InCommon Bronze and Security

IAM Online
October 15, 2014

Todd Haddaway, University of Maryland Baltimore County
Sharon Welna, University of Nebraska Medical Center
Ann West, Internet2
Thank you to InCommon Affiliates for helping to make IAM Online possible

Brought to you by Internet2’s InCommon in cooperation with the Higher Education Information Security Council
InCommon Assurance Program

Ann West, Associate Director, InCommon
Federated Transactions

Services Relying on External Identities:
- I need to trust you to manage online identities for me?
- What are my risks?
- What are the odds and the degree of harm?

Parties need agreed-upon criteria for identity assurance

We have MFA, Why Worry About Passwords?

- Do you use passwords to protect sensitive data?
- Not every risk is about phishing...

Strategy and choices

- Use stronger credentials where you can
- Improve passwords until you no longer need them
InCommon Identity Assurance Profiles

1. Business, Policy and Operational Criteria
2. Registration and Identity Proofing
3. Credential Technology
4. Credential Issuance and Management
5. Authentication Process
6. Identity Information Management
7. Assertion Content
8. Technical Environment
Provenance: InCommon Profiles

- US Government FICAM
  - Based on NIST 800-63
  - Assesses comparability

- Profiles
  - Developed for HE
  - Address FICAM requirements with HE flexibility
Due Diligence

- What standard do you use now?
Purpose

How has bronze contributed to the UNMC Security Program?
Agenda

Introduction
UNMC Identity Management Program
Why obtain bronze certification?
Next steps
Sharon Welna

Information Security Officer
Associate Director
Information Systems Compliance and Project Planning

Academic Medical Center
500 mile wide campus
Where are we located
Clinical enterprise

• 2 hospitals
• 39 clinics
• 3 faculty practice plans

• OUT OF SCOPE FOR FEDERATION
Academic enterprise

College of Nursing
College of Pharmacy
College of Medicine
College of Dentistry
College of Public Health
Graduate College
Allied Health School
Eppley Cancer Institute
Monroe Meyer Institute
Research enterprise

Research Expenditures $129.3 Million
Nebraska Strategic Research Initiative (NSRI)
Research enterprise

Major Research Programs

– Gastrointestinal Cancer (SPORE)
– Mass Spectrometry in Clinical Diagnosis of Nerve Agent Exposure
– The Molecular Biology of Neurosensory Systems (COBRE)
– Nebraska Center for Cellular Signaling
– Nebraska Center for Nanomedicine
– Nebraska Research Network in Functional Genomics (INBRE)
– Nebraska Regenerative Medicine Project
– Neural Immunity in HIV Dementia
– Proteomic Strategies for AIDS and Drug Abuse - HIV and METH CNS Synergy
– Staphylococcal Biofilm and Disease
– Chronic HIV Infection and Aging in NeuroAIDs (CHAIN) Center
### Campus Growth

<table>
<thead>
<tr>
<th>Year</th>
<th>Networked Devices (active network ports)</th>
<th>Wireless Access Points</th>
<th>Enterprise Mobile Devices</th>
<th>Classroom Technology Spaces</th>
<th>UNMC FTE</th>
<th>ITS FTE</th>
<th>Building Growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>7,200</td>
<td>NO Wireless</td>
<td>NO Mobile Devices</td>
<td>17</td>
<td>3,425</td>
<td>120</td>
<td>Campus Expansion Begins +14 bldgs</td>
</tr>
<tr>
<td>2005</td>
<td>11,000</td>
<td>300</td>
<td>Beginning</td>
<td>89</td>
<td>3,483</td>
<td>120</td>
<td>+32 bldgs</td>
</tr>
<tr>
<td>2010</td>
<td>16,000</td>
<td>1,000</td>
<td>500</td>
<td>150</td>
<td>4,120</td>
<td>120</td>
<td>+34 bldgs</td>
</tr>
<tr>
<td>2011</td>
<td>22,000</td>
<td>1,400</td>
<td>1,224</td>
<td>171</td>
<td>3,915</td>
<td>121</td>
<td>+34 bldgs</td>
</tr>
<tr>
<td>2013</td>
<td>28,500</td>
<td>2,400</td>
<td>6,597</td>
<td>196</td>
<td>4,108</td>
<td>121</td>
<td>+34 bldgs</td>
</tr>
</tbody>
</table>

### Building Growth

- 2000: Begins
- 2010: +14 bldgs
- 2011: +32 bldgs
- 2013: +34 bldgs

---

... unprecedented enterprise expansion for UNMC and its healthcare partners
Why IDM now?

Enterprise growing dramatically

- 8 new buildings
- 1,000 new accounts to manage
Fred and Pamela Buffett Cancer Center
IDM project goals

Improve the process
  – Not make a perfect process

From operational perspective
  – Be positioned to handle increase in accounts needed without increasing staff
From an ISO perspective

- Need to meet compliance requirements
  - HIPAA, PCI, GLBA, FERPA, NIH, DOD
- Need to simplify user experience by streamlining user id/password
- Ask your users how many user id/passwords they have to manage
- Can not have good security if access control is difficult
Information security shift

Can not manage the device
Have to secure the data
And
Verify the user
UNMC Security Program

Based on SANS Top 20 and NIST framework
Have been audited by Deloitte using the HiTrust Framework
Utilized the Bronze framework to audit the IDM program
IDM Program

Formed a Steering Committee chaired by CIO

Key Decisions

- Adopt federation
- Utilize 389DS
- Utilize Shibboleth

Project would be accomplished with existing staff and low expenditure of funds
IDM Program

Formed a Technical Committee

- Information Security Officer
- Application Director
- Technical Architect
- IDP analyst
- SP Analyst
- IDM Analyst
- Access Control staff
Steps followed

Performed a gap analysis based upon the template documents provided.
Work required: Verify vetting process

Formed an IDM Advisory Committee

- Information Security Officer
- Human Resources Hiring Officer
- Compliance Officer/HIPAA Privacy Officer
- Risk Manager
- Vice Chancellor Academic Affairs

Who is on campus and why?
What are prerequisites to obtain an account?
Work required: Clearly define your account terms
**UNMC Identity Management**

<table>
<thead>
<tr>
<th>UNMC LDAP (Provides access to the following if role requires access)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blackboard</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UNMC NETID</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetID created automatically</td>
</tr>
<tr>
<td>UNMC Faculty, Staff, emeritus faculty, and Registered Students</td>
</tr>
<tr>
<td>AD: Department OU</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UNMC Affiliate NETID</th>
</tr>
</thead>
<tbody>
<tr>
<td>People affiliated with UNMC — ID requested by a sponsor</td>
</tr>
<tr>
<td>Contractors/consultants, INBRE, IRB/IACUC/IBC/Grant participants, Seguidor, temp workers, visiting faculty/students, residents, volunteers, vendors (on-campus),</td>
</tr>
<tr>
<td>AD: Department OU</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UNMC Associate NetID</th>
</tr>
</thead>
<tbody>
<tr>
<td>People — ID is requested by a sponsor.</td>
</tr>
<tr>
<td>Includes Vendor (off campus), IACUC Committee, GRASP (Grants, Research &amp; Special Projects) such as TIPS and Redcap</td>
</tr>
<tr>
<td>AD: Remote Accts OU</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Accounts (ADO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not People—Requested by workstation</td>
</tr>
<tr>
<td>Includes accounts for test, equipment, applications, and auto login</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UNMC GUEST ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>People External to UNMC — The ID is requested by a individual</td>
</tr>
<tr>
<td>Includes courtesy faculty, volunteer faculty, preceptors, Blackboard students, IRB application submission and International observers.</td>
</tr>
<tr>
<td>(NOTE: Account should not be granted if home organization has the capability of federated access)</td>
</tr>
</tbody>
</table>

**Temporary Account Access for Former Students**

[Diagram with UNMC AD (Provides access to the following if role requires access) - UNMC Network drives and printers, One Chart, Wireless network, Email in certain cases.]
Close all the doors

Worked closely with parking and the badge office to ensure access is granted with the same rules as those defined by the IDM Advisory Committee for electronic access
Work required: Implement the account criteria

Establish systems of truth

• Employees must be in SAP
• Students must be in PeopleSoft
• Others must be in campus inhouse system
Why certify?

- Framework which could be used to audit the IDM program
- Identified the work required to close the gaps
  - Work required to close the gap identified things we SHOULD do anyway
- Why not certify since work was completed?
Next projects

Improve self service password reset process

Implement identified changes needed for silver certification
  – Have not moved forward and do not plan to move forward at this time

Remember…this is a journey not a project
Our Experience in Obtaining InCommon Bronze Certification
UMBC Facts

- Medium-sized research institution located outside of Baltimore and 30 minutes north of Washington, DC
- 14,000 Students
- U.S. News #1 Up-And-Coming National University
- #6 Nationally in undergraduate teaching
- UMBC: Undefeated football team since 1966
IAM Staff
- VP / CIO Jack Suess
- IAM Director
- IDMS
- Single Sign On

On the Periphery
- Audit and Compliance
- CISO
IAM History

Mostly homegrown legacy code and systems.
• 2000 – Selected as part of Internet2 early adopter program for “middleware”
• August 2000 – Created and launched our own WebISO
• 2005 – Participated in the federal government EAUTH program began moving to 800-63 for passwords
• 2006 – We joined InCommon and started using federation
• 2005/2006 – We extended our WebISO to support multi-factor as part of a grant activity run by a faculty member
• 2010 – Retriever Community System documented
• 2014 – Signed up to participate in the TIER program
Retriever Community System

Document addresses account lifecycle, sponsored accounts, levels of assurance, etc.

1. What is Retriever Community?

Retriever Community is the centralized, enterprise-wide identity management system that stores identifying information about people who are, or were, affiliated with UMBC, whether their affiliation is temporary, such as a summer program participant, or permanent, such as a student or faculty member. It associates identifying information about each person with a myUMBC username that allows its owner to access UMBC-wide and departmental computing resources commensurate with their role within the UMBC community. It also manages and preserves the online identity of UMBC students, faculty, staff, alumnae, emeritus faculty and staff, contractors, visitors, or guests.

Retriever Community consists of the various procedures, technological controls, and IT systems that assure that individuals with an interest in or connection to UMBC can access online computing resources while protecting those resources from unauthorized use.

It is a flexible, centralized, identity management system that enables UMBC departments and offices to provide access to information technology resources and services for their staff or customers by relying on the individual’s established UMBC identity. The Division of Information Technology (DoIT) is responsible for the Retriever Community identity management system.
Why UMBC is Interested in Bronze / Silver Assurance Profiles

Benefits of Assurance
Why Bronze vs. Silver
Why UMBC is Interested in Bronze / Silver Assurance Profiles

Benefits of Assurance

• Identity management is absolutely essential to campus cyber security
• Bronze and Silver represent consensus best practice
• Future-proofing our practices to support new and evolving needs
• Formalize and document what we are already currently doing
• Understanding where we need to improve
• Preparation for legislative auditors

Why Bronze vs. Silver
Why UMBC is Interested in Bronze / Silver Assurance Profiles

Benefits of Assurance

Why Bronze vs. Silver

- Simplified Bronze — Just sign the agreement and go. No audit required.
- UMBC generally believes it complies with Silver. Haven’t had the opportunity to schedule the audit.
Journey to Bronze

Understanding the IAP
Evaluating where we were
Determining what was left to do
The final bronze submission process
Journey to Bronze

Understanding the IAP

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Criteria</th>
<th>Bronze</th>
<th>Silver</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.1 Business, Policy and Operational Criteria</td>
<td>1. InCommon Participant</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>2. Notification to InCommon</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>3. Continuing Compliance</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>4. IdPO Risk Management</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>4.2.2 Registration and Identity Proofing</td>
<td>1. RA Authentication</td>
<td>n/a</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>2. Identity Verification Process</td>
<td>n/a</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>3. Registration Records</td>
<td>n/a</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>4. Identity Proofing</td>
<td>n/a</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>4.1 Existing Relationship</td>
<td>n/a</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>4.2 In-person Proofing</td>
<td>n/a</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>4.3 Remote Proofing</td>
<td>n/a</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>5. Address of Record Confirmation</td>
<td>n/a</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>6. Protection of Personally Identifiable Information</td>
<td>★</td>
<td>★</td>
</tr>
</tbody>
</table>

Evaluating where we were
Determining what was left to do
The final bronze submission process
Journey to Bronze

Understanding the IAP

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.

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.

4.2.2 REGISTRATION AND IDENTITY PROOFING
Identity proofing in this IAP uses verified information to create a record for the Subject in the IdPO’s IdMS.

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 Approved Algorithm that also authenticates the IdMS platform.

Evaluating where we were
Determining what was left to do
The final bronze submission process
Journey to Bronze

Understanding the IAP
Evaluating where we were

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Area</td>
<td>Criteria</td>
<td>Description</td>
<td>Needed for Bronze</td>
<td>Needed for Silver</td>
<td>UMBC Meets</td>
<td>Notes</td>
<td>Link 1</td>
</tr>
<tr>
<td>32</td>
<td>4.2.6 Identity Information Management</td>
<td>.1 Identity Record Qualification</td>
<td>√</td>
<td></td>
<td>√</td>
<td><a href="#">IDM Silver Certification Overview</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
<td><a href="#">IDM Silver Certification Overview</a></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>4.2.7 Assertion Content.</td>
<td>.1 Identity Attributes</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td><a href="#">IDM Silver Certification Overview</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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 (In-C-AtSum).</td>
<td></td>
<td></td>
<td></td>
<td><a href="#">IDM Silver Certification Overview</a></td>
<td></td>
</tr>
</tbody>
</table>

Determining what was left to do
The final bronze submission process
Journey to Bronze

Understanding the IAP
Evaluating where we were
Determining what was left to do
  • Kerberos upgrade
  • Document, document, document – adding some specific items to the Retriever Community System.

The final bronze submission process
Journey to Bronze

Understanding the IAP
Evaluating where we were
Determining what was left to do
The final bronze submission process

• Took one last verification pass
• Created a document outlining how UMBC met each requirement
• Filled out and submitted the Bronze application
Planning for Silver

What Remains to be Done?

• Documentation fine tuning
• Audit

Selecting an Auditor

• Making use of our University Systems of Maryland (USM) auditors.
And now for something completely different...

Duo second-factor authentication

- IAP 4.2.3.2: Basic resistance to guessing authentication secret
- Duo tied to web single sign on
- Required enrollment for employees with access to sensitive data
- Others have option to self-enroll
Resources and URLs

- Retriever Community System
- Spreadsheet used to track IAP progress
- Duo resources
Questions?
Assurance Update

- Federal Gateway
  - Hub and Spoke
  - Citizen-to-Government
- GSA Joined InCommon
  - Coordination point for Agencies
  - Business-to-Government
- NIH and NSF
  - Research & Scholarship Category
  - Bronze plus “ish”
Questions? Answers.
Framework and Profiles

Identity Assurance Assessment Framework
www.incommon.org/docs/assurance/IAAF.pdf

Identity Assurance Profiles: www.incommon.org/docs/assurance/IAP.pdf

Resources

Monthly Call: First Wed of the month – Noon ET
Website, discussion list and implementers wiki: assurance.incommon.org

Community Contribution – AD Silver Cookbook
spaces.internet2.edu/display/InCAssurance/AD+Silver+Cookbook

Research & Scholarship Category: https://spaces.internet2.edu/x/-IKVAQ
Evaluation

Please complete the evaluation of today’s webinar

Register today for the Technology Exchange

REFEDS, Advance CAMP, CAMP

See the CAMP 101 and CAMP 201 schedules here:
http://www.incommon.org/techex2014.html

October 26-30, 2014 - Indianapolis, Indiana

Complete Technology Exchange information here:
http://events.internet2.edu/2014/technology-exchange/
InCommon Shibboleth Installation Workshops
Single Sign-on and Federating Software

November 10-11 – University of Utah – Salt Lake City

Details and registration at www.incommon.org/shibtraining
Thank you to InCommon Affiliates for helping to make IAM Online possible

Brought to you by Internet2’s InCommon in cooperation with the Higher Education Information Security Council