**Security and Identity Management (IdM)**

**Accomplishments in Year 1:**

**\* Items are carried over to year 2 workplan**

1. Operations
   1. Various vulnerabilities, actively warning and helping sites: multiple HTCondor vulnerabilities, gsi-ssh, kernel,
   2. Released the Pakiti software in OSG VDT. Sites can use the software to locally monitor their vulnerabilities
   3. SHA-2 transition. Handed off to Software team. Consulting help.
   4. Risk assessments for: CVMFS/Oasis (Accepted by Fermi Security team after several iterations), MD5-SHA-2 proxy certs, proxy lifetime assessment.
   5. Audit requirements for HTCondor team provided.
2. Identity management—CILogon Basic CA \*
   1. OSG IT services (docdb, twiki, ticketing, etc) accepts CIlogon Basic CA for access
   2. Fermi Grid resources accepted CIlogon Basic CA certs vouched by Indiana Univ, U of Chicago, and U of Wisconsin.
   3. Worked with Glow VO, IU CSIU VO to change their submission model to include CIlogon Basic CA \*
   4. MWT2, Purdue, Sprace, Nebraska, BNL decided to accept Cilogon Basic CA certs for access.
3. Identity Management – Traceability of Jobs without Certificates \*
   1. Wrote down site requirements document. Accepted by OSG ET and Fermilab Security Board
   2. Conducted an assessment of Pilot system for tracing jobs without user certificates. Conducted three security exercises with OSG-XSEDE Frontend, Factory, and U of Nebraska Site. The assessment passed the Fermilab security team’s main requirements. \*
4. Identity Management – Surveyed 5 OSG Resource Providers on their consumption of Identity Information. Report is presented to OSG and the Magic meeting.
5. Identity Management – Identity Management Roadmap is completed. Significant contribution from Von. \*
6. Identity Management – Completed OSG PKI Transition

**Plans for Year 2 (New Items Only):**

1. Operations
   1. Smooth transition to SHA-2. Help software and production teams with planning, consulting, tips, etc,
   2. Gather site’s attention to Pakiti service and how they can benefit from this.
   3. Update Security Test and Controls, update the Risk Assessment
   4. Keep up the regular operational work (oversight, risk assessment, incident response, so on)
2. Identity Management—Campus Identities; CILogon Basic CA Adoption
   1. Increase CILogon Basic Adoption.
      1. Create a risk assessment document, updating https://www.opensciencegrid.org/bin/view/Security/CiLogonPilot2010#Risk\_of\_using\_CILogon\_Basic\_CA
      2. Include the Basic CA in default CA distribution.
   2. Identify more VOs who can benefit from Cilogon Basic CACA
3. Identity Management – Traceability of User Jobs without Certificates
   1. Revisit the requirements document
   2. Revisit the assessment document; address i) isolation of jobs; ii) traceability of users; iii) ability to ban users at sites.
   3. Explicitly state the changing trust models
4. Identity Management – Better understand and document how all OSG VOs are using current IdM services today, along with unmet and poorly met needs of those VOs.
   1. Work in collaboration with XSIM OSG Satellite Project to apply and validate their model.
5. Identity Management – Renew DigiCert Contract for Y3+
   1. Form team of stakeholders to provide input to contract
   2. Re-assess OSG certificate needs
6. Identity Management – Conduct survey of OSG PKI satisfaction, make improvements as resources allow.

**OSG Security Team**

* Mine Altunay (FNAL) 70%
* Kevin Hill (FNAL) 80%
* Anand Padmanabhan (NCSA-UIUC) 50%
* Von Welch (IU) 5%