TN - Levels of Assurance

1) There is a need for a formal process to assess the severity of the risk and exposure that results when an SP is accessed using a stolen credential.

The existence of this process, the model it is based on, and the process for using it to evaluate a specific SP needs to be communicated to IT staff, business owners, and the security group.

-- education needed for everyone (IT staff included) that just because two systems use passwords doesn't mean they're comnparable on LoA

-- important role of auditors was noted

2) Do campuses currently have any relevant policies or frameworks ?

-- campuses have policies related to abusive behavior; some campuses have data-driven policies (ie data owner responsible for classifying data)

3) Are there other approaches in wide use to assessing risk at an SP ?

-- OMB 04-04 describes a framework for assessing the impact at an SP of an "Authentication Error" (ie someone using a stolen identity).

http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

which is the foundation for the US Federal government's work on risk and Levels of Assurance.

Section 2 contains useful suggestions on how to assess risk. It identifies several categories of harm or impact:

Inconvenience, distress or damage to standing or reputation
Financial loss or agency liability
Harm to agency programs or public interests
Unauthorized release of sensitive information
Personal Safety
Civil or criminal violations

For each of these categories, it provides a definition and examples of low, moderate, and high impacts.

It also provides guidance on mapping low, medium, and high risk in these categories to an appropriate required LoA.

Table 1 – Maximum Potential Impacts for Each Assurance Level (from OMB 04-04)

Assurance Level Impact Profiles				
Potential Impact Categories for Authentication Errors	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

4) How is the NIST work applied to this situation ?

Campuses and Service Providers could use the NIST framework to evaluate, for a specific SP and for each category, whether an "Authentication Error" would create a Low, Moderate, or High Impact situation. They would then use Table 1 above to determine the minimum LoA that is required of an Authentication Event in order to access the SP.

5) Is the NIST work relevant to this problem ?

The Consensus is YES, but that its not sufficient.

social identities are at LoA 1 (as decreed by the US government).

Most campus identities are also (currently) at LoA 1 (also referred to as InCommon Bronze; sometimes called "whatever the campus is doing today").

However, there was consensus that a campus-asserted identity was "stronger" than a social identity. Currently, no attempt is made to link a social identity to a real world identity. Campuses do make this effort, and promulgate policies prohibiting the sharing of identities and passwords. Campuses may not be operating at NIST Level 2 (InCommon Silver), but do have have business practice and policy in place to create a "reasonable" assurance about who is using a specific credential.

Implementation Issues

6) LoA is orthogonal to differentiating social vs enterprise identities. SPs won't implement complex algorithms, just a couple of differentiators at this point. Initially, avoid the temptation to provide an SP with too much information.

7) Consensus -- GW should assert both authN source and forward any LoA value that it receives; the application can use application context + whatever algorithm it wants to determine how it wants to treat an incoming Assertion (eg any SP can decide that social + LOA 1 --> treat as LOA 0)

8) Does the GW compute an LoA value ? Should the GW differentiate social, campus bronze, silver in some sort of LoA assertion that it computes ?

Consensus -- NO. Social identities are LoA 1; GW forwards any eduPersonAssurance attributes or Bronze/Silver assertion that it receives. But, it does NOT attempt to compute or derive such a value.

.. as long as the operational characteristics of the GW don't impact LoA that is being presented.

9) some applications might want to know some of the properties of the authentication event, separate from LoA (eg was google 2-factor used)

Let any further categorization emerge from experience and practice...

10) There's also a need to ensure that enough logging is being done, so that forensics are possible, and a campus/site manager could take an SP out of service quickly, do the required investigation and recovery/correction, and return the site to service.