MEMORANDUM OF UNDERSTANDING

This Memorandum of Understanding (this "MOU") is made as of _____ __, 2013 (the "Effective Date") by and between the University Corporation for Advanced Internet Development, Inc. d/b/a Internet2, a District of Columbia nonprofit corporation ("Internet2"), P20W Education Standards Council, a [_____] nonprofit corporation ("PESC"), and _____, a _____ _____ (the "Participant"). Internet2, PESC, and the Participant shall hereinafter be referred to individually as a "Party" and collectively as the "Parties." For the purposes of Section 3 below, the Participant shall be a [University/Organizational] Participant.

1. BACKGROUND

(a) In April 2011, the Electronic Authentication/Authorization (EA2) Task Force of the PESC discussed how organizations could leverage existing identity verifications during the college admissions process. It became clear that aggregating these events could significantly increase the validation of a college applicant's identity. Two major benefits were discussed: simplifying the matching process of electronic records to college student applicants combined with the creation of a unique electronic credential that will radically streamline and make the entire application process easier for students, parents, colleges and universities and the myriad number of external service providers and stakeholders involved in the process.

(b) Since PESC's interest in authentication and authorization overlapped with the work of Internet2, the recognized leader in higher education for authentication, PESC engaged Internet2 in discussion to propose formation of a closer relationship. Subsequently, PESC and Internet2 engaged in a strategic alliance whose first deliverables include the development of a task force and project known as the Common Identity and Trust Collaborative ("CommIT"). For purposes of clarification, "CommIT" refers to the joint efforts of PESC and Internet2, and is not a separate legal entity. As used herein, actions taken or to be taken by CommIT are intended to be taken by PESC, Internet2 and/or another person to be agreed upon by PESC and Internet2, the details of which are to be determined in a future definitive agreement.

(c) CommIT is now working on "Project Phase One," which is a one-year project including several universities and vendor participants to demonstrate on a small scale what CommIT might bring to education, with the end goal of moving to a larger product release.

(d) The Project Summary and Overview set forth on Exhibit A are hereby incorporated into this Section 1.

2. PURPOSE OF MOU

(a) The purpose of this MOU is to develop a framework for exploring opportunities to support the Parties' mutual interests through, among other things, and as described in greater detail in Section 3 below, to support and enhance identity and trust as foundational services for the higher education admissions process through the creation of an identity store, a unique student identifier, an identity provider, and an ecosystem for "Digital Notaries," thereby permitting only applicants themselves to initiate electronic records aggregation and release.

(b) Notwithstanding anything in this MOU to the contrary, no Party shall have any legally binding obligation to any other Party as a result of the execution of this MOU, or otherwise relating to this MOU or the subject matter hereof, other than with respect to the Confidentiality section of this MOU (Section 6). Although the Parties will try to reach one or more future agreements as to the matters described in Section 3 below, this MOU shall not require the Parties to reach any future agreement, and, notwithstanding anything in this Agreement to the contrary (including Section 10 below), no Party shall have any liability to any other Party as a result of the Parties' failure to reach one or more future agreements.

(c) If the Parties reach any future definitive agreement, the agreement must contain terms that identify the following with respect to the project the Parties will jointly undertake:

(i) the nature, scope, timeline and location for the project;

(ii) the estimated budget; and

(iii) each Party's scope of obligations and duties, including with respect to the manpower and resources required.

3. SCOPE OF COLLABORATION

The Parties will explore opportunities to collaborate with each other regarding some or all of the following:

- A technical infrastructure that can support the Participant (as well as other participants in the CommIT Project Phase One), including:
    - A scalable person registry with all the mechanisms for adding applicants, setting and resetting passwords, and all the expected functionality.
    - A scalable identity store.
    - A scalable Shibboleth Identity Provider
    - A web based user interface
    - Documentation
- A Project level unified and automated helpdesk solution
- A request for proposals to transition the CommIT project into Phase Two:

- A business plan
- A governance plan
- A technical plan
- The helpdesk model

Set forth on Exhibit B hereto is a list of Class A Services and Class B Services (each as defined therein) with respect to the University Participants and Organizational Participants. If any point prior to the execution of a definitive agreement it becomes clear that the Participant will be unable or unwilling to perform any of the Class A Services set forth on Exhibit B under "University Participants" or "Organizational Participants," as the case may be, then, upon mutual agreement between the Internet2 and PESC liaison persons, the Participant shall be removed from Project Phase One upon thirty (30) days written notice to all the Parties. Upon execution of this MOU, the Participant shall provide written notice to the Internet2 and PESC liaison persons of the Class B Services it intends to provide, if any.

4. LIAISON PERSONS

Any approvals, notices, and other communications between the Parties under this MOU shall be sent to the applicable Party liaison person as follows:

Internet2:	[Contact Name] University Corporation for Advanced Internet Development [Address] [Email address] [Phone No.]
PESC:	[Contact Name] P20W Education Standards Council [Address] [Email address] [Phone No.]
Participant:	[Contact Name] [Participant] [Address] [Email address] [Phone No.]

Each Party may replace its liaison person at any time(s) by providing notice to the other Parties' liaison persons of such change. The Parties' liaison persons shall jointly conduct monthly reviews to ensure efficacy of joint activities hereunder.

5. TERM

This MOU commences as of the Effective Date and shall continue until terminated by any Party at any time and for any reason upon thirty (30) days written notice to all of the other Parties without liability for such termination.

6. CONFIDENTIALITY

(a) Except to the extent otherwise required by applicable law, without the disclosing Party's (the "Disclosing Party") prior written consent, no Party may (i) use for any purpose other than to perform hereunder, or (ii) disclose to any third party, other than the Party's directors, officers, employees, and agents (collectively, "Representatives") solely in connection with the Party's performance under this MOU, Confidential Information of such Disclosing Party. "Confidential Information" shall mean any information, documents or materials that relate to or include past, present or future products, software, research development, inventions, processes, techniques, designs or technical information and data, marketing plans, financial statements, pro forma financial statements, customer lists, or other proprietary information relating to the business affairs and operations of the Disclosing Party. Each Party shall be responsible for ensuring that its Representatives agree to comply with, and do comply with, the confidentiality obligations set forth in this Section 6. Upon expiration or earlier termination of this MOU or upon the Disclosing Party's request, each Party receiving Confidential Information (a "Receiving Party") shall return to the Disclosing Party all physical and electronic copies of Confidential Information of such Disclosing Party in such Receiving Party's possession or control, or, at the Disclosing Party's election, destroy all such copies and provide to the Disclosing Party a certificate of such destruction. For the avoidance of doubt, the existence of this MOU is not confidential.

(b) The confidentiality obligations in Section 6(a) above do not apply with respect to any information, documents or materials that a Receiving Party can document (i) are or (through no improper action or inaction by such Receiving Party or its Representatives) become generally available or known to the public, (ii) were rightfully in its possession or known by it prior to receipt from the Disclosing Party, (iii) were rightfully disclosed to it by a third party having no obligation of confidentiality, (iv) were independently developed without use of or derivation from any of the Disclosing Party's Confidential Information, or (v) are approved for public disclosure and release by written authorization of the Disclosing Party. A Receiving Party also may make disclosures of the Disclosing Party's Confidential Information to the limited extent required by court order, or other government demand that has the force of law, or as otherwise required by applicable law, provided such Receiving Party has, if permitted by applicable law, prior to any such disclosure, promptly notified the Disclosing Party of the court order, government demand or applicable law, and has allowed the Disclosing Party to participate in the matter (including participating by seeking to limit disclosure or obtain a protective order to the extent permitted by applicable law).

7. USE OF NAMES

No Party may use in its external advertising, marketing programs, or promotional efforts any name, insignia, trademarks, pictures or other representation of another Party in connection with, relating to or arising out of this MOU without such other Party's prior written permission.

8. NO FINANCIAL OBLIGATION

Unless the Parties mutually agree otherwise in writing, each Party will be responsible for its own costs, fees and expenses (including all costs, fees and expenses of its agents and representatives) incurred in connection with the activities contemplated by this MOU. This MOU does not, however, create an obligation on the part of any Party to expend any certain amount of funds in furtherance of this MOU or the activities described herein.

9. RELATIONSHIP BETWEEN PARTIES

Nothing herein shall be construed to create a partnership, agency, or joint venture between the Parties. No Party will hold itself out as being part of, controlled by, or acting on behalf of the other Parties. The Parties agree to inform third parties that no Party is part of any other Party.

10. LIABILITY

Each Party will be responsible for the acts, omissions and negligence of its own officers, employees, and agents acting within the scope of their respective authority. Nothing in this MOU is or shall be deemed to be a waiver by any Party of any defenses that may be available by law. In addition, without limiting the scope of Section 2(b) above, but in addition thereto, to the extent permitted by applicable law, no Party nor its Representatives will be liable to any person or entity, including any other Party, for any direct, indirect, consequential, exemplary, punitive, special, or incidental damages, or damages for lost profits, revenues, or business interruption, arising under or in connection with this MOU or the performance thereunder, even if advised of the possibility of such damages or if such possibility was reasonably foreseeable, except that a Party may be liable to another Party for direct damages only (i.e., not for indirect, consequential, exemplary, punitive, special, or incidental damages, or damages for lost profits, revenues, or business interruption) with respect to a breach of Section 6 above.

11. ASSIGNMENT

No Party has the right to assign this MOU or any of its responsibilities hereunder without the other Parties' prior written consent.

12. WAIVER

The failure of any Party to enforce any term hereof shall not be deemed a waiver of any rights contained herein.

13. INVALID PROVISION

If any provision of this MOU is determined to be invalid or unenforceable under any controlling law, the invalidity or unenforceability of that provision shall not affect the validity or enforceability of the remaining provisions of this MOU.

14. MODIFICATIONS

The Parties may modify this MOU only by mutual written agreement.

[Signature Page Follows]

IN WITNESS WHEREOF, the Parties have executed this MOU as of the Effective Date.

UNIVERSITY CORPORATION FOR ADVANCED INTERNET DEVELOPMENT

By: _____
Name:
Title:

P20W EDUCATION STANDARDS COUNCIL

By: _____
Name:
Title:

[PARTICIPANT]

By: _____
Name:
Title:

Exhibit A

PROJECT SUMMARY AND OVERVIEW

Background and Goals

The US higher education admissions process involves over 20 million students each year, interacting with 4,400 degree-granting colleges and universities, 24,000 K-12 secondary schools, dozens of service entities such as testing services, admissions handlers, transcript handlers, and advisory services. All of these stakeholders offer online services to applicants using a disparate network of backend, data-exchanging relationships. As a consequence these current systems provide a poor end-user experience, poor level of identity assurance, and cumbersome data flows that emulate paper-based processes at best. Each organization duplicates services that are needed for security and communication, but are not core to its mission, leaving prospective students to manage an array of accounts, forms, and information flows.

Federated Authentication, an approach to reducing credential duplication and increasing privacy, has experienced significant pockets of adoption across the higher education and research sectors globally, including deployments with U.S. Federal and corporate service partners. For instance, 5.9 million individuals, mostly students, have access to over 700 InCommon federated services. However, large-scale linkages are needed at broader and earlier points of entry for individuals. In particular, the millions of students applying annually to college need fewer temporary credentials, higher identity assurance for the credentials they do have, and an easier process that provides user control of their transactional attributes across a wider gamut of relying parties.

Problem Statement

Technology can help solve several of the biggest challenges we face related to the electronic process for the higher education admissions. The key to creating a smooth, reliable, and easily implemented experience begins with a quality electronic authentication solution.

Contrast that vision with today's reality: applicants establish separate accounts, and therefore potentially different passwords, for every service they consume and at nearly every institution to which they apply, but are rarely expected to prove their identity until after they have been accepted. Simultaneously, stakeholders incur significant costs in provisioning and support without reaping the rewards of identity assurance and are ultimately left with the costly challenge of accurately matching records to applicants. Security practices are inconsistent, and at times duplicative, thereby increasing the risk of privacy concerns and making it difficult to broadly enhance such security practices.

CommIT believes that social networking, by itself, is not a viable solution to this identity as it may raise privacy concerns, but should be considered as a potential entry into the system, or as a linking opportunity in the future.

Mission Statement

The mission of the CommIT project is to streamline the higher education admissions process by developing and expanding identity and trust services.

Vision Statement

To transform the higher education admissions process by creating smooth, reliable, and easily implemented electronic authentication that solves the challenges inherent in the current process.

The CommIT Project

The initial goal of the CommIT project is to support and enhance identity and trust as foundational services for higher education by addressing the challenges of the higher education admissions process. Through the creation of an identity store, a unique student identifier, an identity provider, and an ecosystem for "Digital Notaries", the goal of CommIT is to bring identity verification and trust into the marketplace, and, when combined with corresponding policies and technologies, to protect user control and privacy. With CommIT, only the applicants themselves will initiate record aggregation and release, which enhances security and privacy by preventing third party access without student authorization. The initial goal may change from time to time as the project is explored, developed, and tested, and the information contained herein is intended for general purposes only.

As currently contemplated, CommIT will provide a person registry to store the minimum data required (and only the minimum data) to support user uniqueness and password resets. In essence, CommIT believes it can provide an enabling service for some identity management and is not a central student/applicant data repository.

Single sign-on (SSO) is a technology that provides users with a single set of credentials that can be used across various services because the services are in a trust relationship. Alone, SSO implementation for the application process would represent a significant advancement for all involved; however combined with the voluntary assignment of a unique identifier and vetting events already being performed, the validation of that applicant's identity is significantly increased. The CommIT project strives to provide a scalable secure approach to matching electronic records for all college applicants and institutions and the creation of a unique electronic credential to:

- resolve matching problems at the university level,
- simplify the entire application process for students, parents, colleges and universities, and their external service providers, and
- do away with the last remaining vestiges of dependency on the social security number.

Service Descriptions

As currently contemplated, the CommIT project is to be accomplished in two phases:

1 Phase One: CommIT will support the creation and management of student accounts and the assignment of a unique identifier.

   a Research and Exploration of the CommIT Project

   b Pilot Implementation, upon execution of a definitive agreement

   c Project Development and Rollout

2 Phase Two: CommIT will provide mechanisms for improving the quality of credentials through vetting by digital notaries.

   a Discussion, Research, and Exploration regarding the CommIT Product

   b Issue requests for proposals for CommIT Product development

   c Pilot Implementation, upon execution of a definitive agreement

   d Product Development and Rollout

Fundamentally, the difference between Phase One and Two relates to assurance. The difference between the projects and the products are scope of deployment: the projects will be limited scope pilots and the products will be generally available on a larger scale. This MOU is intended to set forth the framework for exploring opportunities to accomplish the goals of CommIT. Prior to any implementation of the contemplated pilot CommIT project, those participants wishing to be included in the pilot CommIT project would enter into a definitive agreement, which will set forth the respective rights and responsibilities of each participant and the terms and conditions of the CommIT project, including, but not limited to, ownership of work, indemnification and liability, privacy and data security and protection.

If the participants enter into a definitive agreement, CommIT may proceed to the pilot portion of Phase One. Because Phase One will only use a limited pool of schools, it is intended that prospective students will reach CommIT through a referral from one of the University Participants participating in the pilot when the prospective student first visits the school's web presence to begin the admissions process. This would allow our Organizational Participants to know which applicants to connect to the CommIT identifiers. Any application processes not fitting this model will be addressed within the pilot. Later, applicants will create an account directly through a CommIT web portal, or through a referral from one of CommIT's Organizational Participants. This will typically be done when an applicant first applies to take an entrance exam, or when an applicant is referred by their high school guidance counselor. Once a student has their CommIT credential, this will become their single sign-on access to all CommIT Organizational Participants. Organizational Participants will perform an account linking action the first time an applicant visits their site and uses their CommIT credential, allowing each Organizational Participant to hold student data that is relevant to that Organizational Participant.

More details on the use Cases for user onboarding and account management supported in the First Production Stage are Integration Strategy 1 and Integration Strategy 2. These flows enable

the services discussed in this document. The difference between the two strategies is the starting point for account creation.

As currently contemplated, CommIT supports federated authentication and related identity management services through the CommIT Identity Provider, which will be part of the InCommon Federation. Organizational Participants will no longer need to support authentication service for CommIT accounts. For participants who wish to maintain local credentials, mechanism to enable optional account linking from CommIT accounts to local accounts would be in place.

A key component of student onboarding to CommIT is the assignment of a unique identifier to each student. The unique student identifier would be available for use by CommIT participants in their own services.

It is intended that the CommIT project will offer a unified help desk to provide primary end-user support for applicants. Issue resolution will be coordinated with the University Participants and Organizational Participants.

Further, CommIT, together with the University Participants and Organizational Participants, is dedicated to providing single sign-on, user and records matching, and assurance for voluntary participant students applying to higher educational institutions. In furtherance of this, the goal of CommIT and the University Participants and Organizational Participants is to obviate the need for using a student's social security number as the primary identifier in education, promote privacy, and eventually be used on an international basis.

The CommIT project is limited to applicant-initiated processes and cannot be used to aggregate data about an applicant without the applicant's knowledge and active participation. CommIT is not mandatory and applicants must have alternate paths to accomplish the things that CommIT facilitates. While the CommIT project facilitates data aggregation regarding an applicant to ease his or her entry into advanced education, CommIT does not itself offer aggregation tools or services.

Moving beyond project Phase One will include much of the vendor community of PESC, as well as a larger cross-section of educational institutions as a widely available product. It is intended that Phase Two will begin with another limited access pilot, and will include raising the level of assurance to the InCommon Silver standard.

Business Model

The initial concept and design grew from nearly two years of voluntary work by PESC members with active support from InCommon. Subject to the terms of the definitive agreement that will be executed by the parties, Internet2 will be funding the creation of certain infrastructure that will be used in connection with the Project. Additionally, the governance plan is part of the Project deliverables. As Internet2 currently intends to fund certain infrastructure, University Participants and Organizational Participants are expected to fund the work necessary to connect their services to such infrastructure provided by Internet2.

The CommIT project is designed to enhance, not modify, participants' business models. It is believed that every participant has an opportunity to save money by participating in the CommIT project once it becomes a product. While the product business plan still needs to be developed, it is currently assumed that participants will be charged a minimal fee to connect to the infrastructure as the goal will be a self-sustaining, non-profit infrastructure. It is also anticipated that there will be opportunities for organizations to earn revenue for providing assurance for credentials.

Exhibit B

SCOPE OF COLLABORATION

UNIVERSITY PARTICIPANTS

Class A Services

- Through the admissions office, the University Participant will provide a process for prospective students to have the option to create and utilize the CommIT process
- The University Participant will utilize the unique CommIT identifier to match applicants with records provided through their admissions applications tools.
- The University Participant will allow any applicant who possesses a CommIT identity to use their credentials to authorize access to online applications.
- Representatives from the University Participant will be encouraged to share their experiences and lessons learned at various conferences.
- Commit at least one admissions office to using CommIT for a one-year pilot.
    - Provide appropriate redirects to send applicants to CommIT to perform the voluntary applicant onboarding process.
    - When provided, leverage the unique CommIT identifier to match an applicant with some records via their admissions applications tools.
    - Use CommIT credentials to authorize access to online applications.
    - Provision applicants to access marketing related content specifically targeted to known applicants without the generation of university credentials.
- Assign appropriate university resources to coordinate with the CommIT technical team and their chosen vendor(s) or organization(s) to make all modifications necessary to accommodate the change, including changes to the web presence, adapt to accept SAML authentication if not already done, and any alterations to the admissions flow that may need to be accomplished.
- Sign a definitive agreement outlining the details of such University Participant's deliverables.

Class B Services

- At acceptance, leverage the CommIT login credentials to:
    - Obtain access to University Pariticpants' systems directly, or
    - Link and share assurance information from the University Participants' credentials to the CommIT project's credentials.

ORGANIZATIONAL PARTICIPANTS

Class A Services

- Accept the CommIT credential from applicants who login with them.
- Support the storing of such unique identifier.
- Support the capability to attach the unique identifier to all applicant documents that are passed to CommIT participating institutions.
- Register students who come from participating schools within such Organizational Participant's systems, and attach the CommIT unique identifier to the records of students who will be applying to a participating school.
- Provide a mechanism to transport this unique identifier to the records as they are transmitted to the participating schools.
- Provide a mechanism by which the unique identifier will be ignored by non-participating school's systems.
- Provide technical resources to work with participating schools to accommodate all the workflow, user interface, and background technical requirements to adapt such Organizational Participant's system to support these activities.
- Sign a definitive agreement outlining the details of such Organizational Participant's deliverables.

Class B Services

- Leverage the CommIT applicant login credentials to allow authorization to some or all of such Organizational Participant's systems.
- Provide appropriate redirects to send applicants to CommIT to perform onboarding.