Default Question Block

InCommon Assurance Advisory Committee

InCommon Bronze and Silver IAP 1.2 Gaps Survey

Please indicate for each Silver and Silver/Bronze IAP item whether you believe the item is ready for audit, i.e. whether your believe it would or would not pass an audit. If the item is not ready for audit, please indicate the reasons why.

For Bronze only IAP items, please indicate whether you are compliant. If you are not willing to attest to compliance, please indicate the reasons why.

Thank you for your participation.

Institution and contact information (optional):

Your Name:

Your email address:

The institution you represent:

Are all Silver and Silver/Bronze IAP items ready for audit? ("Yes" will record your response and end the survey)

- ○ Yes
- ○ No

4.2.1.1 (S) (B) INCOMMON PARTICIPANT
The IdPO must be an InCommon Participant in good standing in order to be considered for certification under this IAP. In this context, “good standing” means not in arrears with respect to financial obligations to InCommon nor out of compliance with other
contractual obligations to InCommon.

- ○ This item is ready for audit.
- ○ This item is NOT ready for audit.

4.2.1.1 (S) (B) INCOMMON PARTICIPANTThe IdPO must be an InCommon Participant in good standing in order to be considered for certification under this IAP. In this context, “good standing” means not in arrearswith respect to financial obligations to InCommon nor out of compliance with othercontractual obligations to InCommon.

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Other/Additional Information

4.2.1.2 (S) (B) NOTIFICATION TO INCOMMON
The IdP Operator must notify InCommon of any circumstance that may affect the status of its compliance with this IAP.

1. The IdP Operator must notify InCommon of any significant changes to its operation that may affect the status of its compliance and hence its qualification under this IAP. Notification should occur no less than 30 days before the changes are to be made effective, or as soon as practicable after an unanticipated change is noted.
2. The IdPO must report to InCommon any breach of security or integrity of its IdMS Operations that may affect the status of its compliance and hence its qualification under this IAP. A report must be made as soon as practicable after any such incident is noted.

◯ This item is ready for audit.

◯ This item is NOT ready for audit.

4.2.1.2 (S) (B) NOTIFICATION TO INCOMMON
The IdP Operator must notify InCommon of any circumstance that may affect the status of its compliance with this IAP.

1. The IdP Operator must notify InCommon of any significant changes to its operation that may affect the status of its compliance and hence its qualification under this IAP. Notification should occur no less than 30 days before the changes are to be made effective, or as soon as practicable after an unanticipated change is noted.
2. The IdPO must report to InCommon any breach of security or integrity of its IdMS Operations that may affect the status of its compliance and hence its qualification under this IAP. A report must be made as soon as practicable after any such incident is noted.

Why is this item not ready for audit (check all that apply)?

☐ Insufficient documentation
☐ Working/Waiting on a change to University policy
☐ Working/Waiting on the identification/acquisition of a technical solution
☐ Working/Waiting on a change to non-technical processes
☐ Working/Waiting on the implementation of a technical solution
☐ Other/Additional Information

4.2.1.3 (S) (B) CONTINUING COMPLIANCE
After initial certification by InCommon, IdP Operators must declare to InCommon continued compliance with profiles under this IAP at least every 3 years.

◯ This item is ready for audit.

◯ This item is NOT ready for audit.

4.2.1.3 (S) (B) CONTINUING COMPLIANCE
After initial certification by InCommon, IdP Operators must declare to InCommon continued compliance with profiles under this IAP at least every 3 years.

Why is this item not ready for audit (check all that apply)?

☐ Insufficient documentation
☐ Working/Waiting on a change to University policy
☐ Working/Waiting on the identification/acquisition of a technical solution
☐ Working/Waiting on a change to non-technical processes

☐ Working/Waiting on the implementation of a technical solution

☐ Other/Additional Information

4.2.1.4 (S) (B) IDPO RISK MANAGEMENT
The IdPO's Information Technology operations must align with the organization's risk management objectives as demonstrated by a periodic review process or other equivalent control.

○ This item is ready for audit.

○ This item is NOT ready for audit.

4.2.1.4 (S) (B) IDPO RISK MANAGEMENT
The IdPO's Information Technology operations must align with the organization's risk management objectives as demonstrated by a periodic review process or other equivalent control.

Why is this item not ready for audit (check all that apply)?

☐ Insufficient documentation

☐ Working/Waiting on a change to University policy

☐ Working/Waiting on the identification/acquisition of a technical solution

☐ Working/Waiting on a change to non-technical processes

☐ Working/Waiting on the implementation of a technical solution

☐ Other/Additional Information

4.2.2.1 (S) RA AUTHENTICATION
Each RA must authenticate to the IdMS using a credential that meets or exceeds Silver requirements. Communications between an RA and the IdMS shall be encrypted using an industry standard protocol that also authenticates the IdMS platform.

○ This item is ready for audit.

○ This item is NOT ready for audit.

4.2.2.1 (S) RA AUTHENTICATION
Each RA must authenticate to the IdMS using a credential that meets or exceeds Silver requirements. Communications between an RA and the IdMS shall be encrypted using an industry standard protocol that also authenticates the IdMS platform.

Why is this item not ready for audit (check all that apply)?

☐ Insufficient documentation

☐ Working/Waiting on a change to University policy

☐ Working/Waiting on the identification/acquisition of a technical solution

☐ Working/Waiting on a change to non-technical processes

☐ Working/Waiting on the implementation of a technical solution

☐ Other/Additional Information

4.2.2.2 (S) IDENTITY VERIFICATION PROCESS

1. The identity proofing and registration process shall be performed according to written policy or practice statements that specify the particular steps taken by IdPO staff or systems to verify identities.
2. The above statement(s) shall address the primary objectives of registration and identity proofing, including:
    1. Ensuring a person with the claimed identity information does exist, and that the identity information is sufficient to uniquely identify a single person within the IdPO's range of foreseeable potential Subjects;
    2. Ensuring that the physical person requesting registration is entitled to the claimed identity.
3. Personally identifiable information collected as part of the registration process must be protected from unauthorized disclosure or modification.

◯ This item is ready for audit.

◯ This item is NOT ready for audit.

4.2.2.2 (S) IDENTITY VERIFICATION PROCESS

1. The identity proofing and registration process shall be performed according to written policy or practice statements that specify the particular steps taken by IdPO staff or systems to verify identities.
2. The above statement(s) shall address the primary objectives of registration and identity proofing, including:
    1. Ensuring a person with the claimed identity information does exist, and that the identity information is sufficient to uniquely identify a single person within the IdPO's range of foreseeable potential Subjects;
    2. Ensuring that the physical person requesting registration is entitled to the claimed identity.
3. Personally identifiable information collected as part of the registration process must be protected from unauthorized disclosure or modification.

Why is this item not ready for audit (check all that apply)?

☐ Insufficient documentation

☐ Working/Waiting on the identification/acquisition of a technical solution

☐ Working/Waiting on the implementation of a technical solution

☐ Working/Waiting on a change to University policy

☐ Working/Waiting on a change to non-technical processes

☐ Other/Additional Information

4.2.2.3 (S) REGISTRATION RECORDS

1. A record of the facts of registration shall be maintained by the IdPO.
2. The record of the facts of registration shall include:
    1. Identity proofing document types and issuers;
    2. Full name as shown on the documents;
    3. Date of birth;
    4. Current Address of Record.
3. Records also must include revocation or termination of registration.

◯ This item is ready for audit.

◯ This item is NOT ready for audit.

4.2.2.3 (S) REGISTRATION RECORDS

1. A record of the facts of registration shall be maintained by the IdPO.

2. The record of the facts of registration shall include:
    1. Identity proofing document types and issuers;
    2. Full name as shown on the documents;
    3. Date of birth;
    4. Current Address of Record.
3. Records also must include revocation or termination of registration.

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Other/Additional Information

4.2.2.4 (S) IDENTITY PROOFING
Prior to this process, the Subject supplies his or her full name, date of birth, and an Address of Record to be used for communication with the Subject, and may, subject to the policy of the IdPO, also supply other identifying information. For each Subject, the full name, date of birth and Address of Record must be verified using one or more of the following methods: [4.2.2.4.1 Existing relationship, 4.2.2.4.2 In-Person proofing, 4.2.2.4.3 Remote proofing, see IAP document for details].

- ○ This item is ready for audit.
- ○ This item is NOT ready for audit.

4.2.2.4 (S) IDENTITY PROOFING
Prior to this process, the Subject supplies his or her full name, date of birth, and an Address of Record to be used for communication with the Subject, and may, subject to the policy of the IdPO, also supply other identifying information. For each Subject, the full name, date of birth and Address of Record must be verified using one or more of the following methods: [4.2.2.4.1 Existing relationship, 4.2.2.4.2 In-Person proofing, 4.2.2.4.3 Remote proofing, see IAP document for details].

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Other/Additional Information

4.2.2.5 (S) ADDRESS OF RECORD CONFIRMATION
The Address of Record must be confirmed before the Subject's record can be considered to meet the requirements of this IAP. If the Address of Record was not confirmed as part of Identity proofing, then it must be accomplished by one of the following methods:

1. The RA contacts the Subject at the Address of Record and receives a reply from the Subject; or
2. The RA issues Credentials in a manner that confirms the Address of Record supplied by the Subject.
    1. For a physical Address of Record, the RA requires the Subject to enter online a temporary Secret from a notice mailed to the Subject's Address of Record.
    2. For an electronic Address of Record, the RA confirms the ability of the Subject to receive telephone communications at a telephone number or e-mail at an e-mail address.

Any Secret not sent over a Protected Channel shall be invalidated upon first use.

◯ This item is ready for audit.

◯ This item is NOT ready for audit.

4.2.2.5 (S) ADDRESS OF RECORD CONFIRMATION
The Address of Record must be confirmed before the Subject's record can be considered to meet the requirements of this IAP. If the Address of Record was not confirmed as part of Identity proofing, then it must be accomplished by one of the following methods:

1. The RA contacts the Subject at the Address of Record and receives a reply from the Subject; or
2. The RA issues Credentials in a manner that confirms the Address of Record supplied by the Subject.
    1. For a physical Address of Record, the RA requires the Subject to enter online a temporary Secret from a notice mailed to the Subject's Address of Record.
    2. For an electronic Address of Record, the RA confirms the ability of the Subject to receive telephone communications at a telephone number or e-mail at an e-mail address.

Any Secret not sent over a Protected Channel shall be invalidated upon first use.

Why is this item not ready for audit (check all that apply)?

☐ Insufficient documentation

☐ Working/Waiting on the identification/acquisition of a technical solution

☐ Working/Waiting on the implementation of a technical solution

☐ Working/Waiting on a change to University policy

☐ Working/Waiting on a change to non-technical processes

☐ Other/Additional Information

4.2.3.1 (S) (B) CREDENTIAL UNIQUE IDENTIFIER

1. Each Credential issued by the IdPO shall include a unique identifier (e.g., userID, Distinguished Name, serial number) that distinguishes it from all other Credentials in use by the IdPO.
2. A Subject can have more than one Credential unique identifier, but a given Credential unique identifier must map to at most one Subject.
3. The IdPO shall clearly associate the Credential unique identifier to the Subject's registration record in the IdMS, for use by the Verifier or other parties.

◯ This item is ready for audit.

◯ This item is NOT ready for audit.

4.2.3.1 (S) (B) CREDENTIAL UNIQUE IDENTIFIER

1. Each Credential issued by the IdPO shall include a unique identifier (e.g., userID, Distinguished Name, serial number) that distinguishes it from all other Credentials in use by the IdPO.
2. A Subject can have more than one Credential unique identifier, but a given Credential unique identifier must map to at most one Subject.

3. The IdPO shall clearly associate the Credential unique identifier to the Subject's registration record in the IdMS, for use by the Verifier or other parties.

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Other/Additional Information

4.2.3.2 (B) BASIC RESISTANCE TO GUESSING AUTHENTICATION SECRET
The Authentication Secret and the controls used to limit online guessing attacks shall ensure that an attack targeted against a given Subject's Authentication Secret shall have a probability of success of less than 2-10 (1 chance in 1,024) over the life of the
Authentication Secret. This requires that an Authentication Secret be of sufficient complexity and, in most cases, that the number of invalid attempts to enter an Authentication Secret for a Subject be limited. Refer to NIST Special Publication 800-63-1 [SP 800-63], Appendix A, for a discussion of Authentication Secret complexity and resistance to online guessing.

- ◯ This item is Bronze compliant.
- ◯ This item is NOT Bronze compliant.

4.2.3.2 (B) BASIC RESISTANCE TO GUESSING AUTHENTICATION SECRET
The Authentication Secret and the controls used to limit online guessing attacks shall ensure that an attack targeted against a given Subject's Authentication Secret shall have a probability of success of less than 2-10 (1 chance in 1,024) over the life of the
Authentication Secret. This requires that an Authentication Secret be of sufficient complexity and, in most cases, that the number of invalid attempts to enter an Authentication Secret for a Subject be limited. Refer to NIST Special Publication 800-63-1 [SP 800-63], Appendix A, for a discussion of Authentication Secret complexity and resistance to online guessing.

Why is this item not Bronze compliant (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Other/Additional Information

4.2.3.3 (S) STRONG RESISTANCE TO GUESSING AUTHENTICATION SECRET

1. The Authentication Secret and the controls used to limit online guessing attacks shall ensure that an attack targeted against a given Subject's Authentication Secret shall have a probability of success of less than 2-14 (1 chance in 16,384) over the life of the Authentication Secret. This requires that an Authentication Secret be of sufficient complexity and that the number of invalid attempts to enter an Authentication Secret for a Subject be limited.
2. The Authentication Secret shall have at least 10 bits of min-entropy to protect against an untargeted attack.

Refer to NIST Special Publication 800-63-1 [SP 800-63], Appendix A, for a discussion of Authentication Secret complexity and resistance to online guessing and how to calculate min-entropy.

- ◯ This item is ready for audit.
- ◯ This item is NOT ready for audit.

4.2.3.3 (S) STRONG RESISTANCE TO GUESSING AUTHENTICATION SECRET

1. The Authentication Secret and the controls used to limit online guessing attacks shall ensure that an attack targeted against a given Subject's Authentication Secret shall have a probability of success of less than 2-14 (1 chance in 16,384) over the life of the Authentication Secret. This requires that an Authentication Secret be of sufficient complexity and that the number of invalid attempts to enter an Authentication Secret for a Subject be limited.
2. The Authentication Secret shall have at least 10 bits of min-entropy to protect against an untargeted attack.

Refer to NIST Special Publication 800-63-1 [SP 800-63], Appendix A, for a discussion of Authentication Secret complexity and resistance to online guessing and how to calculate min-entropy.

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Other/Additional Information

4.2.3.4 (S) STORED AUTHENTICATION SECRETS

Authentication Secrets shall not be stored as plaintext. Access to encrypted stored Secrets and to decrypted copies shall be protected by discretionary access controls that limit access to administrators and applications that require access. Three alternative methods may be used to protect the stored Secret:

1. Authentication Secrets may be concatenated to a variable salt (variable across a group of Authentication Secrets that are stored together) and then hashed with an industry standard algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen Authentication Secret file are not useful to attack other similar Authentication Secret files. The hashed Authentication Secrets are then stored in the Authentication Secret file. The variable salt may be composed using a global salt (common to a group of Authentication Secrets) and the userID (unique per Authentication Secret) or some other technique to ensure uniqueness of the salt within the group of Authentication Secrets; or
2. Store Secrets in encrypted form using industry standard algorithms and decrypt the needed Secret only when immediately required for authentication; or
3. Any method protecting stored Secrets at NIST [SP 800-63] Level 3 or 4 may be used.

- ○ This item is ready for audit.
- ○ This item is NOT ready for audit.

4.2.3.4 (S) STORED AUTHENTICATION SECRETS

Authentication Secrets shall not be stored as plaintext. Access to encrypted stored Secrets and to decrypted copies shall be protected by discretionary access controls that limit access to administrators and applications that require access. Three alternative methods may be used to protect the stored Secret:

1. Authentication Secrets may be concatenated to a variable salt (variable across a group of Authentication Secrets that are stored together) and then hashed with an industry standard algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen Authentication Secret file are not useful to attack other similar Authentication Secret files. The hashed Authentication Secrets are then stored in the Authentication Secret file. The variable salt may be composed using a global salt (common to a group of Authentication Secrets) and the userID (unique per Authentication Secret) or some other technique to ensure uniqueness of the salt within the group of Authentication Secrets; or
2. Store Secrets in encrypted form using industry standard algorithms and decrypt the needed Secret only when immediately required for authentication; or
3. Any method protecting stored Secrets at NIST [SP 800-63] Level 3 or 4 may be used.

Why is this item not ready for audit (check all that apply)?

Insufficient documentation Working/Waiting on a change to University policy

- [ ]
- [ ] Working/Waiting on the identification/acquisition of a technical solution
- [ ] Working/Waiting on the implementation of a technical solution
- [ ]
- [ ] Working/Waiting on a change to non-technical processes
- [ ] Other/Additional Information

4.2.3.5 (B) BASIC PROTECTION OF AUTHENTICATION SECRETS

1. Authentication Secrets shall not be stored as plaintext. Access to stored Secrets and to plaintext copies shall be protected by discretionary access controls that limit access to administrators and applications that require access.
2. Plaintext passwords or Secrets shall not be transmitted across a network.

- ◯ This item is Bronze compliant.
- ◯ This item is NOT Bronze compliant.

4.2.3.5 (B) BASIC PROTECTION OF AUTHENTICATION SECRETS

1. Authentication Secrets shall not be stored as plaintext. Access to stored Secrets and to plaintext copies shall be protected by discretionary access controls that limit access to administrators and applications that require access.
2. Plaintext passwords or Secrets shall not be transmitted across a network.

Why is this item not Bronze compliant (check all that apply)?

- [ ] Insufficient documentation
- [ ] Working/Waiting on the identification/acquisition of a technical solution
- [ ] Working/Waiting on the implementation of a technical solution
- [ ] Working/Waiting on a change to University policy
- [ ] Working/Waiting on a change to non-technical processes
- [ ] Other/Additional Information

4.2.3.6 (S) STRONG PROTECTION OF AUTHENTICATION SECRETS

1. Any Credential Store containing Authentication Secrets used by the IdP (or the IdP's Verifier) is subject to the operational constraints in §4.2.3.4 and §4.2.8 (that is, the same constraints as IdMS Operations). When Authentication Secrets are sent from one Credential Store to another Credential Store (for example in an account provisioning operation) Protected Channels must be used.
2. Whenever Authentication Secrets used by the IdP (or the IdP's Verifier) are sent between services for verification purposes (for example, an IdP to a Verifier, or some non-IdP application to a Verifier), Protected Channels should be used, but Protected Channels without client authentication may be used.
3. If Authentication Secrets used by the IdP (or the IdP's Verifier) are exposed in a transient fashion to non-IdP applications (for example, when users sign on to those applications using these Credentials), the IdPO must have appropriate policies and procedures in place to minimize risk from this exposure.

- ◯ This item is ready for audit.
- ◯ This item is NOT ready for audit.

4.2.3.6 (S) STRONG PROTECTION OF AUTHENTICATION SECRETS

1. Any Credential Store containing Authentication Secrets used by the IdP (or the IdP's Verifier) is subject to the operational

constraints in §4.2.3.4 and §4.2.8 (that is, the same constraints as IdMS Operations). When Authentication Secrets are sent from one Credential Store to another Credential Store (for example in an account provisioning operation) Protected Channels must be used.

2. Whenever Authentication Secrets used by the IdP (or the IdP's Verifier) are sent between services for verification purposes (for example, an IdP to a Verifier, or some non-IdP application to a Verifier), Protected Channels should be used, but Protected Channels without client authentication may be used.
3. If Authentication Secrets used by the IdP (or the IdP's Verifier) are exposed in a transient fashion to non-IdP applications (for example, when users sign on to those applications using these Credentials), the IdPO must have appropriate policies and procedures in place to minimize risk from this exposure.

Why is this item not ready for audit (check all that apply)?

Insufficient documentation	Working/Waiting on a change to University policy
Working/Waiting on the identification/acquisition of a technical solution	Working/Waiting on a change to non-technical processes
Working/Waiting on the implementation of a technical solution	Other/Additional Information

4.2.4.1 (S) CREDENTIAL ISSUANCE
To ensure that the same Subject acts throughout the registration and Credential issuance process, the Subject shall identify himself or herself in any new transaction (beyond the first transaction or encounter) with information known only to the Subject, for example a temporary Secret which was established during a prior transaction or encounter, or sent to the Subject's Address of Record. When identifying himself or herself in person, the Subject shall do so either by using a Secret as described above, or through the use of an equivalent process that was established during a prior encounter.

This item is ready for audit.

This item is NOT ready for audit.

4.2.4.1 (S) CREDENTIAL ISSUANCE
To ensure that the same Subject acts throughout the registration and Credential issuance process, the Subject shall identify himself or herself in any new transaction (beyond the first transaction or encounter) with information known only to the Subject, for example a temporary Secret which was established during a prior transaction or encounter, or sent to the Subject's Address of Record. When identifying himself or herself in person, the Subject shall do so either by using a Secret as described above, or through the use of an equivalent process that was established during a prior encounter.

Why is this item not ready for audit (check all that apply)?

Insufficient documentation
Working/Waiting on a change to University policy
Working/Waiting on the identification/acquisition of a technical solution
Working/Waiting on a change to non-technical processes
Working/Waiting on the implementation of a technical solution
Other/Additional Information

4.2.4.2 (S) CREDENTIAL REVOCATION OR EXPIRATION

1. The IdPO shall revoke Credentials and Tokens within 72 hours after being notified that a Credential is no longer valid or is compromised.
2. If the IdPO issues Credentials that expire automatically within 72 hours or less then the IdPO is not required to provide an explicit mechanism to revoke the Credentials.

This item is ready for audit.

○ This item is NOT ready for audit.

4.2.4.2 (S) CREDENTIAL REVOCATION OR EXPIRATION

1. The IdPO shall revoke Credentials and Tokens within 72 hours after being notified that a Credential is no longer valid or is compromised.
2. If the IdPO issues Credentials that expire automatically within 72 hours or less then the IdPO is not required to provide an explicit mechanism to revoke the Credentials.

Why is this item not ready for audit (check all that apply)?

☐ Insufficient documentation
☐ Working/Waiting on the identification/acquisition of a technical solution
☐ Working/Waiting on the implementation of a technical solution
☐ Working/Waiting on a change to University policy
☐ Working/Waiting on a change to non-technical processes
☐ Other/Additional Information

4.2.4.3 (S) CREDENTIAL RENEWAL OR RE-ISSUANCE

Appropriate policy and process must be in place to ensure that any new Credential and/or new Authentication Secret is provided only to the actual Credential Subject should it be necessary to reissue an Authentication Secret, e.g., due to suspected compromise or the Subject having forgotten the Secret, or to reissue a Credential due to expiration. This process must be at least as trustworthy as the process used for initial issuance of the Credential. Prior to the IdPO allowing renewal or re-issuance of a Credential, the Subject must prove possession of an unexpired current Authentication Secret or, if the Subject cannot supply the current Authentication Secret, one of the following methods may be used:

1. The Subject must supply answers to pre-registered personalized questions designed to be difficult for any other person to know;
2. A short-lived single use Secret sent to the Address of Record that the Subject must submit in order to establish a new Authentication Secret.

Replacing a forgotten Authentication Secret can be accomplished at any time using the above methodology. Authentication Secrets shall not be recovered; new Secrets shall be issued. After expiration of the current Credential or Authentication Secret, or if none of the alternative mechanisms specified above are successful, renewal and re-issuance shall not be allowed. The Subject must re-establish her or his identity with the IdPO as defined in Section 4.2 above.

All interactions conducted via a shared network shall occur over a Protected Channel such as SSL/TLS.

○ This item is ready for audit.

○ This item is NOT ready for audit.

4.2.4.3 (S) CREDENTIAL RENEWAL OR RE-ISSUANCE

Appropriate policy and process must be in place to ensure that any new Credential and/or new Authentication Secret is provided only to the actual Credential Subject should it be necessary to reissue an Authentication Secret, e.g., due to suspected compromise or the Subject having forgotten the Secret, or to reissue a Credential due to expiration. This process must be at least as trustworthy as the process used for initial issuance of the Credential. Prior to the IdPO allowing renewal or re-issuance of a Credential, the Subject must prove possession of an unexpired current Authentication Secret or, if the Subject cannot supply the current Authentication Secret, one of the following methods may be used:

1. The Subject must supply answers to pre-registered personalized questions designed to be difficult for any other person to know;
2. A short-lived single use Secret sent to the Address of Record that the Subject must submit in order to establish a new Authentication Secret.

Replacing a forgotten Authentication Secret can be accomplished at any time using the above methodology. Authentication Secrets shall not be recovered; new Secrets shall be issued. After expiration of the current Credential or Authentication Secret, or if none of the alternative mechanisms specified above are successful, renewal and re-issuance shall not be allowed. The Subject must re-establish her or his identity with the IdPO as defined in Section 4.2 above.

All interactions conducted via a shared network shall occur over a Protected Channel such as SSL/TLS.

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Other/Additional Information

4.2.4.4 (S) CREDENTIAL ISSUANCE RECORDS RETENTION
The IdPO shall maintain records of Credential issuance and revocation for a minimum of 180 days beyond the expiration of the Credential. These records must include, for each Credential issuance/revocation event, the Credential unique identifier and the time of issuance/revocation.

- ○ This item is ready for audit.
- ○ This item is NOT ready for audit.

4.2.4.4 (S) CREDENTIAL ISSUANCE RECORDS RETENTION
The IdPO shall maintain records of Credential issuance and revocation for a minimum of 180 days beyond the expiration of the Credential. These records must include, for each Credential issuance/revocation event, the Credential unique identifier and the time of issuance/revocation.

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Other/Additional Information

4.2.5.1 (S) (B) RESIST REPLAY ATTACK
The authentication process must ensure that it is impractical to achieve successful authentication by recording and replaying a previous authentication message.

- ○ This item is ready for audit.
- ○ This item is NOT ready for audit.

4.2.5.1 (S) (B) RESIST REPLAY ATTACK
The authentication process must ensure that it is impractical to achieve successful authentication by recording and replaying a previous authentication message.

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on a change to University policy

- [ ] Working/Waiting on the identification/acquisition of a technical solution
- [ ] Working/Waiting on a change to non-technical processes
- [ ] Working/Waiting on the implementation of a technical solution
- [ ] Other/Additional Information

4.2.5.2 (S) (B) RESIST EAVESDROPPER ATTACK
The authentication protocol must resist an eavesdropper attack. Any eavesdropper who records all the messages passing between a Subject and a Verifier or relying party must find that it is impractical to learn the Authentication Secret or to otherwise obtain information that would allow the eavesdropper to impersonate the Subject.

- ○ This item is ready for audit.
- ○ This item is NOT ready for audit.

4.2.5.2 (S) (B) RESIST EAVESDROPPER ATTACK
The authentication protocol must resist an eavesdropper attack. Any eavesdropper who records all the messages passing between a Subject and a Verifier or relying party must find that it is impractical to learn the Authentication Secret or to otherwise obtain information that would allow the eavesdropper to impersonate the Subject.

Why is this item not ready for audit (check all that apply)?

- [ ] Insufficient documentation
- [ ] Working/Waiting on a change to University policy
- [ ] Working/Waiting on the identification/acquisition of a technical solution
- [ ] Working/Waiting on a change to non-technical processes
- [ ] Working/Waiting on the implementation of a technical solution
- [ ] Other/Additional Information

4.2.5.3 (S) (B) SECURE COMMUNICATION
Industry standard cryptographic operations are required between Subject and IdP in order to ensure use of a Protected Channel to communicate.

- ○ This item is ready for audit.
- ○ This item is NOT ready for audit.

4.2.5.3 (S) (B) SECURE COMMUNICATION
Industry standard cryptographic operations are required between Subject and IdP in order to ensure use of a Protected Channel to communicate.

Why is this item not ready for audit (check all that apply)?

- [ ] Insufficient documentation
- [ ] Working/Waiting on a change to University policy
- [ ] Working/Waiting on the identification/acquisition of a technical solution
- [ ] Working/Waiting on a change to non-technical processes
- [ ] Working/Waiting on the implementation of a technical solution
- [ ] Other/Additional Information

4.2.5.4 (S) (B) PROOF OF POSSESSION
The authentication process shall prove the Subject has possession of the Authentication Secret or Token.

This item is ready for audit.

This item is NOT ready for audit.

4.2.5.4 (S) (B) PROOF OF POSSESSION
The authentication process shall prove the Subject has possession of the Authentication Secret or Token.

Why is this item not ready for audit (check all that apply)?

Insufficient documentation	Working/Waiting on a change to University policy
Working/Waiting on the identification/acquisition of a technical solution	Working/Waiting on a change to non-technical processes
Working/Waiting on the implementation of a technical solution	Other/Additional Information

4.2.5.5 (S) (B) SESSION AUTHENTICATION
If the IdP uses session-maintenance methods (such as cookies) so that after an initial authentication act new Assertions can be issued without the Subject having to re-authenticate, such methods shall use industry standard cryptographic techniques to
ensure that sessions are at least as resistant to attack as initial authentication.

This item is ready for audit.

This item is NOT ready for audit.

4.2.5.5 (S) (B) SESSION AUTHENTICATION
If the IdP uses session-maintenance methods (such as cookies) so that after an initial authentication act new Assertions can be issued without the Subject having to re-authenticate, such methods shall use industry standard cryptographic techniques to
ensure that sessions are at least as resistant to attack as initial authentication.

Why is this item not ready for audit (check all that apply)?

Insufficient documentation	Working/Waiting on a change to University policy
Working/Waiting on the identification/acquisition of a technical solution	Working/Waiting on a change to non-technical processes
Working/Waiting on the implementation of a technical solution	Other/Additional Information

4.2.5.6 (S) (B) MITIGATE RISK OF CREDENTIAL COMPROMISE
The IdPO must have policies, practices, or guidelines in place that prohibit Subjects from sharing their Credentials and mitigate risks of a Subject's Credential being acquired by someone else through other means. Subjects must be informed of these
policies, practices or guidelines and educated about the importance of keeping their Credentials secure.

- ◯ This item is ready for audit.
- ◯ This item is NOT ready for audit.

4.2.5.6 (S) (B) MITIGATE RISK OF CREDENTIAL COMPROMISE
The IdPO must have policies, practices, or guidelines in place that prohibit Subjects from sharing their Credentials and mitigate risks of a Subject's Credential being acquired by someone else through other means. Subjects must be informed of these
policies, practices or guidelines and educated about the importance of keeping their Credentials secure.

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Other/Additional Information

4.2.6.1 (S) (B) IDENTITY RECORD QUALIFICATION
If Subject records in an IdMS do not all meet the same set(s) of IAP criteria, then the IdP must have a reliable mechanism for determining which IAQ(s), if any, are associated with each record.

- ◯ This item is ready for audit.
- ◯ This item is NOT ready for audit.

4.2.6.1 (S) (B) IDENTITY RECORD QUALIFICATION
If Subject records in an IdMS do not all meet the same set(s) of IAP criteria, then the IdP must have a reliable mechanism for determining which IAQ(s), if any, are associated with each record.

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Other/Additional Information

4.2.7.1 (S) (B) IDENTITY ATTRIBUTES
The actual meaning of any attribute values identified as attributes recommended for use by InCommon Participants should be consistent with definitions in the InCommon Attribute Summary [InC-AtSum].

- ◯ This item is ready for audit.
- ◯ This item is NOT ready for audit.

4.2.7.1 (S) (B) IDENTITY ATTRIBUTES

The actual meaning of any attribute values identified as attributes recommended for use by InCommon Participants should be consistent with definitions in the InCommon Attribute Summary [InC-AtSum].

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Other/Additional Information

4.2.7.2 (S) (B) IDENTITY ASSERTION QUALIFIER (IAQ)
An IdPO may be certified by InCommon to be eligible to include one or more InCommon IAQs as part of Assertions. The IdP must not include an InCommon IAQ that it has not been certified by InCommon to assert and must not include an IAQ if that Assertion does not meet the criteria for that IAP. The IdP must be capable of including an InCommon IAQ when the necessary criteria are met for the Subject.

- ○ This item is ready for audit.
- ○ This item is NOT ready for audit.

4.2.7.2 (S) (B) IDENTITY ASSERTION QUALIFIER (IAQ)
An IdPO may be certified by InCommon to be eligible to include one or more InCommon IAQs as part of Assertions. The IdP must not include an InCommon IAQ that it has not been certified by InCommon to assert and must not include an IAQ if that Assertion does not meet the criteria for that IAP. The IdP must be capable of including an InCommon IAQ when the necessary criteria are met for the Subject.

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Other/Additional Information

4.2.7.3 (S) (B) CRYPTOGRAPHIC SECURITY
Cryptographic operations are required between an IdP and any SP. Cryptographic operations shall use industry standard cryptographic techniques. The Assertion must be either:

- Digitally signed by the IdP; or
- Obtained by the SP directly from the trusted entity (e.g., the IdP or Attribute Service) using a Protected Channel.

- ○ This item is ready for audit.
- ○ This item is NOT ready for audit.

4.2.7.3 (S) (B) CRYPTOGRAPHIC SECURITY
Cryptographic operations are required between an IdP and any SP. Cryptographic operations shall use industry standard

cryptographic techniques. The Assertion must be either:

- Digitally signed by the IdP; or
- Obtained by the SP directly from the trusted entity (e.g., the IdP or Attribute Service) using a Protected Channel.

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Other/Additional Information

4.2.8.1 (S) SOFTWARE MAINTENANCE
IdMS Operations shall use up-to-date supported software.

- ○ This item is ready for audit.
- ○ This item is NOT ready for audit.

4.2.8.1 (S) SOFTWARE MAINTENANCE
IdMS Operations shall use up-to-date supported software.

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Other/Additional Information

4.2.8.2 (S) NETWORK SECURITY

1. Appropriate measures shall be used to protect the confidentiality and integrity of network communications supporting IdMS operations. Protected Channels should be used for communications between systems.
2. All personnel with login access to IdMS Operations infrastructure elements must use access Credentials at least as strong as the strongest Credential issued by the IdPO.

- ○ This item is ready for audit.
- ○ This item is NOT ready for audit.

4.2.8.2 (S) NETWORK SECURITY

1. Appropriate measures shall be used to protect the confidentiality and integrity of network communications supporting IdMS operations. Protected Channels should be used for communications between systems.
2. All personnel with login access to IdMS Operations infrastructure elements must use access Credentials at least as strong as the strongest Credential issued by the IdPO.

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Other/Additional Information

4.2.8.3 (S) PHYSICAL SECURITY
IdMS Operations shall employ physical access control mechanisms to restrict access to sensitive areas, including areas such as leased space in remote data centers, to authorized personnel.

- ○ This item is ready for audit.
- ○ This item is NOT ready for audit.

4.2.8.3 (S) PHYSICAL SECURITY
IdMS Operations shall employ physical access control mechanisms to restrict access to sensitive areas, including areas such as leased space in remote data centers, to authorized personnel.

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Other/Additional Information

4.2.8.4 (S) RELIABLE OPERATIONS
IdMS Operations shall employ techniques to minimize system failures and ensure that any failures are not likely to result in inaccurate Assertions being sent to SPs.

- ○ This item is ready for audit.
- ○ This item is NOT ready for audit.

4.2.8.4 (S) RELIABLE OPERATIONS
IdMS Operations shall employ techniques to minimize system failures and ensure that any failures are not likely to result in inaccurate Assertions being sent to SPs.

Why is this item not ready for audit (check all that apply)?

- ☐ Insufficient documentation
- ☐ Working/Waiting on a change to University policy
- ☐ Working/Waiting on the identification/acquisition of a technical solution
- ☐ Working/Waiting on a change to non-technical processes
- ☐ Working/Waiting on the implementation of a technical solution
- ☐ Other/Additional Information

Finally, do you plan on applying for:

- ◯ Bronze first
- ◯ Silver first
- ◯ Silver first, but we assume that means we'll be Bronze certified automatically