Credential Assessment Framework (CAF) Self-Assessment Tool – July 7, 2008

Instructions for Completing the Assessment

1. Review previous assessment reports.
2. Complete the CAF Follow-Up Self-Assessment based on the following guidelines:
   a. Answer ***Yes*** or ***No*** for each question regarding the credential store (CS) that connects to the IAA Authentication Hub.
   b. Answers are to be based on the current state of the CS.
   c. If the answer is unknown, mark the answer as ***No***.
   d. If plans have been documented to modify the CS for compliance with the question, ***identify the date that the control or procedure is to be implemented***.
   e. If additional information is needed to justify a Yes/No answer or if there are alternative mitigating controls implemented, please identify these in *Part 6: Comments or Mitigating Controls.*
   f. Terms underlined can be located in the glossary in Appendix A
   g. If you have questions about the survey, please contact Stefan Wahe at smwahe@wisc.edu.
3. Conduct a Nesses network vulnerability scans from both outside the CS private network and inside the CS private network (or as appropriate). Save the results in an .nbe format. Header information needs to be included with the scan. If you do not have a vulnerability scanner or need assistance with these tools, contact Stefan Wahe at smwahe@wisc.edu.
4. Coordinate with Stefan Wahe on how to securely submit the survey and scan results.

About the CAF Self-Assessment

The survey is broken into an introduction, a survey of five sections and two appendices:

Intro: Compliance Agreement: Identifies the contact and system information and establishes the terms in complying with this survey.

Part 1: ***Credential Store Management Operations:*** Verifies the authority of the credential store, the existence of a security program and identifies if procedures and controls are in place to protect the operations and maintenance of the credential store.

Part 2: ***Authentication Protocol:*** Verifies how the shared secret (e.g. passwords) are encrypted, stored and transmitted.

Part 3: ***Token Strength:*** Verifies the complexity and resilience of the Personal Identification Number (PIN) or Password?

Part 4: ***Registration and Identity Proofing:*** Verifies that implemented steps for the identity proofing process.

Part 5: ***Credential Store Availability:*** Verifies the availability of the credentials.

Part 6: ***Comments or Mitigating Controls:*** Identify any comments or mitigating controls regarding the question or the other Parts.

Appx A: ***Glossary of Terms***: Provides definitions for terms used in this document.

Appx B: ***List of Acronyms***: Provides terms associated with acronyms used through this document.

Appx C: ***Suggested Compliance Techniques***: This appendix offers suggested actions for compliance. These suggestions are based on InCommon's Identity Assurance Profile Release 12 and NIST 800-63-1 *Electronic Authentication Guideline*.

Appx D: ***Changes to Assessment Tool***: Identifies the changes to the assessment tool between versions 10-2 and 11.

Appx E: ***CAF Information***: Information about the CAF that was included with the original assessment in May 2007.

The survey was developed based on the following resources:

- *InCommon Identity Assurance Profiles Release 12* (4/17/2008) (http://www.incommonfederation.org/)
- National Institute of Standards and *Technology Electronic Authentication Guidelines* (800-63-1) and *Recommended Security Controls* (800-52) (http://csrc.nist.gov/publications/nistpubs/index.html)
- Office of Campus Information Technology's *Restricted Data Security Standards* (http://www.doit.wisc.edu/security/resources/restricted.asp).

Contact Information and System Description

CS Operational Management Contact Information		
	Primary	Secondary
Name		
Phone		
Title		
Email		
Provide contact Information for others assisting with the survey:		

CS Information	
Name *e.g. IAA Auth Hub*	
Number of Records *e.g. 10,000 active identities, 50,000 identities with revoked credentials*	
Documentation Location *e.g. www.uwsa.edu/olit/iaa/*	
System Diagram *Be prepared to proved if assistance is needed for scans*	

The operational management agrees to complete this assessment according to the current state of the <u>Credential Store</u> (CS). Planned upgrades or modifications should be identified where appropriate to a corresponding *No* answer. The answers provided are understood to be the best information provided by those listed above who are completing the survey. The information will be maintained and distributed in a confidential and secure manner between the CS Operational Management, the CAF Coordinator and the recipients of the compiled reports.

Credential Assessment Framework Survey

Part 1: Credential Store Management and Operations

Date*- For answers marked No, identify the planned date for complying with the requirement.

1. **Authority and Responsibility**	**Yes**	**No**	**Date***
a) Has the Campus CIO and the IAA Governance Group identified the Credential Store (CS) as a valid entity of the UW-System community for the purpose of identity assertion, assigning and managing credentials associated with an identity and, authenticating identities to approved services? (If the credential store is currently used by the IAA, the CS can be considered as approved)			
b) Has the CS been designated by executive management of the responsible institution to perform this function as required by the institution's policies?			
2. **General Disclosure**	**Yes**	**No**	**Date***
a) Are the Terms, Conditions, and Privacy Policy available to identity subjects in the CS and the consumers of the data?			
b) Does the CS notify identity subjects in a timely and reliable fashion of any changes to the Terms, Conditions, and Privacy Policy that may impact the identity subject?			
3. **Security Program (Documentation)**	**Yes**	**No**	**Date***
a) Does the CS have documented security policies and procedures?			
b) Has management identified and assigned security responsibilities for the management and operations of the CS to staff?			
c) Has staff been notified and trained in their assigned security responsibilities associated with the CS?			
d) Is staff periodically required to review their roles and responsibilities and how they are related to the policies and procedures?			
4. **Subcontracts**	**Yes**	**No**	**Date***
a) Are subcontractors or outsourced components employed to assist with the maintenance and operations of the CS? If Yes, please answer the following:			
i. Are subcontractors or outsourced components of the CS required to have established contractual agreements that stipulates critical policies and practices that affect the assurance of the CS?			
ii. Are the contractual agreements monitored for compliance on reoccurring bases			

5. Helpdesk	**Yes**	**No**	**Date***
a) Is a helpdesk available for identity subjects to resolve issues related to their credentials during the CS's regular business hours, minimally from 9am to 5pm Monday through Friday?			
b) Is helpdesk staff properly trained for supporting calls regarding the CS?			
6. Audit	**Yes**	**No**	**Date***
a) Is the CS audited by an independent internal or external auditor at least every 24 months to ensure the operation's practices are consistent with the institution's policies and procedures for the CS?			
7. Risk Management	**Yes**	**No**	**Date***
a) Does the CS follow a risk management life cycle methodology that adequately identifies and mitigates risks related to the CS operations and availability as well as maintaining the identity subjects privacy?			
8. Continuity of Operations	**Yes**	**No**	**Date***
a) Does the CS have a Continuity of Operations Plan that covers disaster recovery and the resilience of the CS?			
b) Does the CS employ mitigation techniques to ensure system failures do not result in false positive and false negative authentication errors?			
c) Are there plans documented and staff training on the process of recovering the CS from a catastrophic disaster?			
9. Logging	**Yes**	**No**	**Date***
a) Are logging requirements for the CS documented and periodically reviewed?			
b) Does the CS log and retain securely for 6 months all significant events related to credential management (e.g., issuance, and revocation)?			

10. Configuration Management	**Yes**	**No**	**Date***
a) Does the CS demonstrate Configuration Management methodology that includes:			
i. A documented process for reviewing, approving and implementing changes			
ii. Version control for software system components			
iii. Timely identification and installation of all applicable patches for any software used in the provisioning of the CS			
b) Are system logs (e.g. operating system, change management) logs archived for 6 months?			
11. Network Security	**Yes**	**No**	**Date***
a) Are cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) implemented to safeguard authentication tokens during transmission over open, public networks?			
b) Has a firewall configuration been implemented that:	**Yes**	**No**	**Date***
i. Denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the restricted data environment			
ii. Restricts connections between publicly accessible servers and any system component storing token data (e.g. password), including any connections from wireless networks			
iii. Prohibit direct public access between external networks and any system component that stores restricted data (for example, databases, logs, trace files)			
12. Vulnerability Management	**Yes**	**No**	**Date***
a) Do devices that comprise the infrastructure of the credential store run vulnerability software that prevents the insertion of malicious code or detects unauthorized changes to system and application files?			
b) Are all vulnerability detection mechanisms kept current, are actively running, and capable of generating audit logs?			
c) Are all system components and software kept current with the latest vendor-supplied security patches?			
d) Is there a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet)?			
13. Physical Security	**Yes**	**No**	**Date***

a) Are access controls used to limit and monitor physical access to systems that store, process, or transmit credential data implemented?			
14. Incident Response	**Yes**	**No**	**Date***
a) Is there an implemented incident response plan for events of system compromise? If Yes, please answer the following question:			
i. Does the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and notification strategies?			
15. Identity Data Protection	**Yes**	**No**	**Date***
a) Is a data retention and disposal policy implemented?			
b) Is storage amount and retention time kept to a minimum based on the required business, legal, and/or regulatory purposes, as documented in the data retention policy?			
c) Are restricted data elements such as SSN or sensitive data elements such as Date of Birth encrypted at rest, audited or masked from content consumers who do not have a business need to view these data elements?			
i. Are encryption keys protected?			
ii. Are there documented and implemented key management processes and procedures for encryption keys?			

Part 2: Authentication Protocol

Date*- For answers marked No, identify the planned date for complying with the requirement.

16. Secure Channel	**Yes**	**No**	**Date***
a) Are secrets (e.g. passwords) used by claimant for authentication asserted by cryptographic operations between claimant and verifier in order to ensure an end-to-end secure communications channel?			
17. Proof of Control	**Yes**	**No**	**Date***

a) Does the authentication protocol prove the claimant has control of the authentication password token?			
18. Session Authentication	**Yes**	**No**	**Date***
a) Are session tokens cryptographically authenticated? For example, session cookies must be encrypted, digitally signed, or contain an Hash-based Message Authentication Code (HMAC).			
19. Stored Secrets	**Yes**	**No**	**Date***
a) Are secrets, such as passwords, NOT stored as plaintext?			
b) Is access to secrets protected by discretionary access controls that limit access to administrators and only applications that require access?			
20. Password Sharing (Non-repudiation)	**Yes**	**No**	**Date***
a) Is there a documented policy that prohibits identity subjects from sharing passwords?			
b) Are identity subjects periodically required to review the policy?			
c) Are records maintained that confirmations that identity Subjects understand and will comply with the policy?			
21. Threat Protection	**Yes**	**No**	**Date***
a) Are controls in place to reduce the likelihood of successful On-Line Guessing and Replay attacks against the authentication protocol?			
b) Are controls in place to resist on-line guessing and replay attacks?			
22. Protocol Types	**Yes**	**No**	**Date***
a) Which of the following authentication protocol types are allowed:			
i. Tunneled password: show that claimant who provides a password does so through a secure (encrypted) TLS protocol session (tunneling).			
ii. Zero knowledge-base password: show that claimant who provides password does not tell receiver anything about the password the receiver does not already know.			
iii. Other			

23. Approved Cryptography	**Yes**	**No**	**Date***
a) Are cryptographic operations required between the Verifier and Relying Party?			
b) Are all cryptographic operations done in compliance with cryptographic techniques (see question 24)?			
c) Are cryptographic operations used between the Claimant and Verifier?			
24. Cryptographic Algorithms (FIPS 140-2)	**Yes**	**No**	**Date***
a) Which of the following cryptographic algorithms are being used to protect the token (e.g. password) at rest:			
i. SHA-1			
ii. SHA-2 or other SHA-X variants			
iii. AES			
iv. DES3			
v. RSA			
vi. Self-Developed Algorithm (if yes, identify when migration to a approved standard can be expected)			
vii. Other			
25. Protected Secrets	**Yes**	**No**	**Date***
a) Are secrets (e.g., password, Personal Identification Number (PIN), key) that are involved in authentication protected from third parties by verifier or CS, with the following exceptions of (1) the sharing of session (temporary) shared secrets may be provided by the CS to independent systems that must verify the secret and (2) Long-term secrets and session (temporary) secrets can be shared with infrastructure elements controlled and designated by the CS?			

Part 3: Token Strength

Date*- For answers marked No, identify the planned date for complying with the requirement.

<table>
<tr><th>26. Uniqueness</th><th>Yes</th><th>No</th><th>Date*</th></tr>
<tr><td>a) Are identity subjects given a credential (e.g., UserID + Password) such that the visible portion (UserID) is unique across all such elements issued by the CS?</td><td></td><td></td><td></td></tr>
<tr><td>b) Are LOA-2 credentials in the CS mapped only to a single individual (e.g. no shared accounts).</td><td></td><td></td><td></td></tr>
<tr><td>c) Are unique identifiers, such as PVI, prevented from being recycled after an identity subject credentials have been revoked?</td><td></td><td></td><td></td></tr>
<tr><td>d) Does the CS maintain a record of status that identifies the revocation of credentials and provides controls to ensure that revoked credentials cannot be used to authenticate to systems or services?</td><td></td><td></td><td></td></tr>
<tr><td><b>27. Modifiable</b></td><td><b>Yes</b></td><td><b>No</b></td><td><b>Date*</b></td></tr>
<tr><td>a) Are Identity subjects able to change their passwords?</td><td></td><td></td><td></td></tr>
<tr><td><b>28. Password Policy (Entropy)</b>
Identify the change date for any plans that increase the strength of the password (e.g. increase from six character to eight character passwords).</td><td><b>Yes</b></td><td><b>No</b></td><td><b>Date</b></td></tr>
<tr><td>a) What is the minimum required length of the password?</td><td><b>Yes</b></td><td><b>No</b></td><td></td></tr>
<tr><td>i. There is no minimum</td><td></td><td></td><td></td></tr>
<tr><td>ii. 5 or fewer characters</td><td></td><td></td><td></td></tr>
<tr><td>iii. 6 characters</td><td></td><td></td><td></td></tr>
<tr><td>iv. 7 characters</td><td></td><td></td><td></td></tr>
<tr><td>v. 8 characters</td><td></td><td></td><td></td></tr>
<tr><td>vi. 9 or more characters</td><td></td><td></td><td></td></tr>
<tr><td>b) Is the password required to contain:</td><td><b>Yes</b></td><td><b>No</b></td><td><b>Date*</b></td></tr>
<tr><td>i. Uppercase letters (A-Z)</td><td></td><td></td><td></td></tr>
<tr><td>ii. Lowercase letters (a-z)</td><td></td><td></td><td></td></tr>
<tr><td>iii. Digit (0-9)</td><td></td><td></td><td></td></tr>
<tr><td>iv. Special character (~`!@#$%^&*()+=_-{}[]\|:;”’?/<>,.)</td><td></td><td></td><td></td></tr>
<tr><td>v. Control characters</td><td></td><td></td><td></td></tr>
<tr><td>c) Are passwords prevented from containing:</td><td><b>Yes</b></td><td><b>No</b></td><td><b>Date*</b></td></tr>
<tr><td>i. Username (e.g. NetID)</td><td></td><td></td><td></td></tr>
<tr><td>ii. The Identity Subjects Proper Name (e.g. John, Joe, Sally Smith)</td><td></td><td></td><td></td></tr>
</table>

d) How often are password changes required?	**Yes**	**No**	**Date***
i. Once every 90 days			
ii. Once every 180 days			
iii. Once every year			
iv. Users are not required to change their passwords			
e) Are there a maximum number of failed logon attempts?	**Yes**	**No**	**Date***
i. Four or fewer failed attempts			
ii. Five to eights attempts			
iii. Nine or more attempts			
iv. There are no limits for failed logon attempts			
f) Is a password history maintained? If so how many password changes and stored?	**Yes**	**No**	**Date***
i. Four or fewer password rests			
ii. Five to six password resets			
iii. Seven or more password resets			
iv. Password history is not maintained			
g) Is password history maintained and used to enforce the re-use of passwords?			
h) From the inception of the password, is the total number of failed attempts tracked? If the total number of failed attempts reached 1,800, is the credential de-valued to LOA-1?			
i) Are controls in place that prevent a consecutive character string of three or more (e.g. aaa, 111, @@@)?			
j) Are there procedures for individuals to be able to recover from forgotten passwords?			

Part 4: Registration and Identity Proofing

Date*- For answers marked No, identify the planned date for complying with the requirement.

29. Identity Verification Process (IVP) Disclosure	**Yes**	**No**	**Date***
a) Is the identity proofing and registration process performed according to a written policy and procedures that specifies the particular steps taken to verify identities?			
b) Do the procedures address primary objectives of registration and identity proofing, including:	**Yes**	**No**	**Date***
i. Ensuring a person with the applicant's claimed attributes does exist, and those attributes are sufficient			

to uniquely identify a pre-registered single person or other entity?			
ii. Ensuring the applicant whose token is registered is in fact the person who is entitled to the identity?			
iii. Ensuring the applicant cannot later repudiate the registration; therefore, if there is a dispute about a later authentication using the identity subject's credential, the identity subject cannot successfully deny a registered credential?			
c) Is personal identifying information collected as part of the registration process protected from unauthorized disclosure or modification?			
30. Records	**Yes**	**No**	**Date***
a) Is the record of the facts of registration maintained by the CS or its representative (e.g., Registration Authority)?			
b) Are records identifying the revocation of credentials maintained?			
c) Are the record of the facts of registration maintained that identifies:	**Yes**	**No**	**Date***
i. Identity proofing document number (e.g. passport or drivers license number),			
ii. Full legal name			
iii. Date and place of birth			
iv. Current address of record (typically the address stored in the human resources or student records systems; does not need to match drivers license).			
d) Is the minimum record retention period for registration data established for seven years beyond the expiration or revocation (see your Campus Records Retention policy)?			
e) Is the CS required to comply with other records retention policies, or federal, state or local laws and regulations?			
f) Do credentials include identifying information that permits recovery of the records of the registration associated with the credentials?			
31. Confirmed Relationship	**Yes**	**No**	**Date***
a) Does the CS know the identity of the applicant for at least one of the following purposes:			
i. Employment			
ii. Registered or former student at the institution			

iii. Visiting scholar or researcher receiving services from the institution			
iv. Extension of credit of $2,000 or more			
v. Regular payment of fees for services and a duty of the organization to know the true identity of the customer			
vi. Matriculation at an accredited degree granting educational institution			
vii. Compliance with public safety, health or other government regulations that impose a duty to verify the identity or members or participants			
b) Does the CS confirm that the applicant is a person with a current relationship to the organization?			
c) Do employers and educational instructors who verify the identity of their employees or students follow comparable procedures to those stated for In-person Proofing or Remote Proofing?			
32. Remote Proofing	**Yes**	**No**	**Date***
a) Does the Registration Authority (RA) establish the applicant's identity based on possession of a (1) valid Government ID number (e.g. a driver's license or passport) and (2) a financial account number (e.g., checking account, savings account, loan or credit card) or a utility service (e,g, electricity, gas or water) with confirmation via records of either number?			
b) Does the RA inspect both ID number and account number supplied by applicant? (e.g. verifies information provided by applicant including ID number or account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, date of birth, address and other personal information in records are consistent with the application and sufficient to identify a unique individual).			
c) Does the address confirmation and notification process include:	**Yes**	**No**	**Date***
i. RA sends notice to an <u>address of record</u> confirmed in the records check			
ii. RA issues <u>credentials</u> in a manner that confirms the <u>address of record</u> supplied by the applicant			
iii. RA issues <u>credentials</u> in a manner that confirms ability of the applicant to receive telephone communications at telephone number or email at email address associated with the applicant in records.			
33. In Person Proofing	**Yes**	**No**	**Date***

a) Does the Registration Authority (RA) establish the applicant's identity based on possession of a valid current primary government issued picture ID that contains applicant's picture, and either an address or nationality (e.g. driver's license or passport)?			
b) Does the RA inspect the given photo-ID, compare picture to applicant, record ID number, date of issuance and expiration, address and date of birth? If ID appears valid and photo matches applicant then:			
i. If ID confirms address of record, authorize or issue credentials and send notice to address of record, or			
ii. If ID does not confirm address of record, issue credentials in a manner that confirms address of record.			
34. Identity Re-Confirmation	**Yes**	**No**	**Date***
a) Are identity attributes re-confirmed not less that every 2 years, or when notified by the identity subject of a change?			
35. Credential Revocation	**Yes**	**No**	**Date***
a) Does the CS revoke credentials and tokens within 72 hours after being notified that a credential is no longer valid or a token is compromised?			
36. Delivery Confirmation	**Yes**	**No**	**Date***
a) Does the CS issue or renew credentials and tokens in a manner that confirms the applicant's either the (1) Postal address of record or (2) the telephone number of record (either a traditional line or a cell phone)?			

Part 5: Credential Store Availability

Date*- For answers marked No, identify the planned date for complying with the requirement.

37. Credential Store Availability	**Yes**	**No**	**Date***
a) Has the infrastructure for the CS been designed to maintain a high level of availability for individuals and service providers (e.g. redundant servers, redundant sites, fail over)?			
b) On a yearly average has the credential store experienced more than 87 hours of scheduled and unscheduled unavailability?			

Part 6: Comments and Mitigating Controls

Date*- For answers marked No, identify the planned date for complying with the requirement.

Question	**Comment or Mitigating Control** * Include date if it is a planned mitigating control)	Date*

Appendix A Glossary of Terms

Term	Definition
Active Attack	An attack on the authentication protocol where the attacker transmits data to the claimant or verifier. Examples of active attacks include a man-in-the-middle, impersonation, and session hijacking.
Address of Record	The official location where an individual can be found. The address of record always includes the residential street address of an individual and may also include the mailing address of the individual. In very limited circumstances, an Army Post Office box number, Fleet Post Office box number or the street address of next of kin or of another contact individual can be used when a residential street address for the individual is not available.
Approved Cryptography	FIPS approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation. Approved cryptographic algorithms must be implemented in a crypto module validated under FIPS 140-2. For more information on validation and a list of validated FIPS 140-2 validated crypto modules see http://csrc.nist.gov/cryptval/.
Attack	An attempt to obtain an identity subject's token or to fool a verifier into believing that an unauthorized individual possess a claimant's token.
Attacker	A party who is not the claimant or verifier but wishes to successfully execute the authentication protocol as a claimant.
Assertion	A statement from a verifier to a relying party that contains identity information about an identity subject. Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol.
Assurance Level	Level of trust, as defined by the OMB Guidance for E-Authentication. This guidance describes four identity authentication assurance levels for e-government transactions. Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as 1) the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. The four levels of assurance are: Level 1: Little or no confidence in the asserted identity's validity. Level 2: Some confidence in the asserted identity's validity. Level 3: High confidence in the asserted identity's validity. Level 4: Very high confidence in the asserted identity's validity.
Authentication	The process of establishing confidence in user identities.
Authentication	A well specified message exchange process that verifies possession of a

Protocol	token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected.
Authentication Service Component	Interface specifications that describe the requirements for IdPs to technically interoperate with Relying Parties.
Bit	A binary digit: 0 or 1.
Challenge-Response Protocol	An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a shared secret (either cryptographically or by hashing the challenge and secret together) to generate a response that is sent to the verifier. The verifier knows the shared secret or decryption key and can independently compute the response and compare it with the response generated by the claimant. If the two are the same, the claimant is considered to have successfully authenticated himself. When the shared secret is a cryptographic key, such protocols are generally secure against eavesdroppers. When the shared secret is a password, an eavesdropper does not directly intercept the password itself, but the eavesdropper may be able to find the password with an off-line password guessing attack. An example of this is the “proof of possession of the Private Key” during a PKI certificate verification interchange.
Claimant	A party whose identity is to be verified using an authentication protocol.
Credential	Digital documents used in authentication that bind an identity or an attribute to an identity subject’s token. Note that this document uses “credential” broadly, referring to both electronic credentials and tokens.
Credential Assessment Framework (CAF) Coordinator	A person responsible for coordinating the Credential Assessment Framework process. Responsibilities include maintaining an assessment survey tool, combining the results of the surveys and reporting back to the groups involved in the process.
Credential Assessment Framework (CAF)	A list of related criteria used to *assess* the Assurance Level of a Credential Service. The InCommon CAFs are derived from Federal E-Authentication Initiative CAFs.
Cryptography	The discipline which embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof. [ANSI X9.31] Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and transformation of ciphertext into plaintext by decryption. [NIST SP 800-2]
Cryptographic Key	A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, keys must provide at least 80-bits of protection. This means that it must be as hard to find an unknown key or decrypt a message, given the information exposed to an eavesdropper by an authentication, as to guess an 80-bit random number.

Cryptographic Module	The set of hardware, software, and/or firmware that implements Approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.
Digital Signature	An asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection.
Electronic Credentials	Digital documents used in authentication that bind an identity or an attribute to an identity subject's token.
Eavesdropping Attack	An attack on a data connection where one simply records or views data instead of tampering with the connection.
Entropy	A measure of the amount of uncertainty that an attacker faces to determine the value of a secret. Entropy is usually stated in bits. Guessing entropy is a measure of the difficulty that an attacker has to guess the average password used in a system. In this document, entropy is stated in bits. When a password has n-bits of guessing entropy then an attacker has as much difficulty guessing the average password as in guessing an n-bit random quantity. The attacker is assumed to know the actual password frequency distribution.
FIPS 140-2	Specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The FIPS 140-2 standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.3 d) FIPS 140-2 shall be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract.
Guessing Entropy	A measure of the difficulty that an attacker has to guess the average password used in a system. In this document, entropy is stated in bits. When a password has n-bits of guessing entropy then an attacker has as much difficulty guessing the average password as in guessing an n-bit random quantity. The attacker is assumed to know the actual password frequency distribution.
Hash-based Message Authentication Code (HMAC)	Hash-based Message Authentication Code: a symmetric key authentication method using hash functions.
Identity	The set of attributes that apply to an individual person. Some attributes will be unique to a single person; others may be shared. Since the legal names of persons are not necessarily unique, certain identity assertions intended to

	refer to a single specific person must include sufficient additional information (for example an address, some unique identifier such as an employee or account number, or a specially constructed unique identifier that is never reassigned to a different person) to make the complete asserted identity unique.
Identity Proofing	The process by which an IdP and an RA validate sufficient information to uniquely associate a physical person with a record in the IdP database. The database record may be created if no match is found to a previously existing record.
Identity Provider (IdP)	A trusted entity that issues or registers identity subject tokens and issues electronic credentials to identity subjects. The IdP may encompass Registration Authorities and verifiers that it operates. An IdP may be an independent third party, or may issue credentials for its own use. If an IdP offers more than one type of credential then each one may be provided a separate IdP identifier for use in identity assertions.
Identity Subjects	A person associated with a record and credential that is maintained in the credential store or associating systems.
Impractical	"Impractical" is used here in the cryptographic sense of nearly impossible, that is there is always a small chance of success, but even the attacker with vast resources will nearly always fail. For off-line attacks, impractical means that the amount of work required to "break" the protocol is at least on the order of 280 cryptographic operations. For on-line attacks impractical means that the number of possible on-line trials is very small compared to the number of possible key or password values.
Min-entropy	A measure of the difficulty that an attacker has to guess the most commonly chosen password used in a system. In this document, entropy is stated in bits. When a password has n-bits of min-entropy then an attacker requires as many trials to find a user with that password as is needed to guess an n-bit random quantity. The attacker is assumed to know the most commonly used password(s).
Network	An open communications medium, typically the Internet, that is used to transport messages between the claimant and other parties. Unless otherwise stated no assumptions are made about the security of the network; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking…) and passive (e.g., eavesdropping) attack at any point between the parties (claimant, verifier, CSP or relying party).
Nonce	A value used in security protocols that is never repeated with the same key. For example, challenges used in challenge-response authentication protocols generally must not be repeated until authentication keys are changed, or there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable.
Off-line Attack	An attack where the attacker obtains some data (typically by eavesdropping on an authentication protocol run, or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing.

On-line Guessing Attack	An attack against an authentication protocol where the attacker either assumes the role of a claimant with a genuine verifier or actively alters the authentication channel. The goal of the attack may be to gain authenticated access or learn authentication secrets.
Password	A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. See also PIN.
Password Token	A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings; however some systems use a number of images that the identity subject memorizes and must identify when presented along with other similar images.
Passive Attack	An attack against an authentication protocol where the attacker intercepts data traveling along the network between the claimant and verifier, but does not alter the data (i.e. eavesdropping).
Personal Identification Number (PIN)	A password consisting only of decimal digits.
Possession and control of a token	The ability to activate and use the token in an authentication protocol.
Practice Statement	A formal statement of the practices followed by an authentication entity (e.g., RA, IdP, or verifier); typically the specific steps taken to register and verify identities, issue credentials and authenticate claimants.
Proof of Possession (PoP) protocol	A protocol where a claimant proves to a verifier that he/she possesses and controls a token (e.g., a key or password).
Protocol Run	An instance of the exchange of messages between a claimant and a verifier in a defined authentication protocol that results in the authentication (or authentication failure) of the claimant.
Public Key Certificate	A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of an identity subject to a public key. The certificate indicates that the identity subject identified in the certificate has sole control and access to the private key. See also [RFC 3280].
Registration	The process through which a party applies to become an identity subject of a IdP and an RA validates the identity of that party on behalf of the IdP.
Registration Authority	A trusted entity that establishes and vouches for the identity of an identity subject to an IdP. The RA may be an integral part of an IdP, or it may be independent of an IdP, but it must have a defined and appropriate relationship to the IdP(s).
Relying Party	An entity that relies upon the identity subject's credentials, typically to process a transaction or grant access to information or a system.
Replay Attack	An attack in which the Attacker is able to replay previously captured messages (between a legitimate Claimant and a Verifier) to masquerade as that Claimant to the Verifier or vice versa.

Repudiation	Intentional denial of registration (i.e., identity subject claims that he/she did not register that token) or of authentication (i.e., identity subject intentionally compromises his/her token, to repudiate authentication).
Restricted Data	Data the includes but not limited to: (A) social security number; (B) driver's license number or state identification number; (C) financial account number (including credit/debit card) or any security code, access code of password that would permit access to an individual's financial account; (D) deoxyribonucleic acid profile as defined in S. 939.74 (2d) (a); (E) unique biometric data, including fingerprint, voice print, retina or iris image or any other unique physical representation; and (F) protected health information (any information about health status, provision of health care, or payment of health care).
Revocation	The disabling of the identity subject's credentials.
Secure Sockets Layer (SSL)	Protocol for transmitting private documents via the Internet by using a private key to encrypt data that's transferred over the SSL connection.
Session Cookie	Small transient file that contains information about an end user that disappears when the end user's browser is closed. Unlike a persistent cookie, a transient cookie is not stored on an end user's hard drive, but is only stored in temporary memory that is erased when the browser is closed.
Shared Secret	A secret used in authentication that is known to the claimant and the verifier. There are two durations for a shared secret: • Session (temporary) secret – duration of the secret is limited to the duration of the user session. That is, the secret is created, used, and expired during a single user authentication session. • Long-term secret – duration of the secret persists ongoing, and is used from one user authentication session to another user authentication session.
Subject	The person whose identity is bound in a particular credential. A party who receives a credential or token from an IdP and becomes a claimant in an authentication protocol.
Token	Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity.
Transport Layer Security (TLS)	An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by [RFC 2246] and [RFC 3546]. TLS is similar to the older Secure Socket Layer (SSL) protocol and is effectively SSL version 3.1.
Tunneled Password Protocol	A protocol where a password is sent through a protected channel. For example, the TLS protocol is often used with a verifier's public key certificate to (1) authenticate the verifier to the claimant, (2) establish an encrypted session between the verifier and claimant, and (3) transmit the claimant's password to the verifier. The encrypted TLS session protects the claimant's password from eavesdroppers.
Verified Name	An identity subject name that has been verified by identity proofing.

Verifier	An entity that verifies the claimant's identity by verifying the claimant's possession of a token using an authentication protocol. To do this, the verifier also may need to validate credentials that link the token and identity and check their status.
Zero Knowledge password	Claimant who provides password that does not tell receiver anything about the password the receiver does not already know.

Appendix B Acronyms

Acronym	Definition
ANSI	American National Standards Institute
ASC	Authentication Service Component
ATO	Authorization To Operate
CAF	Credential Assessment Framework
CAF	Credential Assessment Framework
CS	Credential Service
CSP	Credential Service Provider
DR	Disaster Recovery
FIPS	Federal Information Processing Standard
HMAC	Hash-based Message Authentication Code
ID	Identification
IdP	Identity Provider
IT	Information Technology
IVP	Identity Verification Process
NIST	National Institute of Standards and technology
OMB	Office Of Management And Budget (Federal government)
PIN	Personal Identification Number
RA	Registration Authority
RFC	Request For Comment (see www.ietf.org)
RP	Relying Party
SSL	Secure Socket Layer
TLS	Transport Layer Security

Appendix C: Suggested Compliance Techniques

The following identifies suggested actions for compliance for specific requirements. Not all requirements are reflected in this list.

2-General Disclosure

The CS may notify identity subjects in a timely and reliable fashion of any changes to the Terms, Conditions, and Privacy Policy via email or by posting to a centralized authentication page.

4-Help Desk

Help Desk staff should receive training at time of hire that identifies processes associated with assisting identity subjects with identity proofing for the purpose of password recovery; call escalating in the event of the CS becoming unavailable; and call escalating in the event of compromised credentials. These procedures should be documented and available for Help Desk staff. On-going training should be conducted annually or in the event of a procedural or technical change.

9-Logging

The CS should log date, time, nature and outcome of all significant events related to identity management (e.g., issuance, vetting, revocation, reactivation, successful and failed authentication events, etc.) and retain such logs securely for at least 6 months after the date of the last entry.

12-Vulnerability Management

Controls such as anti-virus, host based intrusion detection/prevention and host based firewalls should be implemented to reduce the likelihood that malicious code is injected into the host. Network vulnerability scanning with tools like Nessus should be used periodically to check for vulnerabilities associated with network devices.

13-Physcial Security

The CS infrastructure should be located in an area that is segmented from public traffic, maintains access controls to the space and maintains environmental controls that ensures the physical protection of the resources and the availability of the CS.

21-Threat Protection

If some type of compromise of a Subject's password is suspected, the IdP must not include the Silver IAQ in any identity assertions until the password has been reset successfully by the identity Subject.

- If an Identity Subject's password has been compromised, the Identity Subject should be immediately notified.
- If a credential verifier detects 10 or more successive failed attempts to submit an authentication secret for a given credential within 10 minutes, this could indicate a brute force attack on the Subject's credential.3 In this case CA should take at least one of the following steps:
    i. The credential verifier shall insert a 30 second delay before acting on

password submission from that IP address until verification is successful. If the failed attempts continue for more than 48 hours, the Subject shall be notified and required to reset her or his password; or

ii. The CS shall not include the LOA-2 in identity assertions for this Subject until the Subject resets her or his password (LOA-1 still may be included); or

iii. Lock out use of this Identity Subject's account until the Subject resets her or his password.

28-Password Policy (Entropy)

The following identifies an example of password controls to comply with ensuring password entropy:

- Be a minimum of eight (8) characters in length
- Contain at least one (1) character from three (3) of the following categories:
    - Uppercase letter (A-Z)
    - Lowercase letter (a-z)
    - Digit (0-9)
    - Special character (~`!@#$%^&*()+=_-{}[]\|:;”’?/<>,.)
- Passwords chosen must not contain a common proper name, login ID, email address, initials, first, middle or last name or contain three or more consecutive characters.
- Passwords should be reset or the credential reverted to LOA-1 after a total of 1,800 failed logon attempts through the lifetime of the password.
- It is strongly recommended that:
    - Passwords are changed twice per year
    - Each password chosen is new and different

More information about password entropy can be found in Appendix A of the *NIST 800-63-1 Electronic Authentication Guideline*.

32- Remote Identity Proofing

The RA should establish the applicant's registration identity based on possession of at least one valid Government ID number (e.g. a driver's license or passport) and either a second Government ID number or (1) a student or employee ID number; or (2) a financial account number (e.g., checking account, savings account, loan or credit card); or (3) a utility service (e.g., electricity, gas, or water) account number.

The RA should verify other information provided by applicant using both of the ID numbers above through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, date of birth, address and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual.

The RA should send notice to an address of record confirmed in the records check and receive a mailed or telephone reply from applicant; or the RA should issues credentials in a manner that confirms the address of record supplied by the applicant, for example by requiring applicant to enter on-line information from a notice sent to the applicant; or the RA should issues credentials in a manner that confirms ability of the applicant to receive telephone communications at telephone number or e-mail at e-mail address associated with the applicant in records. Any secret sent over an unprotected channel shall be reset upon first use.

33- In-Person Identity Proofing

The RA should establish the applicant's IdMS registration identity based on possession of a valid current Government Picture ID that contains applicant's picture, and either an address or nationality (e.g., driver's license or passport)

The RA should inspect the photo-ID, compare picture to applicant, record the ID number, date of issuance and expiration, address and date of birth. If ID appears valid and photo matches applicant then: If ID confirms address of record, authorize or issue credentials and send notice to address of record; or if ID does not confirm address of record, issue credentials in a manner that confirms address of record.

36 – Delivery Confirmation

In order to confirm delivery a letter may be sent to the physical mailing address of record; an email sent to a valid, confirmed email address; or available to the identity subject through a history page that is accessible to only the RA and identity subject.

Appendix D: Changes to Assessment Tool

The following table identifies changes to the self-assessment questioner based on changes in the NIST 800-60 and InCommon IAP standards.

Requirement	Action	Description of Change
1c-Authority and Responsibility	Deleted	Does the institution understand and comply with any legal requirements incumbent on it in connection with the CS function (e.g. FERPA, other)?
2b-General Disclosure	Modified	added: "that may impact the identity subject"
9c-Logging	Deleted	Are system logs (e.g. operating system, change management) logs archived for 12 months?
10b-Configuration Management	Added	Are system logs (e.g. operating system, change management) logs archived for 6 months?
12a-Vulnerability Management	Modified	Changed content from anti-virus software to vulnerability management.
12b-Vulnerability Management	Modified	Changed content from anti-virus software to vulnerability management.
13-Physical Security	Modified	Changed "entry controls" to "access controls"
16-Secure Channel	Modified	Changed wording from "across open network" to "end-to-end secure communications".
19b-Stored Secrets	Removed	Alternative Methods
20a-Password Sharing	Modified	Changed "individuals" to "Identity Subjects"
20b-Password Sharing	Modified	Changed "individuals" to "Identity Subjects"
20c-Password Sharing	Added	Are records maintained that confirmations that identity Subjects understand and will comply with the policy?
21b-Threat Protection	Modified	Changed eavesdropper attacks with "on-line guessing and replay attacks"
22a-Protocal Types	Modified	Removed Tunneled Password (this is for LOA-1 not LOA-2). Added Evidence of compliance statements to describe Tunneled password and Zero knowledge.
23a-Approved Cryptography	Modified	Re-worded
23b-Approved Cryptography	Modified	Re-worded
26b-Uniqueness	Modified	Identified that this requirement pertains to identities for LOA-2.
26d-Uniqueness	Added	Added based on a change in InCommon.

Requirement	Action	Description of Change
30c-Records	Modified	Included identity proofing document number, described address of record.
32a-Remote Proofing	Modified	Added utility service
36-Delivery Confirmation	Modified	Clarified the cell phone is a legitimate method of contact.
Part 5: Status Management	Modified	Modified title to be Credential Store Availability.
37-Credential Status	Modified	Modified title to be Credential Store Availability.
Appx A: Glossary of Terms	Added	Added Replay Attack
Appx C: CAF Information	Moved	Moved to Appx E
Appx C: Suggested Compliance Techniques	Added	Content added
Appx D; Changes to Assessment Tool	Added	Content added
Appx E: CAF Information	Added	Formerly Appx C

Appendix E: Information About the CAF

The following is information that was published with the original CAF Survey from April 2007.

Credential Assessment Framework (CAF) for SFS

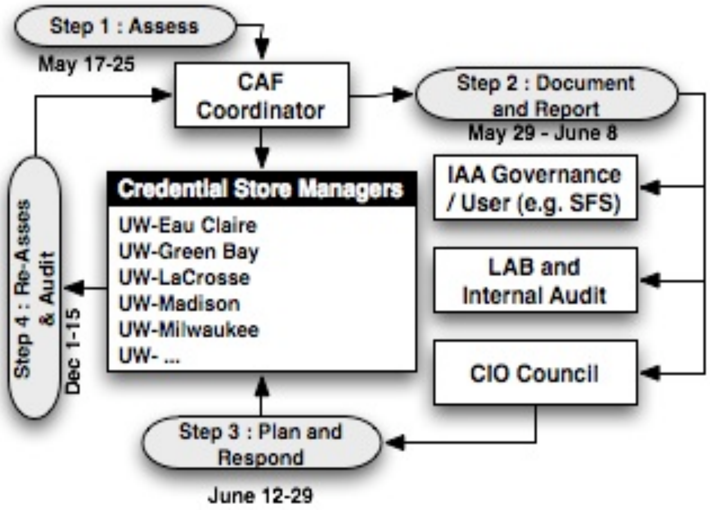
It is important for applications, such as the Shared Financials System SFS, that store and propagate restricted data, to have a high-level of assurance for user authentication. This includes how credential stores are secured. SFS is considering migrating to the IAA Auth Hub. This will require a Level of Assurance (LOA) that minimally provides confidence that the asserted identity is accurate, password complexity is established in all *Credential Stores* (CS) and that there are technical controls and procedures implemented for securing each *Credential Store*. This level can be determined through a Credential Assessment Framework (CAF). CAF is based on standards that identify security controls and procedures specific to credential stores. Assessing the credential stores will identify the current LOA and provide a roadmap for establishing the compliance with the LOA for applications like SFS.

Benefits of CAF

- Identifies the current assurance level of each campus.
- Identifies the combined assurance level of the IAA Auth Hub.
- Identifies and prioritizes actions to comply with standards for establishing a high assurance level.
- Increase security of the applications that use the IAA Auth Hub.
- Increase participation of campuses federating with other entities.

Levels of Assurance (LOA)

The National Institute of Standards (NIST) created a document titled *Electronic Authentication Guidelines*. The document covers guidelines for remote authentication of users over open networks. Based in this document, technical requirements are defined for three levels of assurance in the areas of identity proofing, tokens (passwords) and authentication protocols. These levels are based on the type of data being stored and propagated. These guidelines, along with the work in the higher education community (InCommon), have established a baseline for assessing credential stores and complying with these levels.



The CAF Process

1. ***Assess***: The CAF Coordinator (a person coordinating the entire process) will coordinate an assessment of each campus's credential store based on InCommon's *Credential Assessment Framework* and NIST's *Recommended Security Controls* and *Restricted Data Security Baseline Standards*. The assessment will be conducted via a web survey tool.
2. ***Document and Report*:** The CAF Coordinator will report the current level of assurance, security controls and procedures specific to each campus's credential store. The report will be distributed to the CIO Council, the IAA Governance Group and the appropriate applications such as <APPLICATION NAME>, and available to auditors upon request.
3. ***Plan and Respond***: The CIO Council will provide direction, prioritize and identify resources for complying with standards that are not being met.
4. ***Re-Assess & Audit*:** This CAF Coordinator will lead a re-assessment and audit of current controls and provide a compliance status report to the CIO Council, the IAA Governance Group and the appropriate applications such as <APPLICATION NAME>, and available to auditors upon request.