Current Problems and Issues:

1. Most units need to go to multiple data sources to obtain information they need; there is a lack of a common data management strategy.

2. Existing business processes involved in a person’s hire and termination makes it difficult for affiliation data to stay accurate. If an employee is terminated, he or she may need to have their access to resources removed promptly. Currently, data feeds do not arrive quickly enough to fully automate access provisioning or de-provisioning campus-wide. This is particularly problematic for jobs that have high employee turn-over. Additionally, no mechanisms exist to inform units of a change in a person’s status (e.g. a job change).

3. Members of the extended University community, including guests, faculty with very short appointments, unofficial class auditors, temporary employees, visitors, volunteers, contractors, external reviewers, recruiters, etc. are problematic with respect to provisioning access. Their presence at the University tends to be short-lived and/or they do not have an official University affiliation. Going through existing “official” channels to provision access for these individuals is very time-consuming and unrealistic.

4. Providing “guest” accounts can be insecure if not implemented responsibly. Shared guest accounts can grant access to another person’s data or eliminate accountability in the case of a resource abuse. A secure, centralized method for creating guest entities does not exist currently.

5. Locally administrated data stores for directory purposes are difficult to support and maintain when the individual(s) who created them are no longer present.

6. Many units still use manual processes to create identities or allocate resources. For example, the School of Nursing creates uniqnames and UMIDs manually for Wayne State Students studying at the University of Michigan. In general, manual processes introduce error and are very time-consuming.

7. Student and staff data do not propagate in real-time. This makes the generation of accurate departmental lists, org charts, class lists, etc. difficult. Additionally, students who have graduated aren’t incorporated into alumni systems (e.g. DAC) within an acceptable amount of time.

8. It is difficult to classify people with multiple affiliations or roles. For example, someone can be a student, staff, and alumnus simultaneously, or a faculty member could have joint appointments in several departments. It is difficult to determine which role or affiliation takes precedence or has administrative “ownership” of an entity.

9. There are no common standards for how objects are named. For example: the University of Michigan Transportation Research Institute appears as UMTRI, “Trans. Res. Inst.,” etc., depending on which data source is examined. Another example is non-canonical names used for buildings. Mosher-Jordan Hall, for example, is referred to as “MoJo” by many. Inconsistencies like the above make it difficult to generate reliable search results.

10. A common identifier across campus does not exist. Some systems use UMID, DAC EID, Social Security Number, etc. The use of Social Security Number as a primary key to the uniqname system is unacceptable and conflicts with University of Michigan Standard Practice Guidelines.

11. UMOD is widely and inaccurately viewed as an authoritative source of person data. However, the actual sources defined as authoritative can be inaccurate as well. For
example, duplicate IDs can emerge, phone numbers and physical addresses can become out-of-date, and so can affiliation data.

12. A user’s ability to modify attributes of their own UMOD entry renders those attributes unusable for administrative purposes. User-updated attributes are often inaccurate and don’t conform to a common format, accepted naming standards, or reality.

13. UMOD allows a group and a user to have the same name, resulting in identity ambiguity.

14. A more generic level of affiliation classification (e.g. faculty, staff, student, alumni, etc.) is needed.

15. It is desirable to track information beyond what currently exists in centralized systems, such as: information about teaching certificates; public keys; user profiles; “areas of interest” for graduate students and researchers; and multiple types of addresses and phone numbers.

16. Access to resources needs to be granted to those who may not be able to present themselves physically for identity verification; password resets currently require a physical presence and cannot be performed securely via e-mail. Many other e-mail providers (such as Yahoo!) have this capability.

17. When uniqnames are chosen automatically, it increases the likelihood that a person won’t like what they have been given. Uniqname changes are time consuming and problematic.

18. Storing user information locally can create data inconsistencies and in many cases causes a duplication of effort. Many departments keep their own copies of data that are less current or accurate than authoritative sources.

19. There are multiple formats for the data used by card-key systems on campus.

20. Students who take unofficial time off or graduate students who are not taking classes can be purged prematurely from existing systems.

21. The current search functionality of UMOD is insufficient. The ability to perform “fuzzy” searches on other criteria, such as phone number, location, or what an entry “sounds like” is absent.

22. Existing authoritative data sources are difficult to use, and it is difficult to gain access to them. The Data Warehouse requires an interactive log-in, so it is difficult to automate many processes.

23. Some data exist in UMOD that units need to override. The “home directory” attribute, for example, exists but can be used only in specific circumstances.

24. No common orientation or training process exists to inform new affiliates how directories can or should be used. It is unclear where information comes from, where it is stored, or how it is updated. No directory services “roadmap” exists.

25. Many users do not know to whom they should go if they find errors in their UMOD entry, nor do they have a clear understanding of why the information is wrong or how it got there in the first place.

26. There is significant unease about which information is stored in directories, what is being done with the information, and who has access to see it. There is also confusion with
respects to the purpose of UMOD. Some alumni users expect it to be a directory of their former classmates, for example.

27. Different UMOD interfaces show different data. For example, the output of “finger” is different than that of the Directory web site.

28. Easier programming hooks and APIs are needed. For example, it is not clear how to integrate Oracle, Kerberos, LDAP, and CoSign.

29. Existing privacy flags are too restrictive; some administrators with legitimate need to see data are hindered from doing so. A greater degree of control over which attributes are visible, and to whom, is needed. Incoming freshmen have been frustrated because they have been unable to find themselves in directory, as FERPA flags have been set initially. Additionally, the protocol necessary for appropriate administrative persons to obtain access to see private data should be simple and well-documented.

30. UMOD lacks a good group structure. There is no way to have group-owned identities or attributes. There is no sufficient way to use UMOD groups for authorization to specific resources.

31. People like their privacy, and don’t want personal information exposed. However some attributes should be visible “no matter what.”

32. Many users do not wish to be added to e-mail groups without their permission.

33. Existing systems do not interoperate well. For example, the relation of DAC to other systems is unclear and MPathways does not incorporate Flint information.

34. Some regulations, such as HIPPA, require regular password changes. These requirements are unenforceable with the existing Active Directory forest.

35. Units will need sufficient time to implement changes.

36. A single point of authorization implies a single point of failure.

37. The current funding model for directory services is unclear.