Program Summary

DoIT supports NIU's account lifecycle for faculty, staff and students who access many of the institution's core enterprise applications. This centralized service also synchronizes with PeopleSoft Human Resources and Student Administration systems to create and terminate access, managing credentials so that faculty, staff and students can access only those systems to which they are authorized.

DoIT's identity and access management team provide support for the entire authentication infrastructure that is integrated with HR systems to manage employee status and securely force password resets on a regular basis. In order to meet new and existing security and compliance requirements, this program is expanding to include such things as multi-factor authenticated, federate and role-based access.

Criterion 1: Importance to University Mission / Operations

Importance to Mission

While secure identity management systems are not directly attached to the teaching, learning and research activities at the heart of a university, they are essential to every operation that requires secure access to the core of shared and integrated applications. This embedded infrastructure of servers, software and technical staff together provides the centralized account management for every staff and student member affiliated with NIU. DoIT's identity and access management system provides the comprehensive infrastructure needed to manage access so that classes can be taught on premises and at distance, students can access course materials anytime and anywhere, budgets can be managed, and bills can be paid.

Importance to Operations

One way of describing the importance of this program is by envisioning a world in which this program doesn't exist: imagine that all 24,000 faculty, staff and students must access Blackboard, PeopleSoft and MyNIU and have their accounts and passwords either managed manually by each department or, worse yet, by the individuals themselves. Such a distributed system would require more technical staff to develop, manage and maintain separate, duplicative, and therefore more expensive infrastructure for access management into locally managed applications.

The student experience would be a disaster. Depending on which college a student resides in, their experience gaining access to core enterprise applications would be inconsistent at best. As students progress, perhaps moving from one college to another, the effort needed to manage their access to core applications would be cumbersome, inefficient and simply impossible to manage.

Program Portfolio.

For NIU to maintain and grow its programs in new areas, and to stay relevant with new and innovative technology solutions for teaching and learning, a centralized identity and access management program is essential. New programs and tools can be easily integrated with the existing infrastructure to enable user access in an efficient and streamlined manner. Because the employee/student lifecycle infrastructure already exists within the PeopleSoft Human Resources and Student Administration systems, this program provides services to any technical offering in NIU's program portfolio.

Program Synergy

The central identity and access management system is structured to integrate with all relevant enterprise applications. Future deployment of applications that the business deems critical to NIU's success should be integrated with this program infrastructure.

Criterion 2: Quality / Effectiveness

Functions and Services

This program's core function is to create, manage, verify and eventually remove user IDs and passwords so that NIU's faculty, staff and students can securely and properly access NIU's enterprise applications. This function is absolutely critical to NIU's entire application and network infrastructure and represents a core engine by which so many other programs are enabled to support the mission of the University.

There are planned program enhancements not yet in production. Multi-factor authentication and role-based access to enterprise services are two key security requirements, while expansion of existing infrastructure will provide business continuity capabilities and disaster recovery to protect the enterprise against catastrophe.

Measures of Quality

1. System availability is measured against both planned and unplanned downtime.
2. Number of incidents per enterprise application (including wireless infrastructure) login as determined by analyzing how many of the reported incidents are merely password reset failures or forgotten passwords vs. failures in the underlying authentication infrastructure.
3. Number of applications using locally-created accounts instead of enterprise NIU accounts
4. Number of applications using role-based permissioning.

Evidence of Quality

1. System availability for the Identity Manager is over 99% and includes no unplanned downtime.
2. Enterprise applications and the wireless infrastructure receive more than 150,000 logins each day. Of all the user login incidents reported in September-October, 2015 (3,234), only 7 (0.2%) were caused by the core identity and access management infrastructure. This is a high quality and robust program.
3. DoIT is not tracking this at this time, though a new architecture review process for central and distributed applications will develop this metric in 2016.
4. This type of tracking, the most meaningful of the lot, is still aspirational.

Quality Improvement

DoIT continues to focus on increased automation, infrastructure capacity and reliability, while assessing plans to expand the underlying server infrastructure for identity and access management to ensure robust service for all enterprise apps.

An RFP to explore capabilities and improved price/performance options is tentatively planned for the next fiscal year.

Criterion 3: Productivity / Efficiency

Scope of Program

DoIT performs these core duties to securely and appropriately deploy identity and access management:

- long/short-term planning and management of infrastructure;
- infrastructure enhancements to increase reliability, availability and serviceability;
- automation of account lifecycle provisioning including creation, updates and deletion;
- integration with PeopleSoft Human Resources and Student Administration systems for account lifecycle management;
- integration to provide enterprise-class authentication and authorization of credentials to Blackboard, PeopleSoft, Office365, Gmail and departmental applications like Concur Travel, Terra Dotta for study abroad, eXplorance Blue for advising, and Pinnacle for DoIT billing; and
- maintain hierarchical directory structure to enable delegated management of accounts across the institution.

Productivity Comparison

NIU is a recognized leader in the identity and access management space and expects to soon have a seat on the Board of the Internet2 group that guides this field of technology. DoIT staff are frequently contacted by other universities for guidance and technical expertise and sought after for best practices at vendor conferences around the world. DoIT also maintains membership with the Technology Transfer Partners (TTP), a consortium of higher education institutions focused on a range of high-level technology areas in information technology.

Resource Comparison

DoIT supports the identity infrastructure with 2 engineer FTEs and .25 FTE for user access management requests. Most similarly-sized institutions have at least 5-6 engineers on staff to support their similarly-complex identity and access infrastructure.

Cost and Revenues

This is not a revenue-generating program. The annual program costs are approximately $450,000:

- Micro Focus Identity Manager: $80,000
- Micro Focus upgraded modules: $40,000
- Server/network/storage infrastructure: $20,000
- DoIT staff salaries: ~ $300,000
- Other licensing (SLES/HA): $10,000

Looking at the cost profile over the next three years, servers/storage will remain flat or decline in total cost, but there is a slight upward trend in total costs, driven primarily by annual licensing costs (5% per year) for the Micro Focus infrastructure. Other cost increases could be for additional engineering staff.

Criterion 4: Internal & External Demand

External Demand

Any existing or new externally-facing, or Outreach-oriented, program that leverages NIU's enterprise application infrastructure (i.e. Blackboard, PeopleSoft, Email/Calendaring, etc.) must leverage the Identity and Access

Management infrastructure in order for the services to work in support of externally-facing initiatives. Wherever our Outreach services interact with the community or when contractors or consultants need to gain access to NIU's applications, this program is the means by which to verify credentials.

The Payment Card Industry (PCI) requires NIU to enhance the authentication for people who process credit card payments. Multi-factor authentication will bring NIU into PCI compliance by requiring two forms of credentials/identity in order to successfully authenticate. While NIU will grow its use of multi-factor authentication across the enterprise, PCI requires this infrastructure be implemented immediately. Additionally, compliance with HIPAA (Health Insurance Portability and Accountability Act) also requires implementing new authentication technology and access controls to comply with regulations. Finally, the FERPA (Family Educational Rights & Privacy Act) identity management and access control infrastructure has been in place for over a decade in compliance with federal regulations.

Internal Demand

Overall, the internal demand for this program far exceeds the external demand because of the multitude of enterprise applications (MyNIU, Email, Blackboard, PeopleSoft) that access the identity and access management infrastructure to validate user IDs/passwords and enable access into their respective application environments. So far in 2015, this program has processed more than 43,000 additions or modifications to PS-HR accounts and more than 138,000 additions or modifications to PS-SA accounts.

During each semester, on average, the enterprise infrastructure processes more than 200,000 authentication requests each day, more than 22.4 million requests per semester. Each instance of the request is an actual user (student, faculty, staff) logging into one of NIU's enterprise applications to teach, submit an assignment, do work, and more. The identity and access management infrastructure represents the lifeblood for how users can seamlessly and securely access NIU's enterprise application infrastructure.

Criterion 5: Opportunity Analysis

Cost Savings Opportunities

Most cost savings have already been realized by automating account lifecycle management across the enterprise. DoIT is minimally staffed with 4 FTE in this program and there is no opportunity to further reduce staff that support this critical infrastructure.

There is the potential to save nearly $30,000 by finishing the student migration from a Gmail system to Office 365. More than just saving money on licensing, the support burden is reduced when there is only one system to provision and manage.

Future Revenue / Resources

This is not a revenue-generating program.

Improvement Opportunities

The campus **should** consolidate into a single Active Directory structure, reduce the number of LDAP implementations, and insist on Shibboleth Single Sign-On authentication wherever possible. Additionally, moving to role-based authentication will more effectively manage authorization credentials for students, staff and faculty when logging in to the wireless network or applications.

Opportunities in the Field

Based on the existing skillsets and knowledge within DoIT, we have the expertise to share best practices and knowledge of identity and access management technology both within NIU and with other universities. Internally, DoIT **should** engage distributed IT groups at NIU in order to educate and enable them to more effectively manage their own environments.

NIU **should** implement more finely-grained role-based access to the network, which will allow us better data protection and the ability to segregate managed from unmanaged workstations, grant researchers a more freely-managed Science Zone on the campus network, and place administrators with compliance requirements (HIPAA, PCI, CJIS, etc.) into an administrative network zone that did not require VPN or multi-factor authentication for access. All of this would happen just through a login.

Moreover, if we included these roles in the PeopleSoft HR system, we could automatically provision and remove authorizations into our core applications and reduce the amount of time (currently 1.2 FTE) currently spent on manually approving and provisioning security access to PeopleSoft applications.