably be good to increase in-house expertise on doing these integrations and/or look at budgeting for consulting assistance.

Eliminate Paper - Move Processing Online

Systems being able to get access to changes in status on a real-time basis is only one element of improving the speed of the IAM processes. On-boarding and off-boarding also involve people – people who make requests for access permissions, people who review and act upon those requests, and people who go through status changes (e.g. getting a new job, changing a job, ending a job) – and these people need a way to interact with these changes or requests for changes. The more these interactions are tied to paper, the longer they will take and the less transparent they are.

Moving these processes online immediately speeds them up, makes them available for everyone to see their status and raise a problem if one occurs (e.g. plans have changed and the separation date won't be until two weeks later), makes them reviewable to help improve processes, and makes them easily auditable. Eliminating paper and moving all IAM processes online should be an overarching goal.

This paper purposefully leaves aside any discussion of electronic signatures that are needed for legal documents and hopefully restricts itself to workflows and electronic "sign offs" that do not require this level of identity proofing. For instance, multiple focus groups cited savings that could accrue if there were electronic workflows where a person could review a document or a report of financial transactions and check a box as one does with University time sheets. ("If a Principal Investigator could electronically acknowledge their monthly budget statement has been reviewed and approved, it would save a staff person in every department lots of paper and storage." "The paper -> pdf -> paper + signature -> pdf process is laborious and inefficient. 90% of the documents that go through this process are internally generated and many cycles of effort could be recouped by turning these into online forms with electronic approvals.) This restriction does not mean that pursuing this higher level of "signature" is not worthwhile. It simply means that this need was not a recurring topic in the focus groups, and it requires a significantly greater amount of effort and resources in the context of an already large set of resource requirements.

Optimizing Levels of Assurance and Trust

IAM Characteristics addressed in this section:

5. Surrounding business applications are integrated with the enterprise IdM system.
6. The level of rigor employed in identity proofing and authentication at the time of access is based on the risk and value of the transactions to be done

Assurance and Trust Overview

This section is about the fifth cornerstone of the new IAM architecture being recommended:

> **IAM Architectural Cornerstone #5:**
> The Northwestern NetID will remain the core Northwestern electronic credential, but its role needs to be supplemented by external credentials and by other means of insuring identity trust and assurance.

Granting access to resources results from the successful completion of two steps: authentication and authorization.

- *Authentication* answers the question: "Who is this entity and how confident are we that this is the exact entity we believe it to be?"

- *Authorization* then answers the question: "Given the answer to the authentication question, and any other information available about the entity, what functions and data items should be made available for this entity's use?"

In order for the access gateway to be properly protected, the process of answering the authentication question needs to optimize, in relation to the value of the resource to which access is being requested, the extent to which it can establish two types of certainty about the identity: the level of "assurance" that is attached to the identity, and the level of "trustworthiness" that is attached to the credential presented for authentication.

- "*Assurance*" refers to our level of confidence that our electronic identity of a person is accurately associated with a real person, and the correct person.

- "*Trust*" refers to our level of confidence that the person offering the credentials for authentication is actually the person to whom the credential was issued.

The more valuable the resource, the higher the levels of assurance and trust should be; and the higher these levels need to be, the more difficult it should be to get authenticated. Levels of assurance rise along with the number of independent attestations that are presented, and the basis for those attestations. For instance, having someone show up in person and present multiple government-issued photo IDs provides a much higher level of assurance than receiving a request for access based on the self-service online entry of a Facebook or Google credential. Levels of trust also rise along with the type and number of credentials being presented.

Let's take an example from Northwestern. Theoretically, Professor Jones might have the following credentials:

1. A WildCARD issued through standard processes
2. A NetID issued through standard processes
3. A second factor password generator, e.g. a smart phone number for a phone with a multi-factor app on it
4. A fingerprint scan, taken by a Northwestern office, and kept on record
5. A Gmail account

Professor Jones has the following access needs:

a. Buy NU athletic event tickets
b. Read her email
c. Approve payroll timecards for staff
d. Purchase hazardous chemicals for her research from a grant
e. Enter into her laboratory space where hazardous materials are used

The applications (a-e) must each decide which of the credentials they will require in order to be confident Professor Jones is - in fact - making the request. The decision will rest upon a balance between convenience and security/compliance.

For example, "b" and "c" currently require #2, and there is no one asking to change this at this point in time. The level of trust and assurance provided by NetIDs are appropriately balanced with the value of the resource being accessed. However, because NU Athletics ("a" above) wants to serve the public, a NetID is out of the question for being the default credential for their system. Instead they might allow Professor Jones to create an account for herself within their system using Gmail proxy authentication (#5) rather than issuing a new credential (NetID or otherwise) to her. On the other end of the continuum, a NetID or a WildCARD by itself may not be appropriate for either of the latter two ("d" and "e") cases. It may make sense for "d" to require a NetID and second factor authentication process, and "e" might require a combination of swiping a physical WildCARD and having one's fingerprint matched with it.

Each of these credentials have different levels of trust, and combining them in different ways can increase the trust in a particular authentication event. It should be noted that it is vital that assurance be high when issuing what will be considered high trust credentials. For example, it makes no sense to use biometric security if you are unsure if the person involved is really the individual who is supposed to be granted access at so high a level of trust.

Identity assurance ranges from very low (self-attestation) to moderate (one or more third-party attestations) to high (photo IDs, biometric cross-check with government databases, background checks). There may be applications which will want to provide services to an entity only if the assurance is at a minimum level.

Since the original days of the SNAP system, the University's business application set has grown substantially, and its complexity has been multiplied by the world-wide reach of the Internet, AND the lowering of barriers to application provisioning via cloud-based vendors. At the same time, the breadth and complexity of the Northwestern community has grown in parallel, along with a changing set of expectations about the ease of access provisioning that should exist. Clearly, the relatively "heavy" process of NetIDs, even in combination with Manual NetIDs and their much lower level of assurance, is no longer sufficient to provide an authorization process that is appropriately optimized for the range of online resources we now provide. The following section enumerates the ways this process needs to change.

Increasing Trust

In these times of phishing, social engineering to steal credentials, and increased concern about compliance and the security of PII and PHI, it is important to improve our ability to increase the level of trust in certain authentication situations. As noted above, there are multiple ways this can be done utilizing bio-metric methods of authentication and multi-factor methods of authentication. Both of these authentication methods have improved and become easier to deploy, and with the near ubiquity of cell phones these days, purchasing separate key fobs to provide a physical authentication factor is no longer necessary.

Just as a one-size-fits-all approach does not work with NetIDs, adding in these levels of trust needs to be done selectively, adhering to the adage of needing to optimize levels of assurance and trust in relation to the value of the resource. Interestingly, utilizing some of these higher trust authentication methods can also decrease the difficulty of authenticating. For instance, some universities are now using bio-metric scanning devices for residence halls, dining halls, laundry rooms, etc., eliminating the need to carry a physical credential such as the WildCARD, and also speeding up the authentication process.

Multi-factor authentication may also help in the transition away from an authentication dependence on physical location. Many of our most sensitive resources require a physical presence on campus (as attested to by the use of a network IP address that is a Northwestern IP address). If one is not physically on campus, then these resources can only be accessed via VPN, which was frequently mentioned as an irritant to members of the community, and a burden to support teams. While auditors love the requirement that access to these systems is restricted by physical proximity, we should seek to reduce our dependence on physical location

alone and towards person- and risk-based (e.g., logins from unusual locations or at unusual times may require additional means of authentication) means of authenticating.

Reducing our Dependence on the NetID

At the same time we need to strengthen our authentication processes for some resources, supplementing the levels of trust that accompany a NetID, we also need to move away from relying on the NetID so much in other situations.

For people who are less directly connected into the daily fabric of the core Northwestern community, being forced to rely on a NetID for access to Northwestern resources -- getting one, remembering it and its associated password, and dealing with on-campus support when problems arise with it -- often reduces their productivity and positive attitude to their Northwestern experience, while also increasing support loads for Northwestern administrators. There are two ways this can be done in appropriate situations: distributing the control of access management, and using identities offered by other entities. Each is described below.

Distributing Access Management

In some instances, requiring that the owner of a resource use a centrally-vetted and controlled identity to permit access to their own resources is counterproductive to the shared goal of protecting University resources. File sharing is a classic example of this with the rise of Dropbox and the availability of free gigabytes of storage from whichever major cloud vendor (Apple, Google, Microsoft, Amazon) one prefers. Without a well-developed sense of risk and a commitment to support University requirements that institutional information is managed from an institutional perspective (institutionally accessible, secure, backed up, etc.), gaps in functionality between these tools and tools offered by the University will often lead Northwestern faculty and staff to choose personal productivity over the risk of compromised confidentiality.

Unfortunately, in an age of increasing collaboration beyond the traditional on-campus boundaries of the University community -- in research, community involvement/projects, experiential learning, and work with consultants -- limiting University file sharing tools to NetIDs drives people to these less secure, but highly available alternatives. In some situations – e.g., research projects with regulated data – it may well be appropriate to continue to require this set up, and to continue to educate people why there are these expectations. In many other relatively similar situations, however, it may be more appropriate to delegate the control of access management to the person who controls the resources, and rely on their direct connections to their collaborators to supply the needed levels of trust and assurance.

Suppose, for instance, Professor Jones wants to share her research files with a co-researcher at the University of Arkansas and a former student now in the private sector. Unlike an anonymous relation handled by a centralized service, Professor Jones has close personal relationships with these people, has a close working relationship with them, and the odds that the email address is not used by that person, or that the person is not really the person they say they are, are quite low. And when the basis of authentication needs to be changed – e.g. the colleague gets a new job at the University of Wisconsin – or the need to collaborate ends, who is going to know quicker, or have more of an incentive to update the authorized IDs, than Professor Jones will? This on-going personal relationship, in effect, give a higher level of assurance to this external identity.

These situations are similar to the idea behind Manual NetIDs – delegating control over identities beyond the processes attached to the core systems of record. However, this scenario is fundamentally different in several ways:

- The people in the assertion process are closely linked instead of being anonymous to one another.
- The process is handled directly by the person who has a vested interest in, and control over, the resources.

- The identity that is used is already very familiar to the external person, and often it is one that is also known to the person controlling the access.

The same concept, but taken to a further extreme, underlies the deployment of a guest wireless network. Prior to this implementation, anyone using the University's wireless network had to have a NetID. Now, a separate guest network (separate from the regular University wireless network, which is still NetID authenticated) is available, with only a self-reported name and email address required for access. This approach has worked great with parents of students and prospective students who are visiting campus, with guest lecturers, recruiters, and contractors, and on-campus conference and meeting attendees, all of which used to need a NetID to get wireless reception on campus.

In each of these cases, the NetID, with its centralized control, is no longer being utilized as the credential, and the levels of assurance and trust attached to the credentials have been adjusted, though not eliminated, to balance risk with trust and ease of access.

Identity Federation

Another way to reduce our dependence on the NetID is also built around using a credential with which the external person is already familiar: extending Northwestern University's identity management system via federation. When institutions federate their IdM systems, members of one institution can use the credentials they already have for accessing services in the other institution. This enables people who have a more removed connection to our community to use a credential with which they are already familiar to access Northwestern resources (and vice versa: when Northwestern federates with other institutions, members of Northwestern can use their NetID to use services in the federated institution.). It also minimizes labor required to grant and support appropriate access to University assets, thereby enabling us to integrate people and systems much more quickly. We need to utilize this approach wherever possible, and we therefore need to improve our infrastructure and expand our options in this space.

- Multiple standard protocols should be available to connect applications from a wide range of third party vendors easily and directly into our identity and access management ecosystem. The security assertions markup language (SAML) protocol is widely deployed and supported by Northwestern today. Other standards are emerging (OAUTH, OpenID Connect) and should be investigated and deployed as appropriate. (See the earlier discussion of standards in the area of authentication, pages 27 and 29.)

- Medical campus partners must be incorporated into the overall access and authorization plan. Integrated MS Active Directory services appear to be the best approach for direct collaborations between Feinberg, the hospitals and medical practices.

- Research collaborators at other institutions should be supported through InCommon or equivalent services. While the University is a member of the Internet2 InCommon federation and has external partners with whom this service allows convenient NetID authentication, the InCommon technology is a niche higher-education solution that the University cannot assume will be implemented by potential partners.

Federation is also the concept behind using credentials from consumer-oriented vendors (e.g., Facebook, Google, LinkedIn, Twitter, Microsoft). These identities have much lower levels of assurance and trustworthiness associated with them: getting one only requires self-assertion of who you are, and these identities are recycled. Clearly they are not suitable for all IAM functions at the University. At the same time, it's a credential that is already very familiar to the person needing access, and for situations where there is less need for higher levels of assurance and trustworthiness, these can be useful, particularly when they are used in a context where the owner of the resources would know that the social identity is actually connected to the

person being granted access. Higher levels of assurance could be attained by business processes such as in-person or online identity proofing to match an external credential to a real person. ("Online identity proofing" could be done, as for instance banks do it, via links to public records databases: show 5 driver's license numbers, addresses, or car make/models, and then have the person pick the one that is actually theirs.)

Identity federation is already being leveraged in Our Northwestern for alumni. (In order to supplement assurance, Our Northwestern requires the person to answer some basic questions about their relationship to Northwestern before allowing information to be accessed.) Many other use cases exist where this approach could offer benefits: library patrons, students giving their parents or spouses access to their financial records and/or grades, life-long learners, practitioners involved in experiential learning situations.

The idea being outlined here is not that core constituencies of the Northwestern campus – faculty, staff, and students – will begin to have choices of using their NetID or a consumer credential to access University resources. Rather, it is that, for specific combinations of constituencies and resources, using these external credentials can be a better fit for balancing risk with ease of use. In each situation where this alternative is considered, business owners will need to weigh the complexity of University-issued credentials (e.g. NetID) versus the need to maintain direct, institutionally structured control of the identity process. Where the associated risk is acceptable, savings in labor, increased success of online service utilization, and increased constituency goodwill may be substantial.

Recording and Using Levels of Assurance

As we start diversifying our means of identity management, and improving our access management capabilities, we need to make the levels of assurance and trust that are attached to a credential available for use within the authorization process. For instance, we will be increasing our instances of federation, and the institutions with which we federate will undoubtedly have varying degrees of trust and assurance associated with their credentials.

We've already seen that, for instance, not all Google IDs are asserted with the same levels of trust or assurance. Some credentials are simply self-reported for services like the guest wireless network, some are submitted by a person who has answered multiple attribute questions about themselves (Our Northwestern), and some might be submitted by a person who is applying in person to use a University resource such as checking out a book and could easily show a current driver's license.

Similarly, it may be that one will be able to have a NetID with varying levels of trust. For instance, it may be that NetIDs get issued initially with lower levels of trust and assurance as a default, which get raised after their credentials have better levels of attestation. Or, it may be that a person is traveling when their NetID password expires. They are not able to renew it in person but they need to check their email. It's possible that the NetID could be reactivated with a lower level of trust that would allow them to check their email but not allow them to approve their direct reports' timesheets. This also illustrates why applications need to do real-time access provisioning that uses real-time identity attributes in this environment rather than relying on internal security tables with data lags built into their maintenance.

To be effective and efficient, the Northwestern IAM ecosystem must gracefully support this range of methods and situations. As access decision-making diversifies, the applications making these decisions will need to examine real-time assurance and trust levels, and wherever there are secure application requirements, those must trump convenient credentialing with lower levels of trust and/or assurance.

Revised Procedures for IdM

The requirement that people have a NetID to access University resources is a "heavy" process, with requirements to be physically present to get identities changed, the need to go through a limited number of entry points to get into the system, etc. These requirements are complicated by the changing nature of the

Northwestern community, where many of the people who comprise the core constituencies of the community – faculty, students, and staff – are increasingly dispersed geographically.

Being able to maintain appropriately high levels of security when needed becomes much more problematic in these cases. For instance, individuals are currently required to be physically present on Evanston or Chicago to reset a NetID password, but in many cases, these people are not on campus. NU Qatar, Medill's Washington Program, and Kellogg's Miami Campus are all established parts of the University, and in the case of many professional Masters programs, the students are away from campus the vast majority of the time; there are research and study abroad opportunities all over the globe; the number of affiliated partner institutions continues to grow; wholly online programs are growing. These opportunities (and their attendant requirements for identities to access Northwestern systems) will continue to grow, and as the set of people with whom NU has relationships grows, expanding in size and complexity, the mechanisms for maintaining our security need to change in order to lower the barriers to authentication and access.

Maintaining a Secure Environment

IAM Characteristics addressed in this section:

7. Identities are protected and secure.

More data will become available to more partners, both internal and external. Existing tools such as the Service Provider Security Assessment should continue to be used with all vendors hosting our data in the cloud. Processes and procedures developed for data access via the LDAP Registry, and those being developed for the emerging SOA infrastructure, should be consolidated, reviewed, updated as needed and widely publicized. Existing data categorizations should also be reviewed and updated as needed to reflect the increasing likelihood that data may be stored in the cloud and available to multiple external partners, not just stored within systems housed in NU data centers.

Similar policies and procedures should be developed for the use of identity trust and assurance. General guidelines are needed for assessing the risk level of various types of transactions. We also need to decide on a reasonable number of levels of assurance and trust (perhaps as simple as low/medium/high), then match each transaction type to the appropriate level of assurance and trust. Ultimately, those levels will be matched to technology, policies and procedures in the IAM systems. Individual application and data owners will then have to determine their own specific policies within those guidelines, and ensure that they are enforced by their applications – in part by leveraging data made available via the IAM ecosystem.

To the extent possible, data should be stored only in the system which is authoritative for that data. Copying and other replication should be done only when a compelling business need cannot be met in any other way.

Implementation of multi-factor authentication will provide added security functionality on multiple fronts. It will assist in meeting some compliance requirements (e.g., HIPAA); it will supplement our password requirements; it will improve the security around sensitive data by raising the trust levels associated with authentication requests, and it will minimize the impact of people mistakenly surrendering their NetID/password in response to social engineered attacks, e.g. phishing, links to false sites.

Some investigation of the InCommon Assurance (for a brief discussion of InCommon and its assurance levels, see page 27) has already been done and needs to continue in light of discussions related to assurance possibly being required for access to granting agency systems. Full compliance with "Bronze" or "Silver" level requirements would require significant changes to many portions of the central IAM ecosystem, as well as some systems hosted by schools and departments. Multi-factor authentication may also help achieve compliance. Up until now, the need for externally-certified levels of assurance hasn't been compelling enough

to undertake the large body of work, but that should be revisited within the context of evaluating LOA and trust.

Barriers to our achieving Bronze certification include:

1. One requirement is that software in the IAM ecosystem be "up to date" and "supported". Our IdM system has been declared end-of-life by the vendor and would probably not pass an audit. Another component (LDAP Registry) has a more clear upgrade path and more current support, but may still not pass audit.

2. Passwords used in Bronze transactions must *never* be transported without encryption, neither as part of a federated transaction, nor even for purely internal use. Some applications within the data center still use clear-text protocols. These could be detected and reconfigured with appropriate allocation of resources. Applications owned and hosted by schools and departments using local AD forests will be more difficult to track down and remediate.

3. The Shibboleth federation system supports Bronze and Silver, but would require significant work to integrate with other components of an assurance program.

Silver assurance requires everything that Bronze does, as well as:

1. Only "approved" encryption algorithms can be used to protect passwords and assurance-related transactions. Most of our web and application server infrastructure (Active Directory, Microsoft's IIS web/app server, Apache, Tomcat, the NU Portal software, PeopleSoft systems) support both approved and unapproved encryption standards in order to remain as compatible as possible with a variety of end-user web browsers and other applications. Silver certification requires us to disable unapproved encryption across all of the central *and* distributed IAM infrastructure, a task requiring 100% cooperation and compliance across the entire University.

2. A business process will need to be created to establish and change an individual's level of trust. This could include things like appearing in person to have credentials examined by a trained worker.

3. Substantial changes will need to be made to the IdM system in order to establish, maintain and report on the level of assurance currently in effect for each person at the University.

The investment required to meet even Bronze certification is large and likely not a responsible use of resources in the absence of a specific need. However, some of the required steps are already underway for other reasons (IdM replacement), or goals that will likely have broad support (no plaintext passwords, stronger encryption standards, consolidation of AD environment, establishing business processes and technology to facilitate identity assurance) regardless of whether or when we seek a formal certification.

(For a more general discussion of InCommon, see Section III, starting on page 27.)

VII. Next Steps

The preceding pages have argued that the University's current identity and access management system is insufficient for its current and future needs. The coming changes in the number and range of persons to be served, the complexity of relationships in universities with very high research activity, the compliance requirements within academic medical centers, and the revolution in the means to deliver solutions, are examples of the dimensions unanticipated by the current ecosystem that cannot be solved by changes in a single system. The entire complex of identity sources, identity and credential management, and applications

themselves needs to be substantially redesigned and re-implemented to shore up the foundation of all of the University's online resources and services.

As just described, the new, restructured IAM system envisioned in this report rests on five architectural cornerstones:

1. **A consolidated Identity Management System** – The identity management system needs to be consolidated at the center with delegated administrative functionality.

2. **Central Registry** – A central registry should be built to provide access to a more robust set of data (than is currently available via LDAP) about a broad spectrum of people with a relationship to the University (i.e., not just those with NetIDs). Each person's information should be tied to a unique identifier that is not an already existing University identity or identifier. Most of the data will be accessible virtually (rather than being replicated to a database).

3. **"Smarter," more Identity-aware Applications** – Authorization, the permission to access resources, needs to be handled by the surrounding business applications, not by the identity management system. Applications must become identity-aware pieces of an integrated portfolio, rather than heads-down, internally focused silos, and authorization should be flexible enough to open access to individual services as needed.

4. **Online Processes** – Identity and access management processes need to be done online utilizing web services that provide real-time and workflow functionality based on data for individuals.

5. **Northwestern NetID Supplements** – The Northwestern NetID will remain the core Northwestern electronic credential, but its role needs to be supplemented by external credentials and by other means of insuring identity trust and assurance.

Included in the preceding pages is a very large set of work. More than could be accomplished in one year even if all other work was halted. We will need to discuss and prioritize what comes first and what is delayed.

Projects to be Considered Initially

The matrix that follows this brief discussion shows two sets of work. (These projects are a small subset of the more comprehensive list of work included in Appendix C (page 62).

Work related to the Replacement of NUValidate

The first set of work consists of topics that are intertwined enough with NUValidate that they require a degree of envisioning before a replacement product is chosen. This set of work should be prioritized because of NUValidate's product end-of-life status. While the risk associated with its status is viewed as low to medium low (see page 6), the need to replace it is time insensitive.

The actual replacement of the system is expected to take one to two years. There are key discussions, envisioning, and planning to be done in addition to that time due to the many facets of the Identity Management System that are entwined with NUValidate. We cannot wait until everything is perfectly figured out before proceeding with choosing a replacement. However, we also cannot choose a replacement without having a sense of where we're going on some key issues.

The first three pieces of work in this set are relatively straightforward. The ability to do two of them (Wildcard consolidation and Online Directory restructuring) is, however, very much dependent on the ability of groups outside of NUIT to contribute to the effort. The last four pieces, bracketed by bold lines within the matrix, are less formed, and require broader discussions and input.

In some cases, the envisioning in this initial pass through these seven pieces of work may be short – e.g., if the degree of difficulty in moving to a new and improved model is large, the resources required would be difficult to obtain, and the impact on the replacement could be contained, then the envisioning could be limited to making the decision that no work will be done until after the NUValidate replacement is in place. For most of these topics, more depth will be required. (The matrix gives orders of magnitude on their size (both envisioning and implementation) and their relationship to the project.) Nevertheless, the estimate is that with the right mix of people – combining business knowledge with technological understanding – a six month window could provide the needed input for the NUValidate replacement product selection process to proceed.

Other IAM Work

Despite the small size of the NUIT Identity Services team, and their limited capacity for new undertakings, we do not think that all IAM work must stop while this envisioning takes place. The second set of projects are also connected to the Identity Services team, but they differ from the first set in that they are more amenable to being largely delegated to consultants/contractors with oversight by the Identity Services team. To the extent that this is possible, the projects related to the replacement of NUValidate do not take a higher priority than this second set of projects. However, we need to be diligent about moving forward with the NUValidate replacement, and not let it linger behind the scenes.

The second set of projects contain work that is either already underway, address core applications within the IAM experience at Northwestern, or are high visibility business areas that have key IAM needs. There are many other projects that are on the list of IAM work that are not included in either of these lists. Sometimes that is because they are second-order tasks. In other situations it is because the work required is only tangentially related to the NUIT pinch point, and prioritizing them would suppose a broader discussion within the business units or IT Government advisory committees. The projects listed in this second set are being recommended as the leading candidates for the additional bandwidth of the Identity Services team that might be available for IAM projects.

Envisioning the Prioritization of Initial IAM Work

	Outsource-able?	Topic	Involved Parties (in addition to NUIT)	The Business Value attached to changing the way this work is currently done	Impact on Selection Process if the decision is "Just do what you're doing now."	Must Do? (yes, no, maybe)	Envisioning Effort (s,m,l)	Impact on NUV Replacement Selection Process (s,m,l)	Impact on NUV Replacement work (s,m,l)
Tied to Replacing NUValidate	N	Email Provisioning	NUIT only	Makes IdM more flexible - easier and safer to modify.	Moderate, will need to make sure new system is flexible enough to allow us to translate the business logic from current IdM.	Y	S	M	M
	N	Online Directory	UR, HR, Registrar	Makes IdM more flexible - easier and safer to modify.	Minimal, most vendors can handle this level of back-end complexity and front-end UI just fine.	Y	S	S	S
	N	Wildcard/IdM Consolidation	Univ Svcs, FASIS, SES, downstream WildCARD users	Reduces need to maintain two parallel systems. Reduces chances for errors to surface. More consistent data across systems that rely on IdM and Wildcard.	Zero, if consolidation is not planned before the predicted end of life of the new IdM system.	N	M/L	M	L
	N	Manual NetIDs	FASIS, FSM, SCS, ...	Eliminates one of the main sources of duplicate NetIDs, and reduces complexity of overall system. Addresses (or at least shifts) many audit-related concerns over separation of duties and adequate operational contols in financial and other systems.	Moderate, need to ensure that new system has flexible way to delegate appropriate admin privileges and has a good UI for doing this.	Y	M/L	M	S / L
	N	Group Management	Schools	The shortcomings in being able to manage groups both ad hoc and "automatically" has become even more of an issue as more collaboration services have been offered centrally.	Moderate to Large - the current system has many shortcomings, both behind the scenes (what it can do) and in front (bad UI, clumsy & slow tools). Replacing IdM without at least marginal improvements here will seem like a step backwards to many people.	Y	M/L	L	L
	N	Central Registry	Schools, Enterprise apps	Key request from multiple groups: make more data (e.g., historical relationships, multiple roles, organizational attributes, group membership) available centrally.	Negligible. If we never plan to do this work, we don't need to prioritize features to support it when selecting a new system.	Y	M/L	M	L
	N	Data Privacy Considerations with LDAP vs. AD	ASAC, IMC, OGC?	Active Directory has fewer privacy options on attributes than LDAP does. Need to know how to balance functionality and privacy.	Minimal, most vendors can handle the type of AD & LDAP provisioning we do now, and anything we might choose to do in the future, with no problem.	Y	M/L	S	S/M
Selected Other Priorities	Y	Create SOA services	SES, FASIS, NUL, ...	Fundamental building block of new architecture.	NA				
	Y	SSO	SES, FASIS, schools, ...	this is a key building block for user experience improvements (fewer logins and ability to integrate an app into the NUPortal) and for deployment of MFA on an enterprise basis.	NA				
	Y	MFA/SSO Integration	FASIS,SES	Allows more granular application of Multi-Factor Authentication, and allows it to scale to an enterprise level.	NA				
	Y	Social/SAML IdP	ARD, NUL, TGS, IAC, ...	Allows for the use of social identities for more "peripheral" constituencies. Key functionality for the Library's Alma project and desired by multiple other places in the University.	NA				
	Y	Federation enhancement	IAC	Changes the setting up federation between systems to more of a routine operations process from an exception. Makes the infrastructure more robust.	NA				
	?	Pressing School-based IAM needs	Relevant schools	For instance, improving the state of IAM is a key priority for Northwestern Medicine.	NA				

A More Comprehensive Listing of Work

Appendix C: Envisioning an IAM Roadmap (page 62), includes a more comprehensive list of work that is either explicitly recommended, or implied in the pages of this report. It is divided into the three organizing concepts utilized in the preceding section: Integrating Identity Management, Integrating Identity and Access Management, Optimizing Levels of Assurance and Trust.

No attempt has been made to attach beginning or ending dates to these tasks at this point. Those will come out of the discussions that follow the release of this report.

Initial Recommendation for Governance

This initiative will have ties to both ASAC and the IAC. Much of the business-related discussions will happen within ASAC, but the IAC has all of the school IT leaders on the committee, and they will be the best body to advise on the technology decisions.

The initiative will be overseen by one person, who will be supported by NUIT personnel to assist with managing and keeping the work on track.

To begin, we are recommending a steering group for the initiative, similar to the group that is guiding the SOA Initiative, comprised of 6-10 representatives from schools, business units, and NUIT. It will need to have business perspectives and technological familiarity represented within its members.

Appendices

A. Glossary of Terms

Term	Definition
Access Management	Process (supported by underlying technology) by which a system responds to a request by a person for access to information or services. The decision to grant or deny access is based upon business rules and the known characteristics of that person.
AD (Active Directory)	Active Directory is a Microsoft, Inc. database service structure for storing and querying information key to making authentication and authorization decisions. (See also LDAP below.)
Authentication	A process component of access management which confirms, to an understood level of trustworthiness, that a person requesting services is a unique individual.
Authorization	A process component of access management which grants a person certain permissions within a system based upon the known characteristics of that person.
Credential	An item which is presented by a person as a confidential assertion that the corresponding identifier is in his or her possession. A password is a credential which accompanies a NetID to assert identity when requesting access to a system.
Credential Trustworthiness	A dimensionless measure of confidence that a credential is within the control of the original person to whom it was issued with the corresponding identity. Trust may be low for a password (which can be shared), higher for a physical object like a WildCARD (which might still be misplaced), and higher still for a fingerprint.
Domain	A logical container within a directory that allows for the management of a set of accounts (i.e., people) and devices (e.g., printers, computers) via a single directory service.)
FASIS	Faculty and Staff Information System (the Northwestern Human Resources system), formerly known as “HRIS”
IAM (Identity and Access Management)	An industry phrase describing software and business procedures to create unique credentials for each person to be served within a defined group, manage the lifecycle of those credentials, and enable authorization decisions based on identity characteristics.
Identity Assurance	A dimensionless measure of confidence that a given electronic identity was originally created for a real person and the correct person. A low assurance lacks confidence, while a high assurance results from multiple independent attestations of identity for the person at the time the identity is issued.
IdM (Identity Management)	A set of business processes for creating, sustaining, and retiring individual electronic identifiers for persons. Example identifiers at Northwestern include WildCARDs and NetIDs. Other possible identifiers could be external, such as Facebook or Gmail accounts.
LDAP	Lightweight Directory Access Protocol is an industry-defined database service structure for storing and querying information key to making authentication and authorization decisions.
SES	Student Enterprise System (the Northwestern Student Records system)
SNAP	Simplified Network Account Program (the original Northwestern IAM system)

Term	Definition
SOA	Service-oriented Architecture is a name given to a software architectural framework in which systems interact with each other “behind the scenes” using web services (see next item) as the primary means of cross-system integration.
Web Service	A standard, real-time messaging technique to request and return information between applications without human intervention.
Web SSO	Web Single Sign-On is an industry term for a consistent and convenient application experience where multiple systems honor a single authentication step through cached indicators of the types of credentials used.
Workflow	A logical process that moves a request through a series of steps to ultimately satisfy the request. Paper workflows involve forms passed hand-to-hand. Electronic workflows involve data being passed between workers, approvers, and systems through digital forms, email, or other means.

B. Quick Reference Guide to the IAM at Northwestern Report

There are eight main "applications" that work together to comprise the IAM "system at Northwestern:

1. **a core Identity Management (IdM) system** (NUValidate), which stores identities based on NetIDs that are in turn based on data fed primarily from authoritative identity sources such as the Faculty and Staff Information System (FASIS) and the Student Enterprise System (SES), allows people to manage those identities, and updates Northwestern's identity directories;
2. **identity directories** (e.g., LDAP, Active Directory, and Kerberos), which surrounding business applications use to authenticate users requesting access to their system;
3. **a physical identity system** (the WildCARD system), which provides proof of identity for access to buildings, events, etc.;
4. **a directory synchronization utility** (Radiant Logic), which keeps data in multiple active directory domains synchronized;
5. **a web Single Sign-on system** (SSO), which reduces the need to keep logging in with the same credentials for each Northwestern University application that is used;
6. **federation services** (e.g., Shibboleth), which allow people at trusted affiliate, partner, or peer institutions to use their home institution's credentials to gain access to Northwestern systems and services;
7. **a multi-factor authentication service**, which provides an extra layer of password protection using an application on a registered smart phone or answering a phone call to reduce the risk that personal information can be easily compromised should someone learn a NetID password;
8. **an "Identity Provider" bridge service** (currently being run by the Alumni and Development Enterprise Applications team for the OurNorthwestern system), which enables alumni to log in with either an active Northwestern identity or with one of their own external social accounts (Gmail, Yahoo, Microsoft).

See the section on "IAM in Action" in Appendix D (page 71) for a diagram and description of how these parts work together to provide IAM functionality when a person tries to log in to a Northwestern application. Appendix D also has an annotated diagram that shows how data flows within the IAM system (page 68).

If these pieces comprised a highly-functioning IAM system, they would be typified by the following nine characteristics:

1. Each person has a single electronic identity. There may be multiple credentials attached to that identity, but there is only one electronic identity.
2. The IdM infrastructure is integrated within itself, so that data about identities and personal attributes flows smoothly throughout the system.
3. Identities and access to resources are provisioned and de-provisioned rapidly in alignment with the need for their actual usage, with easily auditable trails.
4. Authorization is appropriately granular and based on robust identity information.
5. Surrounding business applications are integrated with the enterprise IdM system.
6. The level of rigor employed in identity proofing and authentication at the time of access is based on the risk and value of the transactions to be done.

7. Identities are protected and secure.

8. Each part of the IAM system is relatively easy to maintain and to replace.

9. Business applications and the IAM infrastructure are flexible and easily modified to take advantage of new IAM technologies as they emerge and become stable.

Northwestern's IAM system has grown organically over the past twenty years without benefit of an overarching architectural strategy. Work needs to be in three main areas, based around five architectural cornerstones:

1. Identity Management (IdM) needs to be restructured, reducing its complexity, better integrating its data flow, and making more identity and personal attribute information available.

IAM Architectural Cornerstone #1: The identity management system needs to be consolidated at the center with delegated administrative functionality.

IAM Architectural Cornerstone #2: A central registry should be built to provide access to a more robust set of data (than is currently available via LDAP) about a broad spectrum of people with a relationship to the University (i.e., not just those with NetIDs). Each person's information should be tied to a unique identifier that is not an already existing University identity or identifier. Most of the data will be accessible virtually (rather than being replicated to a database).

Six areas of consolidation are discussed as ways to improve data flow, User Experience, and resource efficiency:

1. Instead of system-specific credentials, use the NetID as the University authentication credential for system access when a University credential is called for
2. Reduce the use of Manual NetIDs
3. Merge the provisioning of WildCARDS in with the core IdM processes they now mirror
4. Consolidate AD domains, but provide distributed ability to create and manage groups
5. Centralize access to personal attributes that are now isolated in systems and local AD domains
6. Centralize access to identity credentials and identifiers that are now

Notable associated sets of work:

- Envision a new IdM model so that a replacement for NUValidate can be chosen, including:
    - reviews of current and desired functionality associated with manual NetIDs, group management, central registry, and data privacy in access directories
    - conceptualizing the relationship between the central registry and the NUValidate replacement
- Build web services to handle Identity Management
- Replace NUValidate

- Exploring the consolidation of Active Directory domains
- Explore the consolidation of the provisioning process for WildiCARD into the IdM system's

2. Identity Management and Access Management need to be better integrated.

IAM Architectural Cornerstone #3: Authorization, the permission to access resources, needs to be handled by the surrounding business applications, not by the identity management system. Applications must become identity-aware pieces of an integrated portfolio, rather than heads-down, internally focused silos, and authorization should be flexible enough to open access to individual services as needed.

IAM Architectural Cornerstone #4: Identity and access management processes need to be done online utilizing web services that provide real-time and workflow functionality based on data for individuals.

Notable associated sets of work:

- Utilization of web services to make access-related tasks occur in real-time
- Enterprise commitment to web Single Sign-on
- Move identity and access processes online and eliminate paper
- Promote the movement to online processes (e.g., make status attributes available centrally, outside of systems; investigate the usage of roles at the University already; investigate the connection between access permission requests and the provision of training)
- Conceptualize the personal attribute side of the central registry
- Conceptualize a new methodology for applications to make use of more robust data in order to make more informed and, where needed, more granular authorization decisions ("smarter, more identity-aware" applications)

3. The IAM system needs to optimize its ability to leverage Assurance and Trust levels attached to an identity and its credential.

IAM Architectural Cornerstone #5: The Northwestern NetID will remain the core Northwestern electronic credential, but its role needs to be supplemented by external credentials and by other means of insuring identity trust and assurance.

Notable associated sets of work:

- Identify areas where levels of Assurance and Trust need to be optimized
- Deploy Multi-factor Authentication
- Improve our capacity and ease of using Identity Federation
- Expand the usage of Social Identities where appropriate for constituencies less tightly connected to the University
- Associate Levels of Assurance and Trust with electronic identities, and have applications utilize them when making authorization decisions about access to resources and services
- Reduce the need to have a person be physically present in order to change their credentials with appropriate levels of Assurance and Trust

Authentication Overview

Area	Today	Proposed
Main Authentication Mechanism	– LDAP or AD	– LDAP or AD

Web Single Sign-On	– Limited Deployment	– University Standard
Federation	– Limited usage – Exception rather than standard operational process – Shibboleth only	– Standard operational process – Robust infrastructure – Other protocols, e.g., OAuth?
Federation via Social Identities	– OurNorthwestern only	– Multiple cases across the University for constituencies with more limited/removed relationships with the University
Role of NetID	– The Northwestern credential and primary electronic identity – Gateway to all Northwestern online resources for all constituencies (except for OurNorthwestern)	– The Northwestern credential. Gateway to Northwestern resources for core constituencies – Supplemented by credentials from other institutions and by social identities.
Single Northwestern Identity	– NetID comes closest and is widely adopted by applications – Fragmented multiple credentials and identifiers	– NetID becomes "just" a credential – Single identifier gets created, to which all credentials (e.g. NetID, WildCARD barcode, EMPLID, LinkedIn ID, Facebook ID) get tied
Attribute Data	– Replicated in LDAP – Some isolated in distributed Active Directories	– Available centrally – Mostly available via services or virtually
Assurance and Trust Levels	– Not utilized (e.g. no difference between Manual NetIDs and regular NetIDs) – NetIDs are either active or not	– Tied to each credential – Can be changed as a result of a change in status or a verification process (e.g. physically showing up and presenting proof of identity) – Applications should use in determining access to their resources

Authorization Overview

Area	Today	Proposed
Most common Application Relationship to IdM for Authorization	– Authentication = Authorization + Internal Security Table	– Applications should be "Identity aware"
Timing of Personal Status and Attribute data Updates	– Usually overnight	– Real-time
Available attribute data	– Relatively limited	– Wide-ranging (e.g. multiple roles, history, externalized role/permission variables, functional area specific)
Authorization Granularity	– All or nothing based on coarsely-defined roles stored within applications	– Basic lower-level roles defined and stored external to applications – Applications should be capable of refined granularity.

C. Summary Listing of the Sets of Work Included in the IAM Report

The following matrix enumerates the work that is explicitly called out, or implied, in the sections of this report. The work is organized into sections corresponding with the organizing framework used in the Path Forward section (page 32). While each piece of work is only listed once, each one has an envisioning and implementation phase that are not called out separately here because no attempt has yet been made to sequence this work. The Next Steps section of the report (page 51) highlights sets of work from this list that are recommended to be considered for initial prioritization.

Sets of Work Included in the IAM Report		
Category	**Task**	**Notes**
RESTRUCTURING IDENTITY MANAGEMENT		
Service Oriented Architecture	Adopt Web Services as the default method of obtaining identity and personal attribute information. Build core reusable web services to provide personal attribute information for different levels of security from the authoritative systems.	Already in process. Services to integrate IdM will be prioritized.
Develop New IdM Model in light of NUValidate's End-of-Life		Working Group(s) needed here.
Externalize Special Case Logic in NUValidate	As much code as possible must be removed from NUValidate before it is replaced with something else. Examples include: authorization logic for NUL and SPAC; group attribute calculations for Bulkmail system and Kellogg students; maintenance of Unix UID numbers for WCAS and Research Computing. Develop model for placing special authorization logic outside IdM system.	Tied to replacing NUValidate.
Online Directory Strategy	Determine how best to provide Online Directory "white pages" lookup services.	Tied to replacing NUValidate.
Rethink email account provisioning	Should the IdM system continue to provision the email/collaboration environment at the current highly granular level, or should this logic be moved closer to the email system itself.	Tied to replacing NUValidate.
Manual NetIDs and the Identity Lifecycle	Create a working group, under the direction of the ASAC to review the usage of Manual NetIDs. As part of this analysis, attention should be paid to how the usage of Manual NetIDs is related to administrative system functions that are required of individuals as they enter or leave Northwestern.	Tied to replacing NUValidate. Creation of a working group cited here. If possible, the first task of this group should be to determine whether the new IdM system will have to support widespread creatin of manually-asserted netids by deparmental/school IT staff - this will influence the IdM replacement product selection and design. To get a sense of this, the working group would need to look at at least two items: - How often are manual NetIDs used, and for whom? - What are the possibilities for using FASIS' Person of Interest functionality and/or toaccept external credentials – especially from social networks or major service providers – to reduce these needs?
Manual NetIDs	Develop a plan to eliminate the manual NetID process based on the results of the Manual NetID working group.	
Need for group management tools	Evaluate the need for a new group management tool, e.g. Grouper, that allows delegated management of group memberships to support local business needs.	Tied to replacing NUValidate.
Centralized Registry - Phase I	Develop a proposed architecture for a central Registry: Phase I is the Identity Repository (to hold credentials, trust and assurance level attributes, etc).	Tied to replacing NUValidate. Whether this would the job of the NUValidate replacement, or built external to it, will be decided in this envisioning phase. Part of this investigation should be looking at whether the identity de-duping process should be centralized and staffed here rather than being entirely done at the individual system level. A high-level description of the types of services that the Registry should offer, and what types of data it should contain should be a key outcome of this group.

Sets of Work Included in the IAM Report		
Category	**Task**	**Notes**
Evaluate directory infrastructure and strategy	Evaluate the use of AD for LDAP services in place of a separate LDAP infrastructure. Also evaluate other potential replacements (e.g. Oracle, OpenDJ) for current SUN-based LDAP system. The result of this study should be used during the implementation of the IDM replacement to guide provisioning requirements.	Tied to replacing NUValidate. Technical limitations of AD would require revising our policies to allow for making many data items more widely available than they are now. AD does not support nearly as much granularity in controls around access to directory data as our current LDAP environment. Implementing a change to LDAP (either replacing it with a different LDAP product or removing it in favor of a sole reliance on AD) will involve a great deal of work by dozens of application owners both within and outside of NUIT. The technical challenges are probably small compared to the effort required to contact all customers and support/coordinate the change process.
Wildcard Integration	Design a new Wildcard provisioning process that would be integrated within the University's IAM portfolio as simply another credential managed through the central IdM system. Use Web Services between IDM and the Wildcard computer system to support real-time identity assignment for new cardholders, and propagation of barcodes and other card-based attributes into the central authorization services.	Tied to replacing NUValidate. A key early decision to be made is whether this project, which is likely to add significantly to the scope, complexity and timeline for the IdM replacement project, should be done right away or delayed. Are the benefits of Wildcard/IdM integration large enough to justify this increase in scope? Can the most critical needs be met some other way?
Duplicate Identity Avoidance	As part of conceptualizing the creation of the Identity Respository, a working group should look at the implications of this new architecture for controlling the possibilities that duplicate identities can be created.	Creation of a working group cited here. Given that more identity credentials will be tracked in one place for a larger population, the process for avoiding mistakenly issued duplicate identities should be examined to see if it should restructured due to new opportunities and/or the need to avoid larger problems, e.g. should the identity de-duping process be centralized and staffed here rather than being done entirely decentralized and relatively uncoordinated at the individual system level.
Elevated Administrative Privileges	Develop plan for bringing FASIS and SES IdM procedures for administrators with elevated privileges into alignment with NUFinancials. - Eliminate separate ID/PWs. - Reflect the granting/removal of access via identity attribute flags in the IdM system. - Develop a consolidated online request form, with an auditable workflow attached to it, for requesting and granting permissions.	This is a prerequisite to integrating FASIS and SES into Single Sign-on. Over time, the results of these requests could be used to help define roles. This system could be subscribed to status-change events and could notify security administrators that an individual's security should be examined.
Tie credentials to assurance and trust levels	Define Trust and Assurance Levels and processes for using them to authorize access.	Each credential held in the Identity Repository should be associated with trust and assurance levels. The initial implementation can define the attribute and set it to defined values (e.g. assurance based on Registrar, HR, and manual-assertion confidence; trust based on in-person, mail, self-assertion).
Active Directory Restructuring	Review AD usage across the campus (schemas, authentication, etc.) and evaluate the possibilities for domain consolidation.	Important to facilitate the usage of shared services located centrally, reduce complexity of IdM process, relieve support loads in the long run and reduce duplicative infrastructure in the distributed IT units.
Replace NUValidate	Select Vendor and sign agreement	
Replace NUValidate	Replace NUValidate as part of the new model	This will likely be a two-year implementation, AFTER a vendor is selected and an agreement is signed.

Sets of Work Included in the IAM Report		
Category	**Task**	**Notes**
INTEGRATING IDENTITY AND ACCESS MANAGEMENT		
Service Oriented Architecture	Adopt Web Services as the default method of obtaining identity and personal attribute information. Identify core reusable web services to provide personal attribute information for different levels of security from the authoritative systems.	Web Services are a fundamental building block of each side of the IAM relationship. They will enable a tighter integration within IdM and between the IdM system and the applications needing to make access decisions. These sets of services overlap, and the IdM integrating services will probably come first. This entry is for the services to integrate applications with IdM that will remain after this initial work is done.
Web Single Sign-on (SSO)	Commit to having all enterprise applications using web Single Sign-on and develop a path for moving enterprise systems behind it.	SSO is the optimal place to integrate DUO, the Multi-factor solution currently being piloted by FASIS, at the enterprise level. Growing this functionality at the enterprise level addresses not only improved authentication security, but also many user experience requests, gives a unified "choke point" as authorization decisions begin to diversify, and is a precursor to building out NUPortal. (As each enterprise system adopts SSO, access portlets should be created on the NU Portal.) As noted earlier, part of this effort has to be a restructuring of IdM procedures for users with elevated administrative privileges in SES and FASIS.
Central Registry - Phase II	Develop an architecture for extending the centralized Registry. Phase II provides extended access to personal attributes.	Creation of a working group cited here.
Smarter Applications	Re-architect applications so they make their own authorization decisions and use web services to get the data they need. - In the interim, use broadcast web service events (e.g. employee separations) to update applications' internal security tables one-record-at-a-time on a real-time basis - Ultimately, applications should use the centralized registry to make their own more granular authorization decisions in real-time based on query responses spanning a broad range of available attributes.	
Tie credentials to assurance and trust levels	As part of making Applications "smarter", design how they should use the Trust and Assurance Levels associated with credentials.	Applications should utilize Trust and Assurance levels associated with each credential when making authorization decisions.
Process Improvement – application roles	Create a working group, under the direction of the ASAC Information Management Subcommittee, to investigate how application owners have used local security roles to simplify provisioning of user profiles within applications. Document current practices, lessons learned, and the definitions of these roles. Where possible, insert these role definitions into manual request workflows to explain the options available to requesters and streamline fulfillment processes.	Creation of a working group cited here. Some of this work has already started vis a vis NUFinancials. Other areas may already have work started as well (and lessons learned about which approaches are productive and which are unproductive. The roles that get defined in this work should be held external to the system so they can used, when needed, in other instances.
Process Improvement – Permissions Management	Create a working group (it could be the same one cited for the study of role, or a separate one) under the direction of the ASAC, to investigate how access permission request and application training provisioning are currently handled for NUFinancials, Cognos, SES, and FASIS, and to recommend improvement paths for these processes.	Creation of a working group cited here.

Sets of Work Included in the IAM Report		
Category	**Task**	**Notes**
OPTIMIZING LEVELS OF ASSURANCE AND TRUST		
Multi-factor Authentication (MFA)	Building on the current DUO pilot implementation for FASIS, design a more enterprise production level architecture utilizing web Single Sign-On, which allows the implementation to scale across multiple applications and allows MFA to be applied granularly within applications.	
Federation	Develop a roadmap for improving Northwestern's ability to utilize federation (Shibboleth etc.) more widespread as a routine operational process.	Included here would be a more robust infrastructure, changes in documentation on how to ask for and use this technology, improved business processes for setting it up with applications, etc.
Federation	Develop a roadmap for expanding the OurNorthwestern Identity Provider Gateway solution into an enterprise solution that can be used for applications across the University.	Discussions with Uprising (the people who designed and built the OurNorthwestern Identity Gateway) have occurred. The proposed project would generalize the ADEA solution and make it available for appropriate situations in other parts of the University.
Federation	Work closely with the Feinberg School of Medicine to develop a roadmap for integrating Northwestern Medicine credentials into Northwestern University's IAM system via federation.	This is a non-trivial task and will take much effort and attention from both the University IT team and the Northwestern Medicine teams.
Increased Security Controls	Convene a working group to survey areas in need of added security layers to increase levels of trust and/or assurance, e.g. multi-factor authentication, additional controls around changes in a person's privileges and attributes. Working group can assemble use cases and a set of solution requirements, and can use the results of the current DUO pilot as part of its material.	Creation of a working group cited here.
Credential Management	Find ways to eliminate the requirement that a person be physically present to change or re-set a password.	This work might be tied to being able to change levels of Trust and Assurance associated with credentials.
Enable the assurance and trust levels tied to credentials to be changeable.	As part of optimizing the usage of the Trust and Assurance levels tied to credentials, develop workflows and processes for changing these levels when appropriate.	Projects can include workflow and business processes to allow a person to raise the assurance level through various identity proofs.

Areas cited in the list of work where working groups could be helpful

1. Oversight to the IAM Initiative
2. Developing a new IAM model (might be the same as the Oversight Working Group)
    a. Selecting IdM vendor
    b. Implementing a new IAM model
3. Manual NetIDs
    a. Under direction of ASAC
    b. Review usage of Manual NetIDs
        i. 1. Create an inventory of necessary access to resources during the on-boarding and off-boarding phases, and describe how those functions rely upon issuance of NetIDs.
        ii. 2. Determine how often manual NetIDs are used, and for whom?
        iii. 3. Investigate the possibilities for using FASIS' Person of Interest functionality and/or to accept external credentials – especially from social networks or major service providers – to reduce these problems?
4. Duplicate Identity Avoidance
5. Integration of a functional area into NUPortal
6. Process Improvement: Application Roles
    a. Under ASAC IMC
    b. Goals
        i. How have app owners used local security roles to simplify provisioning of user profiles?
        ii. Document current practices, lessons learned, and existing role definitions.
        iii. Where possible insert these role definitions into manual request workflows to explain the options available and streamline fulfillment processes.
7. Process Improvement: Permissions Management
    a. Same as #5?
        i. How are access permission requests and application training provisioning handled for NUFinancials, Cognos, SES, and FASIS?
8. Optimizing Trust
    a. Survey areas in need of added security layers, e.g. MFA, additional controls around changes in a person's privileges and attributes.
    b. Assemble Use Cases and a set of solution requirements
    c. Can use results of the current DUO pilot as part of its material.

D. The Northwestern University IAM Architecture

The general IAM architecture

A comprehensive IAM environment for any organization is based on three items: a personal identifier for each person, one or more credentials associated to that identifier, and a record of relevant personal characteristics for use in authorization decisions.

- The personal identifier is created for each unique person based upon evidence that the person exists and is within the community served.
- Credentials are created and delivered on demand for the person by a managed, accountable process to preserve the integrity (trustworthiness) of the credentials.
- The relevant characteristics of the person are available so that applications can make authorizing service decisions in real-time.

A traditional IAM infrastructure consists of software and services generally outside of the business systems themselves.

Creation of unique identifiers requires software that accepts attestations of a person's existence and status from other, authoritative, records systems. There may be more than one such system, in which case the software must anticipate possible multiple attestations for a single person. This software is called an "identity management system."

The identity management system will have special, secure functions for creating and managing credentials for each person. These functions will be used by trusted staff to create credentials when needed and convey them to the person in a secure manner. The same function will maintain a credential validation service that applications will invoke to test if the identifier-credential pair presented for authentication is correct.

The identity management system will also have functions to gather and organize relevant characteristics of the person – potentially from multiple attesting sources – to make available for real-time authorization decisions. Generally, these characteristics are assembled into directory services (e.g. LDAP, AD) which are queried by applications.

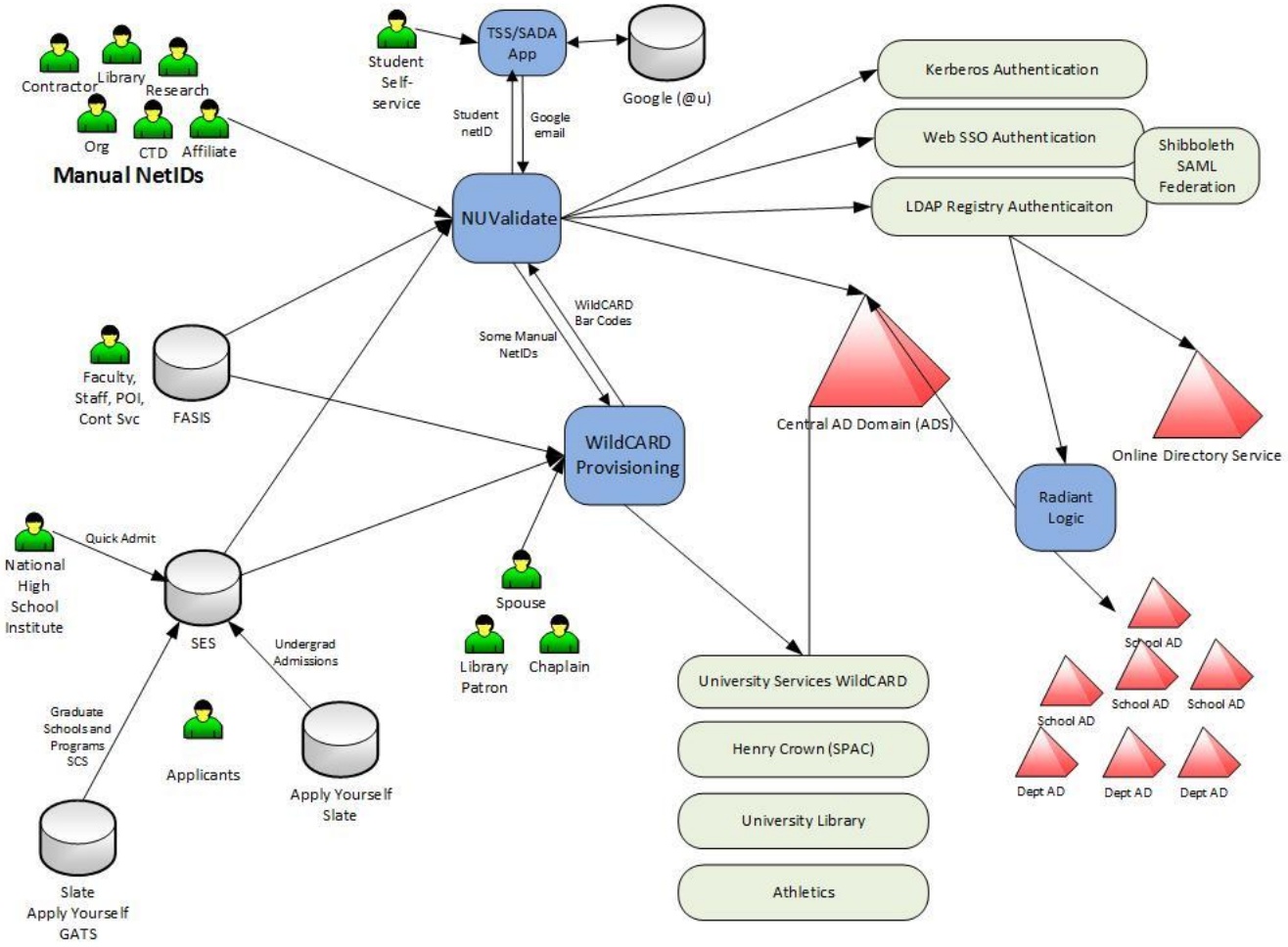
At Northwestern, these three functions rely upon several software systems and application systems. This "ecosystem" of systems must coordinate their overall and detailed approaches to avoid inefficiencies and confusion.

- Creation of unique identifiers involves an identity module within NUValidate reconciling attestations from FASIS, SES, and certain other smaller sources.
- For security purposes, management of credentials is within NUValidate.
- NUValidate gathers the relevant personal characteristics provided by FASIS and SES for a person and populates standard directory services (LDAP, AD) as means to securely expose that data. From that point, applications must query those directory services to use the characteristics in authorization decisions.

The future ecosystem may be different from today's, and this may require changes in the technical approaches. For instance, the definition of the community served may change to where FASIS and SES would contribute only a portion of the attestations, and similarly, the use of traditional directory services to hold and provide characteristics may not be suitable to future applications – especially cloud-based applications. This

may indicate that new services will be needed and that attesting systems could be directly queried instead of aggregating information centrally. It is also clear that self-attested credentials, or credentials from external institutions will have growing importance in our portfolio of identity management services.

Data Flow within the IAM Infrastructure



Data Flow within the Northwestern University Identity and Access Management System

Creating Identities in the IAM systems

1. Employee identity:
    a. Profile records are added to FASIS for new University employees (faculty, staff and student workers) via the normal University hiring process, and for "persons outside the institution" (e.g. research collaborators required to complete an NU conflict of interest disclosure) via a process performed by the Office of Sponsored Research and Human Resources.
    b. Data from these profiles flows nightly to NUValidate and creates new entries, including name and directory information. This also creates a NetID for the new record.
2. Student identity:
    a. Profile information for undergraduate applicants flows into the Student Enterprise System (SES) admissions module from Slate. When a student matriculates, their profile information then flows into the main SES module for students.

b. Profile information for prospective graduate students follows the same path within SES, but comes from a variety of admissions applications supported by the schools.

c. Information for participants in some special programs such as the National High School Institute go right into the main SES module via the Quick Admit application, bypassing the SES admissions module.

d. Basic student profile data for admitted applicants flows from the Student Enterprise System to NUValidate on a nightly basis, creating new entries which include name and directory information. This process also creates a NetID for the new record.

3. Manually asserted NetIDs: Some organizations have the ability to "manually assert" identities in NUValidate in order to create a NetID. This information creates a record for the individual in the NUValidate system, including a NetID. Some of these

Authentication Systems

1. The NetIDs and passwords originating in the NUValidate system are replicated to the following authentication systems: LDAP, Active Directory and Kerberos. (NUValidate is the authoritative source for NetIDs, but it is never accessed for authentication decisions, all of which are done via LDAP, Active Directory, and Kerberos.)
2. LDAP
   a. In addition to providing authentication, the LDAP Registry can provide additional information about an authenticated individual on request. Other authentication systems such as Web SSO ("Online Passport") and Shibboleth/federation rely on LDAP for actual authentication step, then provide additional layers of service (e.g., SSO, SAML federation) on top of that.
   b. The University's Online Directory is also fed from LDAP.
3. Microsoft Active Directory
   a. Active Directory houses a copy of some of the data stored in the LDAP Registry. Most of the data needed by Active Directory flows from NUValidate to the LDAP Registry. An application called Radiant Logic pulls information from the LDAP Registry and populates Active Directory with it in near real time (a few minutes' delay at most, under normal circumstances). A small percentage of the data needed by Active Directory flows directly from NUValidate.
   b. Subsets of the LDAP Registry are also synchronized with locally managed Active Directory domains through Radiant Logic, also in near real time.

WildCARD Provisioning

1. At the same time profile information is flowing from FASIS and SES to NUValidate, the data also flows to the WildCARD provisioning system managed by the Identity Services group in NUIT. This process essentially mirrors the flow to NUValidate (though it is complicated by legacy code that transforms the data to a data format for mainframe computers that is leftover from the days when this functionality was housed on the University's mainframe computer). In this application, a barcode number is generated and associated with the profile, and returned to NUValidate. (The data transformation referenced here could be eliminated, but it would be time-consuming to do so and it has never arisen as a major priority.)

   The data from the WildCARD provisioning system (including barcode) subsequently flows to a separate

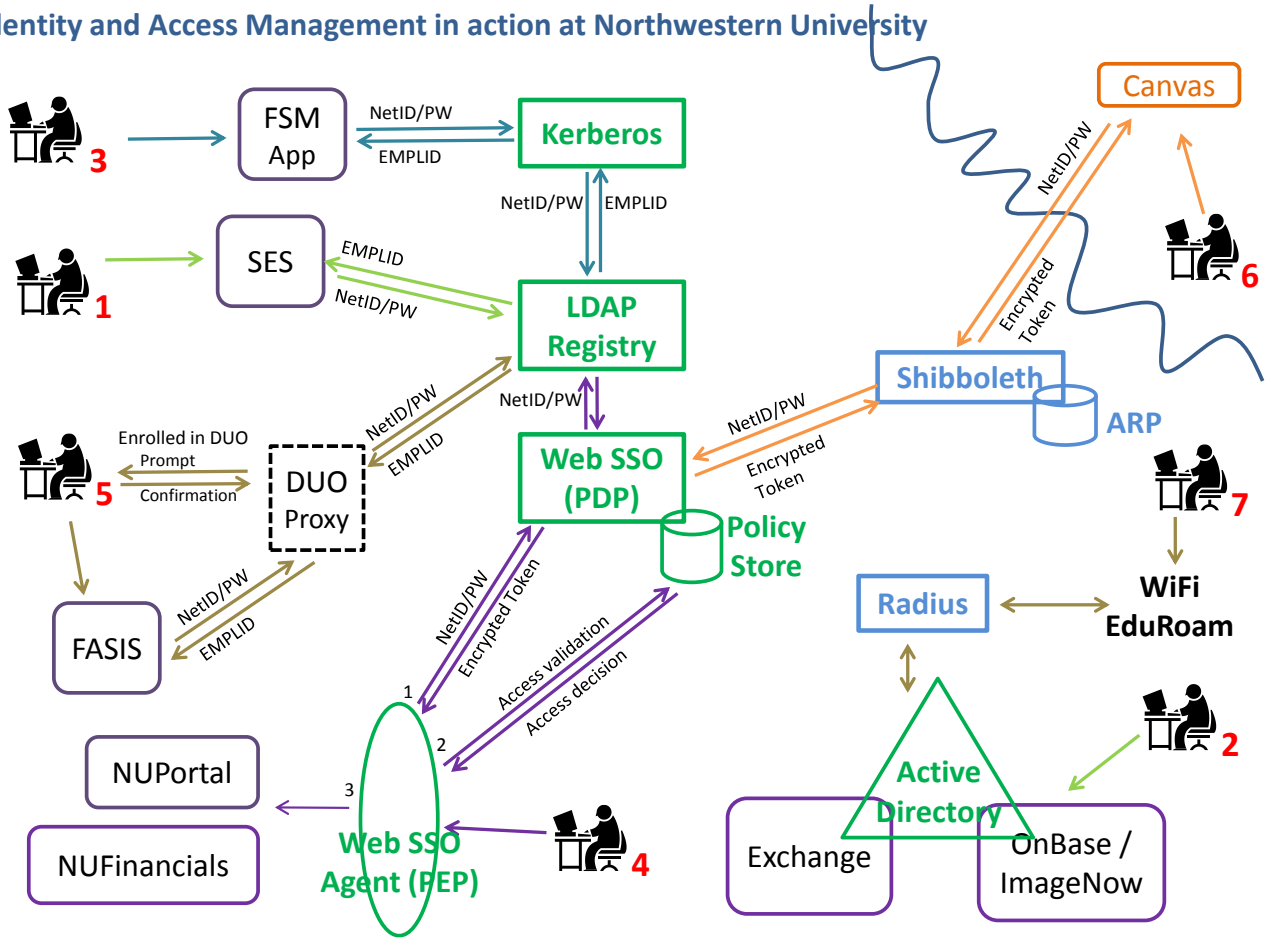
WildCARD application managed by University Services that permits the creation of a physical WildCARD. (These two "WildCARD" systems inevitably lead to confusion when talking about identity at Northwestern. Because Art Monge has managed the creation of WildCARDs for many years, this system is frequently dubbed "Art Monge's WildCARD system" for clarity).

2. In addition to Art Monge's WildCARD system, a special set of enterprise applications also receive data from the NUIT WildCARD provisioning system, but with one significant difference. Before the WildCARD data is sent to these applications (SPAC, University Library, Athletics), business logic is applied to it in order to make access decisions easier for the consuming application. For example, SPAC uses the WildCARD barcode to make decisions about whether someone entering their facility has access to the building. That decision is performed by the WildCARD provisioning system by applying a sequence of rules to the individual's role and status at the University. The output of those rules is a yes/no decision which is attached to the profile and barcode number and sent to SPAC, where it is hosted in a database used to admit patrons. When the user swipes their WildCARD, the barcode on that WildCARD is checked against the barcode number and "yes/no" decision data stored in the SPAC database.
3. There are some individuals whose only identity at NU is recorded on a case-by-case basis in the Art Monge's WildCARD system. These are primarily individuals with a loose affiliation with the University (e.g. spouses, summer camp participants, visiting users of some scientific equipment), but who are approved for a limited subset of services (e.g. NU shuttle, library access, WildCARD discounts). There are some cases where individuals are given a NetID via the manual asserted NetID process and also entered separately into the WildCARD system by the WildCARD production office, which creates duplicate data that is difficult to disambiguate.

Google (@u.northwestern.edu) Email Addresses

1) TSS/SADA: SADA is a vendor that provides an integration application to enable student Google email accounts and populate the resulting email address in NUValidate. Once a student NetID is activated, a student can create his/her @u.northwestern.edu Google account. The student uses the SADA application via self-service, providing his/her preferred email address, a list of nicknames, etc., and then SADA provisions the @u account, and sends the new email address back to NUValidate as a directory element.

IAM in Action – How the different parts of the system work when someone tries to login



When a user logs into a Northwestern application using their NetID and password, different processes and systems are invoked behind the scenes depending on the application the user is trying to access. There are some functional differences between these solutions that are apparent to the end user (Web SSO requires the user to authenticate via NU Online Passport, and then allows him/her to access more than one system without re-entering their credentials) but, for the most part, the noticeable differences are minor. Most users are probably unaware of the variety of authentication tools they are using.

The following paragraphs describe the roles of the pieces of the Identity Management process shown above in green, which are active in the login process. The numbers below correspond to the numbered scenarios shown above:

1) **Lightweight Directory Access Protocol (LDAP)**: This is currently the primary piece of the authentication process at the University. The example above shows what happens when a person logs into FASIS.

   When the person clicks on a link to SES, they are presented with a SES screen requesting their NetID and password. They enter their credentials, and those credentials are passed to the LDAP Registry. If the credentials are valid, then the Registry looks up the SES EMPLID in the directory, and passes it back to SES. The SES application then uses its internal permissions tables to provide access to whatever functions and data have been assigned to this EMPLID.

2) **Microsoft Active Directory (AD)**: Microsoft-centric applications do not use LDAP for their authentication process. Instead, they use Microsoft's directory product, which provides the same functionality as LDAP. The Exchange email and calendar system, OnBase, ImageNow, and a host of

school and department-based applications all utilize AD for authentication.

AD houses NetIDs and passwords, and a set of personal attributes just as the LDAP registry does. When a person attempts to login to Exchange, they are directed to an AD validation screen that prompts for a NetID and password. These credentials are compared to the NetID and password pair housed in AD. If they match, then the application allows the user access to whatever functions and data have been assigned to this NetID within the application.

3) **Kerberos**: Kerberos is an open-source authentication protocol developed at MIT. The protocol itself is still widely used, but is most commonly used as an underlying component of Active Directory authentication. Pure Kerberos is declining, maintained at NU only to support one or two legacy applications that still rely on it. The user enters credentials which are passed through the network for validation.

4) **Web Single Sign-on (SSO) "NU Online Passport"**: The NU Portal and NUFinancials are two applications that utilize Web SSO for authentication. When a person clicks on a link to one of these applications, their computer sends an inquiry to the web SSO Agent Policy Enforcement Point (PEP), which checks to see whether the person already has an active SSO "token". This token is a piece of information that essentially says to the Agent, "the person attempting to access this application with this browser has presented the correct password for a NetID." The token expires after a fixed period of time.

   if the person does not have an active token, the SSO process, as numbered on the diagram, proceeds through the following steps:

   i. If there is not an active token associated with this browser session, the computer is redirected to the Web SSO server, which displays the NU Online Passport page in the browser, asking for a NetID and password. The SSO server does not contain data against which to authenticate the credentials; it simply gets the credentials and passes them to the LDAP Registry to check their validity. If the credentials are valid, then an SSO token is passed back to the person's computer which will satisfy the requirements of the Web SSO Agent.

   ii. Now that the Agent is convinced that the credentials are valid, it performs a second check. It queries the Web SSO policy decision point (PDP) service to determine whether or not the user meets the access policies defined in the Policy Store. These are rules which govern groups who can access a resource. If the user satisfies the access policies, a positive message is sent back to the Agent, which passes credentials to the application.

   iii. The application then allows the user access to whatever functions and data have been assigned to this NetID in its internal security tables. If the same browser is used to navigate to another Web SSO-enabled application before the time limit on the token has passed, the token is considered valid and the Agent will make a policy call to the Web SSO PDP for the additional application.

5) **DUO (Multi-factor Authentication)**: An extended pilot deployment of The Duo MFA software also offers more advanced features, such as requiring MFA only once per day (or week or month) rather than every login, and a better user interface. These features, however, can only be leveraged if the application is modified to interface with the Duo MFA system. Alternatively, NU could invest in integrating MFA into the Web SSO system, which would bring these same features to applications using SSO without modifying each application individually.

6) **Shibboleth**: Shibboleth is used most frequently for applications that are hosted outside of Northwestern but accessed using Northwestern credentials. These applications are not entrusted with the NetID and password data at any point. Instead, when the user attempts to login to the application, they are redirected by Shibboleth to Northwestern's Web SSO PDP for validation. The PDP passes the credentials to the LDAP Registry to check their validity. If the credentials are valid, then a Shibboleth

token (SAML Assertion) is passed back to the application. This token is a time-limited, encrypted piece of information that essentially says to any SAML-enabled application, "the person attempting to login with this NetID has presented the correct password for this NetID." The application then allows the user access to whatever functions and data have been assigned to this NetID. The other component to Shibboleth is an attribute release policy, which tells Shibboleth which pieces of additional information (name, email address, etc.) it is allowed to retrieve from Northwestern's LDAP Registry and pass on to the application.

Shibboleth can also be used to provide access to local NU resources by external users using their own institution's credentials. Only one or two instances of this have been deployed to date.

7) **RADIUS**: RADIUS is an authentication service that uses Active Directory behind the scenes for NetID/password authentication. The Northwestern Wi-Fi network and the traditional (non-SSL) VPN use RADIUS to authenticate access.

   The Radius server also supports a federated authentication service, EduRoam. When a Northwestern employee attempts to connect to the wireless network at an institution that is a member of EduRoam, the Radius server at that institution redirects the authentication to Northwestern's Active Directory authentication tool. Requests to authenticate and use Northwestern's Wi-Fi network using EduRoam are similarly redirected to the authentication tools of the person's home institution.

E. Overviews of the On-boarding and Off-boarding Processes

The two primary process of identity lifecycle management are the on-boarding and off-boarding processes, which are most often associated with a person newly entering the Northwestern community (as a student, faculty, or staff member), or leaving the community (students usually become an alum, and faculty and staff usually get a job at a different place of employment).

Complicating factors in these processes occur when one person falls into two categories – e.g. a staff member and a student, a faculty and an alum – or has a relationship with more than two schools at the University – a student in a joint degree program, or a faculty member with joint appointments. These situations can pose challenging issues with gaining proper access to online resources. Another complicated situation occurs when an employee at the University switches jobs, in essence a simultaneous on-boarding and off-boarding that requires proper handling of turning permissions on and off even though the NetID remains active.

The following sections provide brief overviews of the IAM issues that come to the fore in these two processes.

On-boarding

Bringing people into the Northwestern community involves three phrases:

i. establishing mutual interest in a relationship
ii. making a commitment to the relationship
iii. enabling the person to be a welcomed and productive member of the community in that relationship

In prior times, much of the first two phases were done via paper, a Northwestern identity was only involved at the end of the second phase, and providing access to online services only became a concern once the person was on-campus. In today's world, particularly in the world of student on-boarding, much of the relationship building is done online, enabling access to varying sets of online resources as the relationship builds is increasingly common, and a Northwestern identity is only one of multiple identities employed in the process.

While all constituencies share these three phases in their on-boarding processes, there are significant differences in the student on-boarding from the faculty and staff on-boarding, so it will be enumerated separately.

Student On-boarding

Establishing mutual interest

In the world of Identity Management, a prospect is vetted during this initial phase as appropriate for the desired relationship through attestations from outside sources. The person's very existence as an entity is somewhat in question from the beginning, and such attestations serve to support personal self-descriptions. To proceed to the second phase, the University must be sufficiently convinced of existence and qualifications for the relationship to offer a commitment on its end.

Establishing mutual interest with a prospective student has two distinct phases to it: the Inquiry phase, and the Application phase. Obviously, many more people are interested in getting information about Northwestern (or a school) than actually ending up applying, so this part of the process is commonly handled in a separate system outside of the admissions system. While there is interest in knowing precisely with whom the institution is communicating, and in avoiding duplications of identity, the risk and downside of making a mistake here is much lower. Inquiries, and follow-up solicitations, are usually handled online these days, utilizing an email address provided by the prospective student.

Once a prospect decides to apply, the relationship moves to a more serious level. The person's information is moved into an admissions system, more information is submitted – often through authoritative sources (transcripts, test scores, visa information) – providing more levels of assurance for the identity that is the email address being used for accessing the application system and receiving communications about the application process.

Despite this increasing level of assurance, an institutional identity (a network account and/or an email address) is often seen as a way of increasing their identification with the institution, and of building the relationship with each prospect. In some cases, the network account is also used as a means of gaining access to special online content or resources, and the email address is used as an official vehicle for communications.

Over the years, the issuance of these identities has moved progressively earlier in the relationship-building phase as competition has increased for students and as resources have moved online. This is a double-edged sword, however, for a number of reasons:

- Prospects often do not want yet another email address that they have to check periodically, particularly from a school to whom they have not yet expressed a commitment.
- As more resources become available to students as they progress through the relationship building phase, having to remember a University identity (a network account) can be just another barrier to a relationship rather than an enabler of that relationship.

Making a mutual commitment / Enabling members of the community

As soon as electronic access to relevant materials must be granted reliably and solely to the person in question, IAM becomes much more important. While providing online access to varying pieces of online content for prospects at different stages of the process – inquirer, applicant, admitted prospected, admitted and accepted process – presents IAM requirements around identities and the ability to provision access, the implications of providing access vary along with the content being accessed.

A good example of this is financial aid packages for students. To decide about accepting admission to a program, a prospect must understand his/her financial aid package. If the details are online, then secure access to that information must be opened. This means that the person's identity must be defined within the responsible system and trusted credentials must be associated to that identity and be in the hands of the person him/herself. Another example of this occurred recently, when an online form was created for incoming students to submit I9 information instead of doing it via paper. Shortly after the form was announced, it was discovered that not all the students who needed to use it had been given their NetIDs, which were required for access to the form.

There are key takeaways on both sides of the IAM relationship here: as soon as access to online resources is needed, all of the identity management concerns about uniqueness, ease-of-use, assurance, and trust come into play on the identity side, and being able to accommodate varying levels of access to different resources becomes an issue on the access management side. Some of these resources are available only after a student matriculates, but there are others that require access before matriculation. Some schools want to give out NetIDs early in the process, other schools want to delay it because it prompts applicants to attempt to access materials not intended for them until after matriculation - triggering help desk calls and bad feelings.

The line between the commitment and enabling phases used to be much clearer than it is today. A commitment would be made on both sides of the relationship (admit the prospective, accept the offer and send in the deposit), the student would get moved into the student records side of SES, and then the

correlated sets of permissions that student needs or is entitled to, could begin. With many different schools, and even more degree and non-degree programs, at the University, managing these access permissions centrally via control over the creation and delivery of a NetID becomes exceedingly complicated.

In many situations, the extent to which the surrounding systems that provide online services or resources are integrated with the identity management system and the authoritative system of record for students (SES), this access can flow smoothly. When the information is not available, or is only available on the basis of data feeds with some degree of time lag built into them, the empowerment process (e.g. student services, WildCARD availability, Library privileges) can be diluted. Sometimes, these "lags" are due to the difficulty of matching up business needs rather than a lack of system integration. For instance, University Police might want to include incoming students in the emergency notification system as soon as they are "on campus", but nothing in SES or any other system connected to IdM tracks that. Formal matriculation in SES happens a couple of weeks before they are on campus, while the start of the term (another possible trigger) is too late since most students are on campus at least a few days before the term actually starts.

In short, the IAM scenario is exceedingly complicated. Some technological changes are available that can be relatively easily integrated into the IAM process to improve it: e.g., integrating applications – the IdM system, authoritative sources of personal data, and surrounding business applications -- via web services is fundamental. Others will require a much greater change in the functionality within the applications themselves – e.g. the ability to use something other than basic LDAP calls to get information on multiple appointments at the University (see page 20), and still others will require further thinking about how to link business processes with one another.

Notes on special cases:

Applicants who are already employed by the University: Degree applicants who are already employed by the University can create multiple issues. If their data is not fully entered in the FASIS system, or fails to match with the information they submit to a school or program, the search/match routine will fail to identify them, and they will get two NetIDs. As soon as they become an applicant – e.g., a staff member applying to a graduate degree program – some systems will be challenged as to which of these roles to base this person's access permissions on.

Non-degree students: Because students in these programs are not part of the normal pre-matriculation process for students, their identities are managed in systems outside of the core enterprise systems for the University, and the functional sophistication of these systems – e.g. their ability to retain identities from course to course – will vary.

Faculty and Staff On-boarding

The on-boarding process for faculty and staff goes through the same phases, with some similarities but also with some noticeable differences. Faculty and staff apply for a particular job, not a space in a "class" of varying sizes, so the volume of applicants is usually qualitatively smaller. During the hiring process, a user-supplied email account is again used for communications, and at the end of the process, multiple sets of documents are submitted and identity checking is done to ascertain the veracity of the person's identity and qualifications for the job.

In the case of faculty and staff hiring, there is a much clearer line between the commitment and empowering phases, though this transition is not without its challenges. Both faculty and staff may need access to online resources prior to actually starting their job, particularly with very senior staff and with faculty (e.g., access to research grants and the course management system). FASIS has the capability of, and processes set up for,

getting a NetID for a person 90-days in advance of their official hire date, but this capability, and how to initiate it, is not universally known.

Empowering new faculty and staff (via the granting of appropriate permissions, signing up for required training, getting that training, etc.) remains a process that has built-in time lags due to slow transfers of paperwork, a reliance on over-night batch data feeds, intermittent scheduling of training, lack of documentation on what is needed and how to get it, and many paper-based permissions processes that are only triggered upon request. It can be weeks before a person has everything they need to do their job. Moving processes online to reduce time lags and make them more efficient and trackable, and connecting systems and processes via real-time web services, will greatly improve the on-boarding process. Before that can be done, these processes, and the access permissions implied in them, to be documented, which was a theme that came out in multiple focus groups.

Notes on special cases:

New jobs for existing employees: When a current employee gets a new job in the University, this is in essence a simultaneous off-boarding and on-boarding process. Assuming the person does not have a manually-issued NetID, the odds that a duplicate ID will be created are low, but the transferring of appropriate permissions in surrounding business systems becomes more complicated because the NetID is not turned off.

Multiple appointments: As stated in the paper, people with multiple appointments – e.g. faculty who are also administrators, faculty with joint appointments – can have problems getting access to all the online resources they need because many of these systems are only equipped to have a single status for a person.

Off-boarding

The discussions with the focus groups have made one aspect of identity management clear - no one really wants to "off-board" a person and thus forget everything known about him or her. What they want is to selectively remove access to University systems or services based upon a change in status. In most instances, those interviewed thought in terms of a separation from the University (either employee separation or student graduation or contractor contract expiration, etc.); however, when the larger question was posed as to how to deal with multi-relationship cases, everyone recognizes that their own interest is in appropriate changes to remove a role no longer relevant to the affiliation with NU.

It is also clear that many portions of the institution want to remember all persons forever. There may need to be forensic investigation of access to information, or other needs for which the complete history of a person's affiliations and credentials should be retained. Again, no "off-boarding" without memory. (One noted exception to this is email addresses. While it would be possible, upon request, to not recycle email addresses for notable people, it is impractical to not have the default here be recycling. There are just too many Smiths, Chens, etc.)

Much of the discussion about off-boarding focused on the lack of understanding by a unit about how a separation event is described, detected, and acted upon. There were many comments that reflected wonder at how access to email (for example) is retained after an employee is separated. The fact that NetIDs are not locked upon separation is considered by some as a serious matter - while others acknowledge that access to some University systems (such as HR) must be preserved for some amount of time so that the ex-employee can carry out final reporting or view paycheck information.

All of these issues reflect the deficiencies in the current IAM environment which itself grew up from concerns of managing access more than managing identity. In fact, the current IAM environment has attempted to manage access to many systems (through the NetID being either valid or invalid) in a way which made the

systems themselves unaware that the IAM system even exists. Authentication either works or it doesn't and the application system deals with the result.

Unfortunately, with the proliferation of systems and the rich multi-relationship environment at NU, a simple "on or off" access model cannot continue. If an employee separates from the University, we must anticipate that he or she is also a student and not harm that relationship. Similar to this is the situation where a person gets a different job in another part of the University. Their NetID should always remain active, but their access needs to change, and with a “heads down, is the NetID active or not” approach, this can become problematic vis a vis turning off access to systems.

Given this context, we see an entirely new "off-boarding" environment emerge, where the applications themselves must decide if the new standing of a person warrants the continuation of services - rather than having the IAM system attempt to encode a person's status in a global sense. Notification to the application that a person's status has changed must trigger logic to decide whether that person's access should be ended or modified.

For example, the employee/student who is separated as an employee must be treated differently by NUFinancials, FASIS, the Training Management System, and BlackBoard (or Canvas).

- NUFinancials may immediately block access - meaning that a successful authentication (NetID and password have not changed) is answered with a "not authorized" response.
- FASIS may immediately restrict access to only those functions that are needed by a separated employee and block authorization to participate in open enrollment or approve subordinate timesheets.
- Blackboard/Canvas may see no need to change the status of the person within its own census of participants - or it may be necessary to take action because the employee was the instructor for a particular class.

These are examples of the identity marketplace aphorism "Authentication does not equal authorization". The person continues to have access via NetID and password, but services are curtailed within the context of the valid relationships between the person and NU.

Finally, in the new model being proposed, the person cannot be removed from the central registry even when all relationships have ended. Portions of the University's business want to remember that this person was an employee or a student and mine that past relationship.

F. Focus Group Result Summaries

Overarching Themes within the Feedback

1	Provisioning	Provisioning needs to be faster, easier, and more granular.
2	De-provisioning	Deprovisioning needs to be faster and more granular.
3	Granular Authorization	Authorization should be more granular to allow certain services to be granted, suspended, or revoked without affecting other services.
4	Multiple Relationships	Multiple relationships - joint faculty appointments, students in joint programs, a PhD student teaching a class, a matriculating employee - need to be accepted as normal, and access to resources for all roles needs to be straightforward.
5	Persistent Identities	A person's identity needs to be persistent through role changes and gaps in attachment to the University.
6	Internationalization	International persons present multiple Identity challenges.
7	Multiple ID Difficulties	Needing multiple different IDs causes problems.
8	Small and Medium Programs	There are many small and medium size programs which exist outside of central systems and - in aggregate - represent significant effort for schools and units to administer.
9	Integrated Systems	Systems should be integrated.
10	Single Sign-on (SSO)	All enterprise systems and other systems should implement SSO.
11	Wildcard	The Wildcard could be better utilized.
12	Basic Demographic/ Organization Information	Basic demographic/organizational information is hard to get from systems of record and is recreated locally, leading to inconsistencies and additional work.
13	Group Memberships	Group memberships are critical to the provisioning of access to services, including basic communications, and needs to be more available across the institution.
14	Proliferation of Active Directory (AD) Domains	The current proliferation of Active Directory forests has enabled the ability to provision services locally, but it also creates problems.
15	Manually asserted NetIDs	Manually asserted NetIDs, created outside the normal HR hiring or student matriculation processesare an ongoing identity problem.
16	Duplicate NetIDs	Duplicate NetIDs occur, with no easy way to remediate, and often no readily apparent way to tell they exist.
17	Management of Identities	The management of identities is quite difficult in certain ways.
18	Remote Members	Remote members of the community (out of the country or simply off-campus) pose challenges for retaining levels of assurance for electronic identities.
19	Changing and Expanding Community	The Northwestern community is Expanding and Changing
20	Additional Security Measures	Sometimes NetID authentication is not enough, and additional security measures are needed.
21	Assurance and Trust Levels	Identities need to have appropriate levels of trust and assurance associated with them.
22	External Credentials	Use of non-NetID external credentials would be very helpful for "loosely connected" constituencies, but there is concern about using them for everything.
23	Cloud Services / Federation	The roles of cloud services and Identity Federation will continue to grow as core elements of providing online services.
24	Future Projects	Future projects

Student Admissions

1	Provisioning	In the summer, Law School students often need to be provisioned within a week in order to make a deposit by the end of the week. Multi-stage provisioning makes this difficult. - Schools all use different processes. - Need for pre-matriculation application for housing and student loans flagged as problematic. - Parents often try to proxy for their children but there is not a mechanism in place to enable this as part of smoothly functioning standard operating procedure, e.g. entering freshman off at an international program for the summer, but entering students do not get matriculated until august,and they need to be matriculated in order to do this. If matriculation happens earlier, it is dfficult to unmatriculate and numbers in admissions and registrar's office get out of sync. - summer Academic Workshop (SAW), Weinberg Bridge program, Athletics (student athletes are term activated and matriculated early) are programs that can require special scrambling attention in the summer.
2	De-provisioning	Ditto re unevenly applied and can be mistimed.
4	Multiple Relationships	For a dual degree student, the school that admits them first "owns" them, which makes it hard for the second school to administer them.
5	Persistent Identities	Do not recycle NetIDs; clean-up effort is too onerous. - "Suspects" - people in whom we're interested, but have not contacted us - total about 250,000 annually; purged every 18 months - "Prospects" - people who have contacted us - totally about 90,000 annually; never purged, kept for ongoing reference. - CRM archives and purges data annually
7	Multiple ID Difficulties	The undergrad admissions process involves 3 IDs before they get a NetID: the common app, testing service ID, Recruitment Plus (being replaced by Slate). And there may soon be another ID for a portal to do iDoc checking. Is there a way to reduce this number of IDs? - Would like to have a single stage activation that activates both NetID and @U account instead of the current two-stage process. - there is an Alumni Interviewer application (CRM/CMS) that stores a separate ID. It would be better to have the IDs from OARD joined with other alumni systems to have one consistent alumni credential. - Requiring a separate ID to login to SES is seen as a security benefit rather than a usability negative.
9	Integrated Systems	- Students sometimes give different email addresses to Common App, Supplement and ApplyYourself system, and it's not always clear which one to use.
10	Single Sign-on (SSO)	Too many logins for individual systems, but having a separate SES login for adminstrators using it is seen as an important exception to this rule.
15	Manually asserted NetIDs	Ditto for short-term consultants and visitors. - Parents or those responsible (could be a company) for paying bills.
16	Duplicate NetIDs	- Not all systems use gender, which makes it more difficult to match people.
17	Management of Identities	EmplID removed from the NetID creation report when NUIT changed the process. This is a problem for TGS because EmplID is the unique identifier for TGS. It requires NUIT to run a report for TGS with NetID, EMplID, activation code. - New TGS enrollees often get bounced back and forth between TGS and NUIT help desk by the student workers at the help desk.
18	Remote Members	Ditto re off-campus students.
20	Additional Security Measures	No interest in two-factor authentication.
22	External Credentials	Given the sensitive nature of student information, there is concern about using non-NU identities for access.
24	Future Projects	the 2U Initiative will have its own "host campus ID", and when students enroll in a NU course, they will also need to get a NetID.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

Registrar

1	Provisioning	- Murky regarding what the process actually is. - Rights given to entering students is unevenly applied and can be mistimed for other processes such as applying for housing before registering, putting down deposits. - Systems and rights have "domino effects" - adding or removing from one group may have downstream consequences. - Three layers of access: NetID, group membership, special access within individual systems.
2	De-provisioning	- Ditto re this is murky: students graduate throughout the year but they stick around (active student vs active community member)., and students need to be able to pay bills after leaving. - Decisions are made on an ad hoc basis and nothing is known or coordinated. - All types of manipulations to allow post-graduation access to pay bills, give transcripts, etc.
4	Multiple Relationships	- Current view of a person is "too flat", one role, one term, one school (all the "current" one). - Distance learning has lighter needs, but still needs a profile, a logon, a group, what services they need, support for multiple roles.
5	Persistent Identities	- Every person should have one Identity, lifelong, work in multiple systems. - Profile should have limited but authoritative information. - IAM works well for people with uncomplicated path. Exceptions include: odd timing (taking a year off, compulsory military service for a foreign student, starting out of cycle, returning, switching roles), multiple identities (staff taking courses), multiple or overlapping ownership (BS/MS, Kellogg/Law). Same with faculty/staff.
7	Multiple ID Difficulties	- SES passwords expire quarterly.
9	Integrated Systems	- HR and SES may be giving out identities that are out of sync in SSN, Gender, ID, Name. Hard to fix. - NEED to allow for name, gender, SSN changes. - International names and fake SSNs hard to deal with. - Emergency info feels outdated when compared with directory. (EMergency contact phone numbers fed to emergency contact systems, but not the HBB info..
10	Single Sign-on (SSO)	Every system should use same ID/PW and should not require different logins.
12	Basic Demographic / Organization Information	Current Identity System fails on names (Spanish names, one-name names). - Name management better on HRIS than SES.
15	Manually asserted NetIDs	When a NetID is manually created for a student that is away from campus, how do they gracefully get transitioned back into the pool that is automatically provisioned?
16	Duplicate NetIDs	Makes it hard to match people across systems.
17	Management of Identities	- See manual assertions above. - Off-campus password change.
19	Changing and Expanding Community	- Consortium students (Study Abroad?) growing - Distance learning is going to press many issues to the breaking point - we cannot rely upon manual intervention at scale.
21	Assurance and Trust Levels	- Student calls:not coming back this quarter, can you withdraw me from my classes? - parent calls: what's up with junior? Need permission from Junior. Can't we do this online? (Parent ID?) - if using third party ID, needs to be able to be tied to NU trust levels.
22	External Credentials	- Distance learning has lighter needs, but still needs a profile, a logon, a group, what services they need, support for multiple roles. - Utility could be high for "loosely connected" constituencies (distance learning, Exec Ed, spouses), but concerned with security. - Shibboleth and Federation are important.
23	Cloud Services / Federation	Ditto re cloud services needing NetID authorization integration.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

Student Loans, Financial Aid, and Accounts

1	Provisioning	when and how a person receives a NetID varies - manual vs automated, timing (e.g. when they're admitted vs right before matriculation). Would prefer one uniform process. - give them sooner, require less paper, have the process more automated. NetIDs tied to FinAid, enrollment management, access to FB group. - Could also track people who are not engaged with the process. - Some concern (Law, Medill) expressed about an early NetID distribution creates frustration about not being able to get into different parts of the website. - Late admits need quick turnaround to see FinAid package and make deposit. - PhD students take longer because they're done annually, rather than continuously as the Masters students are. - Smaller program, e.g. Prosthetics/Orthotics, are often more manual and paper-based.
2	De-provisioning	When a student graduates, it's like we have disowned them. Students need to request transcripts, get tax info, see their financial aid history, pay NU via a credit card, see credit balances or account history long after NetID normally expires. - Recently received ability for student to pay via credit card and see their account, but their is concern this functionality will be lost in the next software upgrade.
5	Persistent Identities	Examples of students with intermittent access levels: CTD, PDPs, OLLI (Osher Lifelong Learning Institute - some register by check, can be short turnaround, some need access to Bb and some do not), SRO (Summer Research Opportunity - undergrads we hope will come to NU, can easily turn into early admits), High School Institute (400 students). - Some degree programs do not require continual enrollment. - Faculty also - International summer institute instructors (mid-July thru aug).
7	Multiple ID Difficulties	- Loan system is third party and does not use NetID or EmplID.
10	Single Sign-on (SSO)	Very frustrating to sign in multiple times. Should all be in SSO. - Cannot have multiple enterprise Systems open in the same browser, yet you often need to see information in multiple systems (SES/NUFinancials, SES/FASIS. - Shorter timeout in FASIS than SES.
16	Duplicate NetIDs	Duplicate NetIDS has been becoming less of a problem. - Examples of places where this can occur: employee/student (payroll does not have access to SSN in SES); employee taking an SCS course; High School Institute (Cherubs) applying to UG or grad school. - One program does not collect SSN or b'date. - Duplicate identities occur more on the EmplID side instead of the NetID side.
19	Changing and Expanding Community	Continued access for alumni will be even more of an expectation.
21	Assurance and Trust Levels	Recently received ability for "guest access to student records" (parents, 3rd party, spouses). Student needs to bring in documentation, and student owns the ID/PW. - different identities have different trust levels implied in them. For instance, by the time a person gets a NetID, they have been through many stages of verification, e.g. FAFSA for domestic Financial aid applicants, ApplyYourself, LSAT, AAMC, transcripts, outside firms doing verifications.
22	External Credentials	there is concern about the trust level associated with these identities. Probably more appropriate for the beginning and end of the student lifecycle., particularly for alumni who never had or never use their NetID.
23	Cloud Services / Federation	With online consortiums, perhaps federation could be set up to take the already vetted identity of the participant's own institution.
24	Future Projects	- Less paper, and more online forms with associated workflows. What consitutes a signature?

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

Student Affairs / Career Services

1	Provisioning	
2	De-provisioning	Kellogg students get access to different levels/types of career services depending on their point in matriculation. Electronic access is provided for 3 months after graduation, but exceptions are also made and overall it is hard to track.
3	Granular Authorization	There is confusion about what gets turned off, and when, once an undergraduate student graduates. Complicated by the fact that more students are graduating early, and there is confusion as to what turns off when they finish and what turns off when their degree is conferred.
4	Multiple Relationships	Joint degree students are difficult, for example, access to different career service levels at the two schools.
5	Persistent Identities	What gets turned off, and what remains, when an undergraduate student goes on leave?
7	Multiple ID Difficulties	Students confused by NetID and StudNetID.
9	Integrated Systems	Many systems not connected with basic demographic information. For example, faculty uploads are not linked, so data from FASIS is downloaded and manually entered into SES.
10	Single Sign-on (SSO)	Ditto
11	Wildcard	Would like to use Wildcard for attendance tracking, but it does not have the NetID on it, and that is what most applications systems use.
23	Cloud Services / Federation	Great interest in this and being able to easily connect them to university resources.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

Full-time Degree Program Students

1	Provisioning	Would have liked to have a central place to go to find out about systmes they'll be using and how to access them. Even their own department didn't know that much. Would have liked one more communication about this.
7	Multiple ID Difficulties	- Different systems cited: IBuyNU. - Confusion over u.northwestern Google account and their own Google account that they already had when they came to NU. - ASG trying to get to using NetID for all apps, but not there yet, e.g. some Drupal apps, a Google group uses a separate identity.
10	Single Sign-on (SSO)	Everyone really likes it when systems are set up to use the NetID and SSO is even better. Need to log in 3 separate times to get into Google, Blackboard, and Caesar.
11	Wildcard	- Use Wildcard for library and printing. - Frustration that the NU Library online book checkout doesn't remember your Wildcard Barcode. (Evanston Public Library's online app does, but NUL's does not.) - Like the new Wildcard with RFID for locks in Norris (and one place in McCormick). Better than swiping. - One student a member of two research groups. Needs two big key chains, 10-12 keys to between buildings. Some places require different keys for each side of a door, but there is one place where one key opens all the doors on one floor.
17	Management of Identities	Everyone LOVES having to update your NetID password only once/year.
22	External Credentials	Being able to use external social credentials was not seen as a benefot by these students, and they were leery of allowing it. They liked the separation of their social identities and their Northwestern identity.
23	Cloud Services / Federation	Being able to use a journal articles portal, which the student used every day, should "just work" with NU credentials.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

Non-degree, Part-time, and Certificate Students

1	Provisioning	Non-degree SCS students don't apply, they just register, which results in them getting a NetID quickly, but then they forget to activate it. - Non-paid SCS faculty need access to Bb, so they get a faculty appointment with 0 salary.
9	Integrated Systems	Systems used by non-degree programs are often unintegrated, so it's hard to gain administrative efficiencies.
22	External Credentials	- LinkedIn and FaceBook are sometimes used to attract candidates, but there are security concerns for using these sites beyond this. - Once people leave SCS, it's not clear how to keep in touch with them. Even if they get an NU email address, they don't use it. - Keeping track of inquirers, applications, and graduates takes a lot of effort. Email addresses are often used to identify inquirers, but there is a lot of effort spent de-duping these records. Group login IDs are used for group sites to reduce management overhead.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

NU Qatar

3	Granular Authorization	- See multiple relationships above. - Have built logic into authoritization services so individual services, e.g. network access, can be de-provisioned without interrupting other services, e.g. Bb, that would be affected if the NetID was turned off.
4	Multiple Relationships	- NetID belonging to two "top" groups, e.g. NUQ and Medill, belongs to neither group and must be managed by NUIT. - Want to prevent employee whose relationship with the campus ended, but was still a student, from getting email as an employee.
5	Persistent Identities	Ditto
6	Internationalization	Renewed passport sometimes gets new number, yet SES only allows one number.
10	Single Sign-on (SSO)	Yes
11	Wildcard	May want to utilize Wildcards more for building access.
13	Group Memberships	- Emergency response, bulk email, creating business processes tied to roles not NetIDs. - Ditto re difficulty for a manager to see access permissions for the people in their group.
14	Proliferation of Active Directory (AD) Domains	- Local employees or guests. Faculty/staff who transfer from a permanent position in Evanston. - NO audit trail to tell when out of sync. - Need to be careful if the forests are merged. NUQ uses some of the schema fields (e.g. Telephony IP phone field)locally, and that would have to be worked through before their forest could be merged.
15	Manually asserted NetIDs	- Students from other school, e.g. CMU, come to take NUQ course. Paper process, short turn around, asks if ever taken an NU course before but that is unreliable, only checking on name is not enough. - Need real-time provisioning with better de-dup'ing safeguards built in. (75 students/quarter) - Can be orphaned when "sponsor" leaves the university.
17	Management of Identities	- See multiple relationships above. - There are three different interfaces for account management via NUValidate.
18	Remote Members	Ditto
22	External Credentials	The admissions team wants to be in front of prospective students in 9th or 10th grade, and allowing them to create a persistent NU identity using FB (for example) credentials would be helpful.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

International Office

1	Provisioning	Ditto re mistiming and unevenly applied for enterpring students.
2	De-provisioning	Ditto re murkiness of this process.
5	Persistent Identities	Foreign CTD Students, students becoming staff.
6	Internationalization	Some students have multiple passports. Federal regulations require that they choose one.
7	Multiple ID Difficulties	Using new cloud system (lawlogix) for H1B case management. (500 cases a year, separate ID.)
9	Integrated Systems	- Demographic information (name, birth date, gender, citizenship, passport number, addresses) is critical to match with Federal government systems. - Instead of the Registrar's Office, IO maintains names and citizenship of International students. - Applicants may have applied with a self-reported "preferred" name, but the name in SES needs to match the passport. - Data formatting can be a problem, which can lead to duplicate identities or difficulty in matching information across systems, e.g. - Day and month of birthdate can get reversed - international students can have one name only, government regulations allow abbreviations of FNU / SNU (first or surname unknown), but when that gets printed on Wildcard, or Wildcard doesn't match passport, it can be a problem applying for a SSN. - IO depends on EmplID much more than NetID. Students sometimes get confused which is which.
11	Wildcard	Building a community of family members is hampered by policies pertaining to Wildcards etc.
12	Basic Demographic / Organization Information	Visiting scholars often have incomplete data.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

Alumni Relations and Development

1	Provisioning	Provisioning of EngageNU IDs will be done on a self-service basis. Users will be prompted for information that is in the database - graduation year, degree, etc. If they are not in the database, or cannot accurately answer the questions, they will get a low-access identity, and OARD will check their application and follow up with them if necessary. - Being able to self-provision a low-access guest/affiliate ID has been very helpful for wireless network access, and will be put to use in EngageNU as well.
5	Persistent Identities	OARD gets students who graduate and come to work for them, and yet their credentials don't easily (quickly and accurately) translate into an employee identity / getting paid.
7	Multiple ID Difficulties	- Upon graduation, alumni can either get a new email address with the format - @alumni.northwestern.edu - or keep their @u.northwestern.edu. Few switch to the new address. - Besides EngageNU, there are several other systems that alumni use - Going Global, Northwestern Career Connections, Simplicity - and it would be nice if they were all connected through SSO. (Though Simplicity has a single ID/PW for everyone.)
9	Integrated Systems	CATracks gets information on graduate students only when they graduate. Makes it difficult to log class gifts. Undergrads used to be similar (after admissions deposit taken, and then again upon graduation), but now they get regular updates from SES. - Multiple EmplIDs in FASIS and SES are problematic. - 10% match between FASIS and CATracks (staff who are alumni, donors, or parents). all uploads of staff data need to be manually checked because they need more potential matching points to avoid duplicates being mistakenly loaded into CATracks, e.g. OARD only receives home addresses from FASIS for people who allow their home address to be displayed in the online directory. - with more self service guest IDs for EngageNU, there is concern that it will be difficult to match these people up with other NU IDs, either currently existing or in the future. (A person could try to log in and instead of going through all the steps to vet a person for an ID, say, "Oh, what the heck, I'll just get a guest ID." - They would like to be able to more easily and accurately connect people who attend events with records in CATracks. (Everyone who goes on a travel program gets a CATracks record. It would be nice to do more to capture involvement and channel that into development.)
11	Wildcard	The only reason alumni would get a Wildcard is to get into the library. - OARD uses the Wildcard for access to 1201 Davis. They would like this to be more automated.
19	Changing and Expanding Community	Parents added into CATracks when Undergrads are added for the first time (potential donors). - CATracks also includes donors, people who have given large donations to other institutions, or has a relationship to a donor. - an "alum" doesn't necessarily have to have ever set foot on campus. - Attendees at programs given by Northwestern.
21	Assurance and Trust Levels	See provisioning above.
22	External Credentials	EngageNU will create an overarching identity gateway where persons self-identify and are matched to one or more internal systems.
23	Cloud Services / Federation	EngageNU will also front-end other cloud services for alumni.
24	Future Projects	OARD would like to be able to track engagement better, e.g. attendance at events, and do things like having a loyalty/reward program. - As more events go online, being able to track these participants becomes more important as well.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

Human Resources

1	Provisioning	- One person replacing another should trigger the provisioning of a core set of access permissions, and/or there should be functionality built into the hiring application for access to services to be selected or deselected as part of the process. - Early on-boarding is possible (people can be hired 90 days in advance), but administrators don't know about it, or don't know what is required to do it (e.g. employee must submit a signed Personal Data form to generate a NetID). Not doing this leads to the creation of a manually asserted NetID, which leads to duplicate NetIDs.
2	De-provisioning	- Knowing how this is done is murky and should be better documented and more transparent. - Paperwork is not always submitted in a timely manner, and it can take 5-7 days for HR to process once submitted. Also, resignation dates can change. - These decisions need to be made at the application level, not centrally, but they also need better information. - NetIDs and email accounts are currently kept active for 45 days after termination in case employee is extended. - Would like to use for enrolling new employees in Orientation or providing instructions on COBRA to terminated employees.
7	Multiple ID Difficulties	Should NetID replace EmplID as the unique identifier.
9	Integrated Systems	Many systems not integrated to employment changes in FASIS, e.g. NMFF terminations, building security.
11	Wildcard	Few people know what services are tied to the Wildcard and how those are controlled.
13	Group Memberships	See also provisioning below.
15	Manually asserted NetIDs	HR is committed to POI via FASIS as a replacement for most manually asserted NetIDs.
23	Cloud Services / Federation	Used for benefits (e.g. Dearborn) and NU FitRec.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

Faculty

1	Provisioning	It often takes too long for TAs to get access to Bb. - International students often take too long to gain access to Bb. - Affiliated post-doc access is not well defined or established.
5	Persistent Identities	"Wildcat for Life" is a great opportunity. How do we make it easy for faculty to be connected with alumni? - Will Jive be a good way to integrate alumni more into the fabric of life on campus?
9	Integrated Systems	Having the students in the Google environment and the faculty in Microsoft makes it very hard to share documents. - Being able to integrate alumni into Bb courses should be easier. (SESP's use of Jive, and SoC's use of Drupal address this need.) - As more course materials become digitized, it becomes more difficult to put together a "course pack", as each vendor has a different system that needs integration of identity and access. - Students are using whatever system is available to them to collaborate, whether it is a Northwestern system or not.
10	Single Sign-on (SSO)	Too many logins and disconnected systems. More systems should be linked via SSO and a portal, and more services should be online workflows. Texas A&M has a good faculty portal
18	Remote Members	The requirement of physical presence to gain, or reset a NetID, is problematic for people overseas (or even just off campus).
19	Changing and Expanding Community	As the nature of "the learning experience" grows beyond the classroom, it is important to be able to easily connect people enrolled in a course with those who are not as directly connected.
21	Assurance and Trust Levels	How do we ensure that a person who signed up for a course is the person taking the test and submitting homework and participating in course discussions?
23	Cloud Services / Federation	As more services move online and offcampus, being able to easily connect our systems to them becomes ever more important. - Most learning will be moving towards a blended learning model, and most learning platforms will be moving to hosted solutions.
24	Future Projects	There is a need for digital signatures. Paper -> pdf -> paper -> pdf process is laborious and inefficient. 90% of the documents that go through this process are internally generated and many cycles of effort could be recouped by turning these into online forms with electronic approvals. e.g. Research appointments, faculty pay adjustments, legal contracts and commitments.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

Office for Research

1	Provisioning	- Security access forms are all paper. - Should start earlier so things are available when the person needs them, or arrives, e.g. bulding out lab space, applying for grants, Bb access.
2	De-provisioning	Automated deprovisioning is needed upon termination in FASIS.
3	Granular Authorization	Earlier on-boarding of faculty and post-docs is needed to support grant applications, Bb, etc.
4	Multiple Relationships	Ditto re faculty with joint appointments. A specific would be setting up security access.
5	Persistent Identities	ISIS tracks training requirements and compliance via NetIDs. Recycled NetIDs can create big problems.
7	Multiple ID Difficulties	Get rid of second ID for administrative access to FASIS.
9	Integrated Systems	Many examples of unintegrated systems
10	Single Sign-on (SSO)	Ditto
11	Wildcard	More integration would be helpful. For example, having the barcode available in LDAP/AD as another credential or a 2nd authentication factor. Access to animal facilities. Some people have Wildcard but not NetID.
12	Basic Demographic / Organization Information	- Basic phone number information in FASIS is incomplete because it is dependent on user input rather than being part of the hiring process. - Should be easier to see Visa status. - Animal facility access stores NetIDs, but users have to enter name and email address.
15	Manually asserted NetIDs	- Post docs with dummy NetIDs. - Outside reviewers. - Conference attendees.
20	Additional Security Measures	- VPN is difficult for some people. When do you need it? When should you use it? Which one to use on a public computer? - Too much firewall security, though additional channelling is needed in secure locations such as healthcare locations.
22	External Credentials	Discomfort expressed with this idea, but there was acknowledgement that many faculty do not use their Northwestern email account and students use FB.
23	Cloud Services / Federation	Not interested as much because of sensitivity of data.
24	Future Projects	- Lab membership database (access and protocols) - RFID inventory management system to track cages, people, and supplies. - Global view of faculty member's research profile. - Interaction with external partners (Argonne National Lab, Fermilab, Field Museum, etc..

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

Feinberg School of Medicine – Research Administrators

1	Provisioning	There are often delays in getting NetIDs. They would like to designate the need for a NetID earlier in the process. - It would be better if the provisioning of a NetID could be tied to other on-boarding tasks, e.g. provisioning of a Marlok key.
2	De-provisioning	In general, the expiration of the NetID upon termination works well. - NMFF and NMH require specfic paper requests in order to terminate access. - Project Café security requires a phone call to get access removed upon termination, and sometimes it is difficult to get former employees removed from a contact list for vouchers. - Sponsored research needs to have the NetID stay on when a person leaves.
7	Multiple ID Difficulties	- With multiple institutions providing different services, faculty sometimes have troulbe remembering passwords, e.g. for evaluating residents, or don't know which ID/PW to use where/when.
9	Integrated Systems	You cannot be logged into two enterprise systems at the same time in the same browser, and yet sometimes you need to access information in one in order to confirm or do work in another. - Some doctors have 3 email addresses, so findign them is difficult, and sometimes their administrative assistant can't access one of their calendars.
10	Single Sign-on (SSO)	There are many systems involved in doing research and/or administering research, and they are spread across multiple institutions and used by very busy people. The more they are centrally accessible and the fewer ID/PWs required, the better. Two things that would help: - SSO - Access via a portal, preferably with profiles that provide default access to services for a particular role, e.g. research administrator. - NMFF, NMH, FSM is complex and fragmented, but it would help if Northwestern systems were organized better. - iBuyNU should be on SSO
11	Wildcard	The divisions between Northwestern, NMFF, and NMH make it difficult to provide administrative support for researchers. One way this happens is sometimes it is difficult to get a Wildcard if you're not a direct employee of Northwestern, which limits your physical access to some places to regular business hours. - Wildcard is needed to get a Pcard, and sometimes an administrator can't get one even thought they have responsibility over Northwestern personnel.
15	Manually asserted NetIDs	- Volunteers, contractors, affiliates all need a more smoothly flowing on-boarding process. - If someone is going to work behind a locked door, they're going to need a Marlok key, and you need a NetID to get one.
19	Changing and Expanding Community	The North Shore clinical expansion is going to place more strains on the delivery of services because the new members of the community will be even more remote and will be unfamiliar with the ways of Northwestern. - Collaboration with external people is critical. Everyone figures out a way to make this happen one way or another, and not prioritizing the delivery of this functionality would be a significant oversight.
20	Additional Security Measures	Many of the administrators in the focus group LOVE VPN, but it was also acknowledged that it is a mystery, and therefore a barrier, to many people. (People don't know it's required for some services, e.g. Kronos, don't know you have to go to the NUIT site to get it, and there is no training for it in on-boarding.)
21	Assurance and Trust Levels	If a PI could electronically acknowledge their monthly budget statement has been reviewed and approved would have a huge impact. ("Save a staff person in every department and lots of paper and storage.")

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

NUIT – Academic & Research Technologies

1	Provisioning	There may be time lags getting students access to the research systems (Quest, Vault, Depot) at the beginning of an academic year as they get activated. - Facilitating the sharing of data is often difficult becasue the number of data donors is large, and each requires a NetID (or a User ID on one of the systems - i.e. a UID, good for one time only with a six-month lifespan) to provide the data. - Provisioning by roles, or via a catalog of services, would be beneficial. - Similarly local account User IDs can be created on Bb if a person does not have a NetID.
2	De-provisioning	Knowing when someone is leaving the university, which data is theirs, and what should be done with it can be difficult.
3	Granular Authorization	Research computing often needs to give access to file directories, or academic computing sometimes needs to give access to a Bb course.
4	Multiple Relationships	Ditto multiple relationships.
5	Persistent Identities	Ditto persistent identity through role changes.
7	Multiple ID Difficulties	Quest is a UNIX system which needs a UNIX ID for account creation. This is needed sometime before a NetID is created for the user.
11	Wildcard	A&RT would like to use Wildcard photos as roster photos in Bb.
13	Group Memberships	There is a need to grant access to particular levels of file shares. The administrators may not know who gets access at lower levels of the directory structure.
15	Manually asserted NetIDs	A unique requirement - data donors must access Vault and transfer data into the storage system. Issues of both access and ultimate data administration and data protection/lifecycle exist here. Looking today at certificate based authentication to the facility. - Ownership of relationships outside the university, and management of those relationships, can be difficult.
19	Changing and Expanding Community	See above re research with people at other institutions.
23	Cloud Services / Federation	Much of the collaboration that goes on at Northwestern, and one of the parts that can be problematic in granting timely access, is with faculty and graduate students in other universities. There is interest in addressing this via federation with these other institutions - Multiple cloud vendors being examined for potential inclusion in the portfolio of services, e.g. Box, Aquia, Amazon Glacier. Will need to be interconnected with the Northwestern IAM ecosystem.
24	Future Projects	- Some schools, e.g. Medill, would like to make all their materials accessible by their alumni. - More usage of Social Media and needing to integrate that content with more traditional course content. - Learning Tool interoperability: If a student can get into an instructor's Bb site, s/he can also get into other sites s/he "owns".

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

Feinberg School of Medicine – Medical Affiliates

1	Provisioning	It's unclear who approves new accounts (varies by system). - There is concern about the delivery method of accounts not being secure. - Outside affiliates are even more difficult to manage than the NU/NMFF/NMH issues.
2	De-provisioning	Deprovisioning is very difficult with all the different institutions and different roles and policies within each one.
4	Multiple Relationships	Would like there to be a dashboard view to see a person and their affiliations.
5	Persistent Identities	Transfers are as big a problem as hires and terminations.
7	Multiple ID Difficulties	The Enterprise Warehouse requires different ID/PWs for reporting.
9	Integrated Systems	The systems are not integrated - no portal, no SSO, multiple ID/PWs - and it is therefore difficult to on-board someone effectively, or provide access consistently, e.g. access to the library for people without NetIDs.
19	Changing and Expanding Community	Lake Forest physicians don't get NetIDs, and are not made faculty. - Enterprise Data Warehouse is now expanding to include more institutions outside of NU.
20	Additional Security Measures	Dual factor authorization would be nice to have.
23	Cloud Services / Federation	Cloud services will continue to grow, and they're very attractive due to their convenience, but there is concern about their compliance with PHI and HIPPA regulations. - If there can't be one identity for NU/NMFF/NMH, then they would like there to be federation between the institutions.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

Feinberg School of Medicine – Medical Education

1	Provisioning	Difficulties in provisioning were a major focus on the discussion. The process takes too long, is too much based on paper, the forms get lost a lot (1/3 of the time, either in the Provost's Office or in payroll), and there is no window into the process to see what has been completed and if it is moving. For new administrators, being able to do one's job is often problematic. The hiring process is protracted and indeterminate, there are no role- or position-based lists of what access and training is required, and the training is infrequent, unintegrated (e.g. Cognos and FAMIS), and sequential. Lower-level people can be immobile for weeks (and you're tempted to give them your ID so they can do their work), and it can take 9-12 months for higher-level managers/directors to get all the access they need to do their jobs. Access permission forms are repetitive and nuanced so much that you don't know what they really need. Would like: - a way to say: give this person what the previous person had. - online dashboards that can be seen by HR, hiring manager, new/departign employee. - on-demand, smaller-modules, JIT training Would like to have a list of systems that are available and who to talk to about them. Would like checklists, e.g. if you're a dept admin, you need these sets of access and these training courses.
2	De-provisioning	- When someone is terminated, it's not a process that is done frequently, so it's hard to remember what and how to do it. - Would like a transparent checklist that everyone can access - employee, manager, HR.
3	Granular Authorization	Much frustration with the access permission process - on-paper, not-reliable, new each time. And when a new set of access is added, all the existing permissions get deleted and have to be added back in.
5	Persistent Identities	Being able to register people for non-credit courses (CME - Continuing Medical Education) is difficult. Have to use the CERTAIN system, where a person has to register independently for each course, each time. No way to have a persistent identity.
7	Multiple ID Difficulties	- Many systems require different identities: I9 Login Galter Library Apply Yourself @FSM google accounts GATS IBuyNU administrative ID/PWs for FASIS and SES HR Benefit systems, e.g. FSA - Administrative Systems should work like Kronos does - it gives you access to both sets of information/functionality you need: self-service and as a manager. - People really like being able to use just the NetID.
9	Integrated Systems	- Much of the discussion was about the frustration of unintegrated systems, and the need for multiple ID/PWs. - Business process improvements - on-boarding, off-boarding, uncoordinated registrar offices and systems across the university -- were a major theme of the discussion. This was seen as something that would not linger in the private sector, but was typical of higher education.
10	Single Sign-on (SSO)	Significant chunks of the discussion focused on the lack of unification around the NetID, though no one mentioned SSO by name.
24	Future Projects	Increasing regulations around HIPAA and PII, e.g. FISMA, will be an increasing problem, partially because the standards are increasing but unclear, and partially because our existing systems were not built with this in mind.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

Northwestern University Library

1	Provisioning	Ditto authorization should be more granular. Granular authorizations should make it easier to give out NetIDs with limited permissions. - Ditto when/how authorizations are granted or removed is murky. - Need to be able to handle person who comes in off the street to look at The Tribune for 2 hours, and a graduate student who needs to come for 7 days to research African studies.
2	De-provisioning	Ditto when/how authorizations are granted or removed is murky. - Assigning expiration dates for students are not reliable. - People build personal collections of resources, and because the library systems are not closely connected to systems that track departures, and because the departures are often loosely defined, a lot of "junk" accumulates.
5	Persistent Identities	Ditto persistent identity through role changes. Sometimes role changes are temporary or not even meaningful - grad students who teach during the summer are really NOT faculty.
9	Integrated Systems	Ditto matching individuals across enterprise systems is difficult. - Difficult to provide access to course materials because person identity information is not integrated in one place with course registrations.
11	Wildcard	The fact that the Wildcard is separate from IDM causes problems - such as absence of barcode from LDAP. - Didn't know until this year that the Voyager patron feed was coming from the Wildcard system. This feed has been very problematic. - Wildcard barcodes and NetIDs are not correlated and easily available. - New Wildcard did not have a barcode on it. - Library, SPAC, and Office of Research uses Wildcard heavily.
13	Group Memberships	Custom groups are needed all the time for providing access to a custom set of library resources - e.g. all music faculty, a professor and her graduate students, thesis and dissertation committees. - They would like to have real-time access to course enrollments and instructors.
15	Manually asserted NetIDs	Ditto concerns about affiliates who do not have NetIDs at all.
17	Management of Identities	Ditto IP address range authorization problems. - Didn't know until this year that the Voyager patron feed was coming from the Wildcard system. This feed has been very problematic. - 30,000 records in the feed. Errors cause the feed to crash. 1,500 people had duplicate entries. - 23 different fields are needed to do authentication for all NUL systems. - Creating shadow systems to store data necessary to do authentication and authorization in "local" systems is inefficient and a security concern. Having a centralized way to get access to this data is preferable. - When someone is no longer included in a feed, there is no
20	Additional Security Measures	Very interested in two-factor authentication utilizing people's smartphones as the second factor. The library sees this form of security more effective than longer passwords, VPN, and IP-based access.
21	Assurance and Trust Levels	Identity credentials need to have trust levels associated with them. Lifelong learners, spouses, alumni need access to library services, but NetIDs provide so much more. Galter Library runs Ezproxy because they have so many affiliates that do not have NetIDs. (But EZproxy does not work with our current version of Shibboleth.)
23	Cloud Services / Federation	Federation is essential, Shibboleth must be updated and should be put in front of more systems. - The new cloud-based Voyager (Alma) will need straight-forward Identity Management routines to look up identity information rather than looking at internal database, e.g. getting information from an LDAP database, and current workarounds will not be supported by the vendor. Wildcard barcodes are not in LDAP.
24	Future Projects	Social media to help in research / collection building: people who read this, also read that; people who cited this article, also cited these other articles. (Recommender intelligence.) - Digital preservation functionality requires an audit trail - creation, access, digital signature, and not only NetID, but role at the time, e.g. student, faculty, researcher at FSM.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

Financial Operations

2	De-provisioning	- Procedures are not consistent and are not documented. Some privileges remain longer than they should. - Desire for a single point of access discontinuation instead of the existing, multi-office, multi-step process required today. - Weekly termination reports are suspect, resulting in false positives and access remaining in error. The window for a status change is 60 days. - Paper-based deprovisioning needs to be replaced by eForms with workflows. For example, faculty with Courtesy Appointment files for unemployment but is still listed as "active" because form was either not submitted or entered in a timely manner.
3	Granular Authorization	All or nothing security holds are counterproductive.
4	Multiple Relationships	Ditto
5	Persistent Identities	- Faculty adjunct appointments should be easier to handle than the current practice of creating work-arounds such as courtesy appointments.
7	Multiple ID Difficulties	Vista, ProCard, FundDriver, and iBuyNU do not use NetIDs. (Different password conventions, frequencies for PW change, username conventions, etc.)
9	Integrated Systems	- Electronic signatures. - Reimbursing students is difficult because each one has to be manually entered as a vendor into NUFinancials.
10	Single Sign-on (SSO)	All enterprise systems and other systems should implement SSO.
11	Wildcard	Wildcard processing has high trust for FinOps. Works well to physically verify people as being connected to NU.
12	Basic Demographic / Organization Information	Would like to see more basic info on people in Active Directory, e.g. basic role, NetID source, temp vs NU employee.
15	Manually asserted NetIDs	- Manually asserted NetIDS are a mess and should be eliminated. There needs to be processes to vet individuals before they can request certain authorizations. - Most (90%) of manually asserted NetIDs that need NUFinancials access are from NMFF/NMH. Can federation exist here? - No standardized process, no eVerify or other identification verification. - POI process should be clarified, or adjusted, to include identification verification. - NetIDs have "owners", but this does not equate to "supervisor", often a technical person who created it, often leading to extensions that are not appropriate.. Workflow could help here.
16	Duplicate NetIDs	Manually asserted NetIDs cannot be repurposed for the same person when someone is hired. It must be retired and a new one created, often resulting in multiple NetIDs that require: troubleshooting, manual transfer of Exchange email, transfer of access rights, etc.
17	Management of Identities	No ability to merge NetIDs when one person mistakenly gets two.
20	Additional Security Measures	- Would like to see two-factor authentication for all processes involving cash and health/safety issues, e.g. building access.
21	Assurance and Trust Levels	- Wildcard processing has high trust. NetID is pretty h igh trust for SES/FASIS assertions. - Manually asserted NetIDS are a mess and should be eliminated. There needs to be processes to vet individuals before they can request certain authorizations. - Ultimately there should be a trust level associated with a credential and an identity so that applications can make a decision about which services will be authorized. - Identities should have trust levels associated with them (e.g. 0,1,2,3) or perhaps attributes to allow specific access, e.g. vetted for cash-handling, eVerified.
23	Cloud Services / Federation	Going to become more commonplace. Need to be able to integrate easily with NetID authentication.
24	Future Projects	Automate contract processes, leverage electronic identities and electronic signatures. Want to allow vendors to sign without "wet ink".

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

Project Café

4	Multiple Relationships	Ditto multiple relationships. EngageNU must look at HRIS and SES.
7	Multiple ID Difficulties	Manual ID/password maintenance for iBuyNU is hampered by Shibboleth.
9	Integrated Systems	The lack of integration of EmplIDs between SES and FASIS forces CATracks to look at both.
15	Manually asserted NetIDs	Ditto concerns about affiliates, contractors, etc., on-boarding and off-boarding.
18	Remote Members	Netid password resets are problematic for some users due to requirement of physical presence.
19	Changing and Expanding Community	EngageNU is projected to have a few hundred thousand users., far beyond the NetID user base.
20	Additional Security Measures	IP address range authorization security is becoming more of a problem as the university expands into affiliate institutions such as RIC. This is done as way to remove the need to use VPN, and there is hope to get away from these additional security layers. - If SES and FASIS move to two-factor authentication, NUFinancials probably would follow.
21	Assurance and Trust Levels	The new EngageNU Identity Management process, which will allow alums to use external 3rd party ID/PW to login once they have verfivied their identity, will be innovative and should prove very successful because most alums have struggled with, or resisted, using NetIDs to login to systems. - The risks of using 3rd-party credentials are limited because a) alums already have unique identifying information on file that can be used to vet initial activations, and b) their online activities are limited in scope.
22	External Credentials	The new EngageNU Identity Management process, which will allow alums to use external 3rd party ID/PW to login once they have verfivied their identity, will be innovative and should prove very successful because most alums have struggled with, or resisted, using NetIDs to login to systems. - The risks of using 3rd-party credentials are limited because a) alums already have unique identifying information on file that can be used to vet initial activations, and b) their online activities are limited in scope.
23	Cloud Services / Federation	The version of Shibboleth run at NU is hampering progress with using federation more widely.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

University Services, NU Police, Facilities Management, Athletics/Recreation, Audit

1	Provisioning	When/how authorizations are granted is murky - Would like there to be a catalog of services to assist in provisioning at the local level.
2	De-provisioning	When/how authorizations should be removed is murky.
5	Persistent Identities	There is often confusion when an employee transfers on whether they should keep their same NetID, email address, and/or access.
8	Small and Medium Programs	CBORD is a cashless card system that University Services has implemented for "Munch Money" and Papercut (printing in the all libraries). It does not use NetID. These systems are confusing to parents, faculty, and students to set up accounts, each of which has its own identity. - PACIOLAN - Athletic ticketing system. Uses Wildcard; integrated with feeds from CATRacks. Self-service account creation that does not tie back into NU systems. FAMIS - Facilities management tracking system. Access needed for contractors and vendors, only some of which get a NetID. - Marlock - can be tied to Wildcard. - Millenium parking - very manual process to maintain.
11	Wildcard	- Retrieving WildCards when people leave the NU community could be improved. -The University of Michigan went to a one-access credential and locations that were not connected to the network were problematic.
12	Basic Demographic / Organization Information	It would be helpful to have access to data such as: paid/unpaid, current/former affiliation(s), contact info (email, phone, radio #).
15	Manually asserted NetIDs	There is no central repository to house all contractors, so it is difficult to know who is still working. Sometimes, the contractor's access is cancelled in order to see if someone calls. - Sometime contractors report to other contractors. - Architects arrive before the project officially starts. - Would like to be able to tie contractors to projects.
20	Additional Security Measures	The University of Georgia is using biometrics to allow access to dining facilities, thereby eliminating the need to carry a card.
22	External Credentials	the Athletics website allows connections to FaceBook but they're not sure if using FB credentials is possible.
23	Cloud Services / Federation	The new version of FAMIS is hosted, and Athletics uses a hosted service.
24	Future Projects	Athletics sees mobility and mobile device apps as a potential win for ticketing

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

School IT Architects

1	Provisioning	- WCAS is a large, distributed organization, and being able to provision school level resources quickly or in advance is often difficult. This includes new Staff/faculty member, changes in status or affiliation. Being able to subscribe to an automated event notification would be very helpful. - Medill has a better sense of when people are on-boarded. Their problem is more with the timing to NetID provisioning. Student information is worse than faculty/staff.
2	De-provisioning	Knowing how to de-provision local services, either to terminate the access or suspend it, can be difficult due to the lack of contextual knowledge.
4	Multiple Relationships	Very important to know all relationships have administrative access to a person even if another school is their primary school. - WCAS gets data feeds on dual program students once/year.
5	Persistent Identities	Would like to have a persistent profile for each person.
12	Basic Demographic / Organization Information	Would like to be able to see all data for a person in one spot.
13	Group Memberships	Having better access to this information would help WCAS maintain bulk email lists dynamically rather than manually as it is done now. - Would like a clear view of all group affiliations. - Most of these groups happen at the school level and central systems have no awareness of them.
14	Proliferation of Active Directory (AD) Domains	In Medill, a change in a person's status, something happens to their access and they need to reset their password. - The de-provisioning of NetIDs in the Medill forest seems to not be effective, because they have about 2,500 NetIDs, with a normal anticipated total of 1,500.
15	Manually asserted NetIDs	Ditto concerns about affiliates, contractors, etc., on-boarding and off-boarding. Even for faculty, timing is everything - need an event that triggers local provisioning in file systems, etc.
21	Assurance and Trust Levels	Access to different sets of data needs to be based on the nature of the data and the trust level associated with an indentity.
22	External Credentials	Having a means of identity that is chosen by the user, and is not NetID based, would be very useful for more loosely connected constituencies, e.g. Executive Education particiations, CTD, Cherubs. IAM is an issue even for students, who, by the time they matriculate, have already had 3-4 different IDs in the application process.
23	Cloud Services / Federation	More and more services are moving to the cloud, and we need to be able to easily and via standard mechanisms, integrate those systems into our application ecosystem. And we need to be able to do this for all sizes/types of 3rd-party vendors. Some may want to do Shibboleth, some may want to authenticate straight to our AD/LDAP directories.
24	Future Projects	More and more services are going to migrate to mobile devices. NU Passport, as it now exists, is desktop-centric. Mobile applications generally have longer authentication periods.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

Business Intelligence

2	De-provisioning	Removing access is just as important for transfers as for terminations.
3	Granular Authorization	Information that is effectively public should be available with only low barriers to requesting applications.
7	Multiple ID Difficulties	Matching individuals across enterprise systems is difficult. Cross-system data integration requires extensive manual data matching/massaging because, for instance, matching faculty across systems only gets 80% matcheed without it.
9	Integrated Systems	- Security provisioning/de-provisioning processes are cumbbersome, paper-driven, with signatures and faxing required. For example, removal of access to BI occurs manually upon receipt of a request from a department. - Need better integration of SES and FASIS on unique identities of persons.
10	Single Sign-on (SSO)	SSO works well for BI. If it is more widely deployed, it needs to have a more fault-tolerant infrastructure.
13	Group Memberships	Role-based access authorization is needed to streamline provision of access to aggregated BI data.
22	External Credentials	- OK as long as it's tied back to a Northwestern ID. - More appropriate for "loosely connected" constituencies with less frequent ties to the institution.
24	Future Projects	- Early indicators point to a desire to analyze applicants who do not attend NU, which may necessitate a better understanding of applicant identity. - If BI begins providing its data as a service to other applications, there will need to be NetIDs created for applications (a concept that apparently does not exist now) because access to data is NetID-based.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

NUIT - Collaboration Services

4	Multiple Relationships	- The number of joint appointments is proportionately small, but the people affected are often very important. - Administrators cannot see these people unless they are "in" their department. - Joint degrees (KSM, FSM, Law, WCAS)
5	Persistent Identities	- This can be most annoying in the satellite AD forests. - Re-provisioning NetIDs requires re-provisioning of access as well, e.g. access permissions to the Dean's calendar. - Lag times in the provisioning of access to services, e.g. Bb - for SCS instructors who teach for a quarter (treated as affiliates), can impact ability to do their job. - Retired learners (ILS) are not in SES, so SCS has to create new NetIDs every other quarter for access to Bb. Same is true for CTD students.
8	Small and Medium Programs	Parking in Chicago is not well integrated.
10	Single Sign-on (SSO)	Yes
11	Wildcard	Chicago Wildcards contain a chip for building access. Evanston's do not. Is the future of the Wildcard a card or an app? Could it be used for CTA or purchasing?
12	Basic Demographic / Organization Information	A change made in demographic information within one directory environment should be propagated throughout all environments.
13	Group Memberships	- Collaboration - communications (email lists), access to files (SharePoint sites, network shares), scheduling group meetings - is founded on group memberships - so establishing them, viewing them, and using them are important. - Currently, it is difficult to get this information and to have it ripple across systems, and it is difficult for a manager to see access permissions for the people in their group. - Exs: Tenure-track faculty, class year, program of study, manager, department. - Need common definitions of role, e.g. manager and department.
14	Proliferation of Active Directory (AD) Domains	- General disconnect between ADS and satellite AD forests is frustrating. Pushing of information to the satellite often requires a password change to trigger. (Admitted student gets access to Bb and SES, then matriculates to Law and has to change PW to get access to Law resources.) Changes within the satellite are not promoted upwards. - Satellite AD forests are often preserved so that local group administration can be scripted. - Inconsistent identity management through role changes can be most annoying in the satellite AD forests.
15	Manually asserted NetIDs	- Manually asserted NetIDs are unknown to FASIS. - International students with Dummy SSNs can end up getting multiple NetIDs when they get their real SSN.
16	Duplicate NetIDs	- ApplyYourself feeds also create duplicate NetIDs.
17	Management of Identities	See multiple relationships above.
18	Remote Members	For example, SCS and SESP students, admitted international students. Facilitate by sending automated text or email to use to reset PW.
24	Future Projects	Online students will grow and create new issues

(NOTE: To see brief descriptions of the 24 themes, see page 79.)

NUIT – Identity Management Administrative Units

1	Provisioning	Rights given to an entering student are unevenly applied and can be mistimed for other processes. Just knowing what stage a person is in for the admissions process, and what permissions are tied to that stage, is difficult. - The provisioning of IDs/access to relatives - parents, spouses - is too complicated and results in students often simply sharing their NetID/PW with them.
2	De-provisioning	When/how authorizations are removed is murky. - Ditto authorization should be more granular. Disabling services should be by service, not by disabling the NetID. - When groups are about to be expired, the system should notify the appropriate administrator, not the generic NUIT contact.
3	Granular Authorization	Would like to have a catalog of services to facilitate provisioning and deprovisioning.
4	Multiple Relationships	See below "Management of identities."
5	Persistent Identities	Persistent identity through role changes is very important but has lots of difficulties associated with it.
7	Multiple ID Difficulties	They would like to use regular user NetIDs when working in Enterprise Systems.
9	Integrated Systems	Matching individuals across enterprise systems is difficult.
10	Single Sign-on (SSO)	Web SSO should be used more widely.
12	Basic Demographic / Organization Information	Ditto change made in demographic information should be propagated
15	Manually asserted NetIDs	The format for entering these precludes the entering of data that would be very useful for managing the NetIDs later, e.g. phone numbers or comments. IT people sometimes make themselves owners when they really are only the person entering the data. - System/application NetIDs should never expire, but they are often set up incorrectly, causing support services to fail unexpectedly. - Too often we give someone a manually asserted NetID, and then they leave and come back and get a second ID later. - Early onboarding of NetIDs in order to get them access to a needed service before they are "official" in SES or FASIS leads to duplicate NetIDs. - Departmental NetIDs introduce some of the same and new problems.
17	Management of Identities	All aliases for an email address in Exchange should be visible within the identity system. - There is not a utility for merging NetIDs when someone is given a duplicate by mistake. - There is no audit trail on who changed security permissions, why, or when. - Information in the Identity System is not organized well, e.g. need to look at 3 different fields to tell someone's primary affiliation. Belonging to multiple departments is visible in LDAP, but not in NUValidate. - Would really like to have the ability to view a person's complete access profile. - Small changes within the Identity System take too long to get done. It should be more amenable to small changes.
18	Remote Members	This is a big hurdle for the HelpDesk. They would like to have a system that does not require a physical visit to the HelpDesk to activate or reactivate their NetID. Perhaps using people's smartphones as a second factor authenticator would help here.
23	Cloud Services /	We need to continue to look at this.
24	Future Projects	We need to be looking at how to best secure mobile applications.

(NOTE: To see brief descriptions of the 24 themes, see page 79.)