The Governance and Policy Focus Group was charged with developing a framework for governance and policy for identity and access management (IAM). Our goal was to provide an overview of structural and organizational issues related to governance and policy for IAM as Penn State moves forward. The work of three of the focus groups – Life Cycle and Affiliation, Vetting and Proofing and Levels of Assurance - will lead to specific policy statements and guidelines as will recommendations from the Risk Assessment focus group.

Boundaries that existed in the past are rapidly disappearing. Students take courses at a variety of educational institutions, researchers collaborate well outside the boundaries of the traditional laboratory, clinicians seek input from peers, and patient’s families expect to maintain a sense of normalcy throughout the care continuum. In today’s world, regardless of modality or geography, people expect to access data seamlessly.

IAM is an evolving discipline involving new concepts and technologies. Dynamic business needs necessitate a flexible and responsive IAM model. Where a Penn State identity serves as the basis to access other’s valued information or resources, partners’ trust that requisite policies and procedure are in place and consistently followed. To be successful, the IAM framework must incorporate standardized principles, prudent and responsible best practices, and a multi-disciplinary governance model that respects the diverse nature of Penn State.

A strong IAM system is dependent upon a sustained commitment to administrative and technical privacy and security controls. A key recommendation of the IAM Governance and Policy Focus Group is the establishment of a governance team to ensure coordination and collaboration amongst existing committees and project teams with overlapping objectives (e.g. Information Privacy and Security and Data Classification). To affect the desired outcome, we recommend the establishment of an authoritative governance structure and the development of comprehensive policies, standards, and procedures.

**Governance:**

Clearly articulating the scope, boundaries, and balance between different roles within IAM is critical to building a successful implementation model. We recommend three levels of governance:

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

2. An office or department responsible for the day-to-day operations related to IAM, following established policies, procedures, and standards. This function logically belongs in Information Technology Services.

3. An individual with a strategic perspective, having the authority to move quickly in resolving issues, interpret IAM policy, and facilitate prudent and responsible requests. As appropriate, this person will bring unanticipated needs to the attention of the IAM advisory group. This individual would also be responsible for assuring that policy is developed at the granular level as required by the decentralized departments needing such guidance and building awareness and education campaigns. To ensure checks and balances, consideration should be given to making the reporting line for this role to another central office other than ITS, however, the focus group members did not reach consensus on this issue. The key consideration is to find an individual who has the authority, passion and interest to take on this important work.
To be effective, all three levels of governance must develop mechanisms for gathering feedback from those working in the area of IAM. Governance of IAM will be most effective if there is two-way communication – dealing with issues and concerns pushed-up by departments and end-users, and pushing down policy and standards which resolve issues and maintain controls, but with flexibility in application, if appropriate, for departments.

**Policy**

In large and diverse communities, establishing centralized, overarching policies and standards is critical to ensure consistency among many decentralized environments and the integrity of the person data. As already outlined, the IAM governance structure will have the authority to establish, interpret and modify policy while allowing decentralized business units to decide the best implementation strategy based on operational considerations.

There is no comprehensive IAM policy at Penn State at the present time. Therefore, a framework for future policy development was developed to support a preliminary assessment of current policy and to solicit feedback from other focus group members (See Appendix GP-1). In most cases, the policies reviewed address a specific aspect of IAM – such as network security, ID Cards, or Access Accounts. The purpose of this analysis was to begin to identify gaps and inconsistencies which need to be addressed. The gap analysis completed is preliminary in nature. If the concept is validated, additional work should be performed by knowledgeable individuals reviewing a broader range of policies and procedures, including those at MSHMC.

It is recommended that a comprehensive overarching policy for IAM be developed. As IAM requirements change, both internally and externally, Penn State must respond through adjustments and updates to its IAM policy, standards and procedures.

The governance structure will need to determine the strength of policy in each area. Decisions as to the development of standards and requirements versus behaviors and best practices versus objectives and goals - must be based on the best assessment of what is required to meet the business needs of the University for both internal and external purposes.

Unlike traditional student/faculty/staff policies, IAM policies encompass a much broader spectrum of responsible parties, not all of whom may have a direct affiliation with Penn State (registration authorities, application providers, guest users, federated relationships, etc). IAM policies must be written with the audience in mind and sanctions need to be relevant to the affiliate. IAM policies will need to incorporate meaningful, progressive sanction language that complies with existing laws and complements existing policy.

IAM governance, policy and procedure must be developed and communicated along with other critical aspects of our digital world, especially privacy and information security awareness and training. We will be successful in this area when we not only have policy and procedure, but educated constituencies that have an understanding of IAM and security issues in the evolving digital world.