**DISCUSSION TOPICS**

1. **Usability Items for Discussion:**
	1. Registration Email Message: Feedback was received that there was not sufficient content or context for the email message that a user receives when a new user ID is created. The current text is:

**Hello Michael Q. Commit,**
*Your CommIT Identity has been created.
Your user id is mqc1.*

We need to draft appropriate messaging.

* 1. Registration Date of Birth Parameters: Currently there are no age parameters. It was mentioned that we should restrict CommIT ID’s to those over the age of 13 to avoid touching the Children’s Online Privacy Protection Act (COPPA). This needs to be discussed.
	2. Legal Name Suffix: Currently this is a free-form text field and it was recommended that it be converted to a drop down list with a controlled vocabulary. The CommIT Tech Team is prepared to make this change but needs the list of options. Is anyone aware of a standard list that can be used for this purpose?
	3. Registration Confirmation. The current page has an action button labeled “RETURN” after the user is presented with the “congratulations” message that their registration was successful. Some users found this confusing and recommended a new label. Recommendations from the CommIT Tech Team were “DONE” or “LOGIN”. A decision needs to be made about what to call the action button.
1. **Privacy Policy -  What should our policy look like?

*General Information*:**
* Only the identifier is being shared. This is not Pii but it is tied to Pii in others databases (HEI’s vendors, service providers, etc).
* CommIT is in a more trusted/agnostic role as compared to other entities that may be using data for other purposes.
* The data that CommIT is collecting is only being used for matching purposes.

***Open Questions***:

* Is the CommIT identifier Pii? This will need to be vetted through legal/privacy experts.
* What will be required by Federal agencies?
* Pairwise Identifiers. This is another discussion that we will need to have as we move from pilot to product. Not to be used in the Pilot.
* Do we need an APPROVE/ACCEPT process?

***Concepts for the CommIT Privacy Policy:***

* Our privacy policy can refer to the Terms of Use statement that CommIT will need to have in place with each of the Pilot Participants.
* Keep it simple. Explain to the user WHAT data is being shared and HOW the data being collected will be used, stored and protected.
* Keep it broad.
* Specifically reference the policy’s applicability to the PILOT only. Mention that the policy may/will change for the Product.
* Users need assurance that the data CommIT is collecting is controlled by the user and will not be used for any purpose other than those that are expressly consented to by the User.
* We may share your information with a service provider with your consent.
1. **Terms of Use and/or Service Statement – Do we need one?  What information should it contain?**
2. One for the users
	* Needs to address various user roles
		+ Student
		+ Parent
		+ Will need to consider the further implications when we get to the point of having administrative users from help desks, etc.
	* Boilerplate templates available
		+ Student facing services
		+ Look at the terms of use that any vendors/service providers are using today
			- College board
			- Connect edu
			- Act
			- Etc.
3. One for the participants – HEI’s and Service Providers
	* This will need to be integrated into a contract with terms sheet
4. **Policy for Merging Found Duplicate Records – General preliminary discussion on how this process should work.**

a) User knows they have an account but forgot their user id or password

b) User forgets they have a CommIT account and attempts to re-register

c) ? Are there other flows that need to be considered?

* Flow 1 – User registering and a potential duplicate is found in the CPR
	+ Email address – can we only use email address to identify the duplicate? If an email address has been used, then assume it is the same user and put them through the password reset process.
* Flow 2 – End user merges their own identities
	+ User logs in with one account
	+ User knows they have another CommIT account
		- Can we develop a process for them to merge the two accounts together? (re-authenticate with the 2nd account and then allow the self initiated merge)
		- Should help desk be the only administrator that can do the merge?
		- Ask the schools why having duplicates a big problem? If a student has multiple identifiers that all point to the same individual, does the problem go away? One representation of a person.
1. **Security & Privacy Related Operational Concerns:**
	1. How long will records remain in the CPR? What is the purging process?

		* For the pilot: “When the pilot ends the data is gone?” Not the impression people have been getting. We want continuity of policy, so they should be made “quickly”. 2 years after last login-in? Sliding window based on time since last access. ACRP policy. Does policy for career information deliver systems. PESC affiliate
		* We have to maintain an account for 7 ½ years after it’s deactivated for silver. There’s no upper bound. Our intention is to retain data, we are not “promising” to maintain data.
		* If this is for life-long learning, records can remain “indefinitely”, but we need to look at EU policies, and we will want to have some methods for refreshing the data. So, sliding window (time since last log-in, use ticklers) for refreshing data.
	2. Can you re-use ID’s?
		* Pretty easy no. Can you re-use email addresses? We don’t give the email address out to anyone. But email has to be unique across the system. \
	3. What are our audit requirements? Are we tracking last log-in? Create a field for last log-in? Do we want to add attributes passed? Contents of the attributes? All we intend to pass right now is the identifier. If we ever send more than just the identifier, we should def log what we send. Making audit log available to the end user squelches privacy and security questions? May also create privacy and security issues, reveals where user has been before.
	4. What is CommIT’s process for maintenance of data?  How can the user or others update the information that is contained in the CPR?
		* Data is different from user records. Logs? Transactions? Bigger than user records. Different jurisdictions will have different laws. We need to research government regulations. Anyone with knowledge of these? The right people aren’t in the room. The right people need to be on the calls. We are scoping the pilot to US, but we want to design for international now as possible.
	5. Will credentials be used for other onboarding processes other than the admissions application?  What is the set of service providers we are willing to talk to?
		* If you have signed a participation agreement, you can build a service. Test service, vendor participation, etc. Up to scoping.
	6. What are the US and Global privacy requirements?

**6. Moving Forward – Brainstorming Discussion**

 a. Pilot Phase 2: Assurance, digital notaries, and aggregation of vetting processes

 Several points: We haven’t cracked the spec yet. Have to look at InCommon Silver, comparable to NIST LoA2. Federal approved profile. US DoEd. Ann has a small group of architects looking at the concept of digital notary. What sort of back-end systems? Digital notaries become part of the trust process. Training. Break the spec apart and create a digital notary spec. Developing a white paper to outline these issues. Couple of use cases, testing, guidance counselors. K12 doing proofing based upon prior knowledge. Thinking through issues.

Need to review issues. Needs to be part of the RFP.

Focusing on a more simple version for now.

b. Product Phase 1: RFP for production and hosting of services, including help desk. Not going to be silver. We need to build the infrastructure and the people. The good thing about the identity proofing is that there are a lot of people interested.

Action Item: Make the participation model more clear. Needs to be a “My Account” tab.

Future Governance State: This has been implicit and should be made explicit.

Envision a committee like the steering committee. Executive representatives from vendor and higher ed organizations. A chair should be elected for some period (2 years?). The group should have a mission and a charter. Should grow out of work we do on the business model. This should be in place by the time we go into production.