Issues Identified and Lessons to Learn

Issues Identified and Lessons to Learn

- Accessibility support
    - From device issues to accessing preferences during MFA processes
    - Which MFA approaches are already fully accessible and/or introduce new accessibility concerns? Does one need a combination of MFA technologies/devices/strategies to ensure an accessible option for all users?
    - What about incorporating user display/content presentation preferences into the MFA flow/interface(s)?

- FERPA issues in the release of PII (e.g. cell phone number) to third party authenticator
    - More generally the legal relationship between enterprise and third party authenticators
    - What do we need to ensure NET+ contracts and/or vendor contracts have sufficient language/safeguards/etc. to satisfy registrar/legal council/fall under "school officials"?

- Cloud authenticators and availability
    - DDOS attacks
    - What if/should enterprise authentication fail under external DDOS attack?
    - Generally, identify key barriers to outsourcing components of authentication such as 2nd/additional authentication factors

- Fail-over strategies
    - MFA fails more frequently (does it?), if only for environmental issues
    - “Fallback” approaches for opt-in deployment models?

- ROI of federated MFA
    - The leverage of federation and MFA is enormous, but how do we capture it/measure it/effectively document it?

- What do we (you!) hope to learn in the next 6 months from your involvement in the MFA Cohortium?
    - Possibilities:
        - If we offer MFA as an opt-in option to all users, how many take us up on that?
        - How well does the added Shibboleth Assurance/MFA support work in practice? How easy is it to integrate and deploy?
        - Same question could be asked for CAS and potentially other SSO environments.
        - Answers/guidelines/solutions/active work for all of the above issues?