## Recommended Additions to the Cloud Controls Matrix for the NET+ Security Initiative

InCommon Assurance Advisory Committee and Technical Advisory Committee

Draft - January 2, 2014

InCommon recommends including controls in the Cloud Controls Matrix to support federated authentication and identity management.

**Justification:**

At the end of 2013, InCommon will have served more than 7.5 million end users in the U.S. with federated identity management.[[1]](#footnote-1) Without federation, the credentials for those users would be managed by the service providers.  Over 400 [InCommon Participants](http://www.incommonfederation.org/participants/%C2%A0)are Identity Providers in Higher Education. These institutions are committed to utilizing federated authentication, and their users are counting on using their institution's local credentials to access services in the cloud. With federation through InCommon, the IdPs are responsible for the security of their users' credentials. Minimal information is released to the relying party to facilitate authentication and to allow the service to make authorization decisions. If needed, the service can require a higher level of assurance in the identity of the person authenticating. Those identities are vetted according to the [InCommon Assurance Program](http://www.incommonfederation.org/assurance/).

Federated authentication will relieve the NET+ services from the security liability of managing end-user credentials. By joining InCommon and agreeing to a common authentication method (based on SAML2), the NET+ services and the IdPs with which they interact also benefit from standard authentication integration. There is no longer the need for one-off integration with each IdP.

Federated authentication also supports the goals of the [Identity Ecosystem Steering Group](http://www.idecosystem.org/) which was formed as part of the [National Strategy for Trusted Identities in Cyberspace](http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf). To be consistent with security provided by trust frameworks in the private, public, and government sectors, Internet2 NET+ services should commit to supporting federated authentication and identity management.

**Recommended Additions:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Domain** | **CCM V3.0 Control ID** | **Control specification** | [**InCommon Identity Assurance Profile Version 1.2**](http://www.incommon.org/assurance/) **Section** |
| Identity & Access Management Credential Lifecycle / Provision Management | IAM-02 |  | 4.2.8.2.2 4.2.7 4.2.4.1 4.2.5.6  |
| Identity & Access Management Diagnostic / Configuration Ports Access  | IAM-03  |  | 4.2.8.2.1 |
| Identity & Access Management Policies and Procedures  | IAM-04  |  | 4.2.8.2 |
| Identity & Access Management User Access Authorization  | IAM-09  |  | 4.2.8.2 4.2.8.3 |
| Identity & Access Management User Access Revocation  | IAM-11  |  | 4.2.8.2 4.2.8.3 |
| Identity & Access Management User ID Credentials  | IAM-12  |  | 4.2.7 4.2.4.1 4.2.5.6 |
| **Identity & Access Management****User ID Credentials** | **IAM-14**  | Wherever possible, identity federation using the SAML protocol shall be used to handle authentication and the passing of identity-related data for authorization purposes.  | 4.2.7.2 [InCommon Assurance Assessment Framework v1.2](http://www.incommon.org/assurance/) describes federated framework and control specifications.  |

1. <https://incommon.org/> [↑](#footnote-ref-1)