



# Grid Security

Atlas Tier 2 Meeting

Bob Cowles

[bob.cowles@slac.stanford.edu](mailto:bob.cowles@slac.stanford.edu)

August 18, 2006

Work supported by U. S. Department of Energy contract DE-AC03-76SF00515

# Rapidly Changing Environment



- Federal guidelines / mandates
  - FISMA, PIV, PII ...
- Threats
  - Attacks for profit or national interests
  - Targeted, below the radar
- Vulnerabilities
  - Middleware, applications, users

# Recent Events

- Aug 1-7 saw over 120 vulnerabilities announced (before MS announcement)
- Last week, record amount of PII lost
- This week, holes in GTK, VOMS, etc.
- Growing dissatisfaction with insecurely designed, poorly implemented software

# Security by Design

- Security is your friend
  - Sites cannot allow insecure services
  - Users must be able to work in a trusted environment
- Requires attention in architecture, design, coding, deployment, patching
  - Also logging, version control and lower level dependencies (OS & middleware versions)

# Design Examples

- Mutually authenticate with services
  - Avoid rogue providers
  - Cut off “black hole” sites
  - Validate service requests
- Log resource allocation decisions
- Failover for critical services
- Ease of patching and recovery
- Remove OS & MW version dependencies

# SLAC – Atlas Experience

- Web Server open to the world (needed?)
  - Only SL supported
- MySQL server open to Internet
- Google indexed userid/password
  - Admin privileges on MySQL
- New GTK + VDT rolling out – how will that affect Atlas?

# User AUP Goals

- Short enough for people to read and understand
- No requirement for “incidental use” provisions
- Remove burden on user of knowing use policies for all sites
- Site computer security personnel feel provisions are sufficient

# User AUP Infrastructure

- Each VO is expected to have members agree to terms
- VO must clearly state goals and policies
- RPs evaluate VOs accepted to ensure acceptable goals & policies

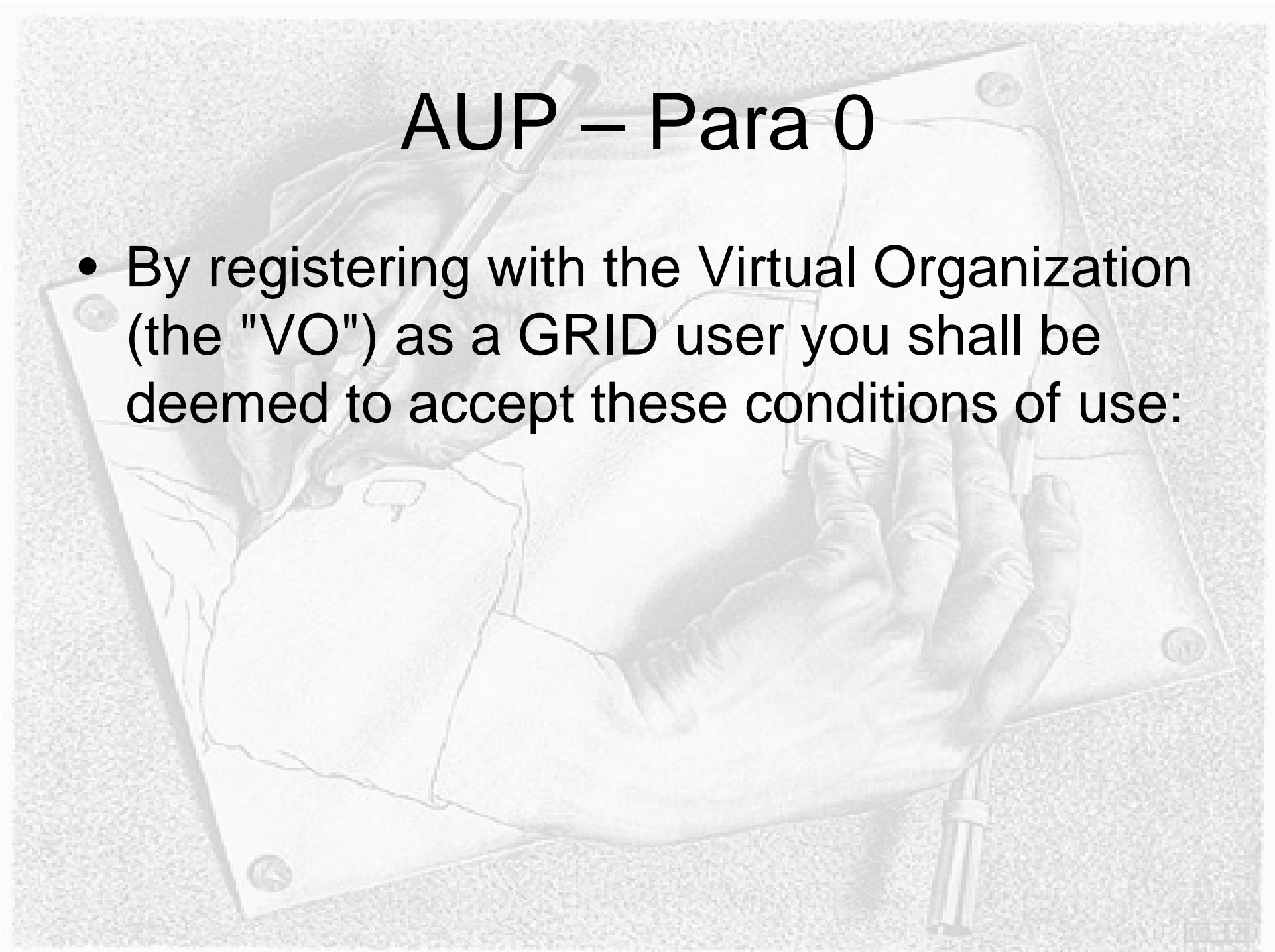


# User AUP

- Initially four paragraphs
- However, needed to pass it by some lawyers (three lawyers consulted)
- Added more scary language but managed to retain the essence of the Taiwan accord
- New AUP is seven paragraphs

# AUP – Para 0

- By registering with the Virtual Organization (the "VO") as a GRID user you shall be deemed to accept these conditions of use:



# AUP Para 1

1. You shall only use the GRID to perform work, or transmit or store data consistent with the stated goals and policies of the VO of which you are a member and in compliance with these conditions of use.

## AUP Para 2

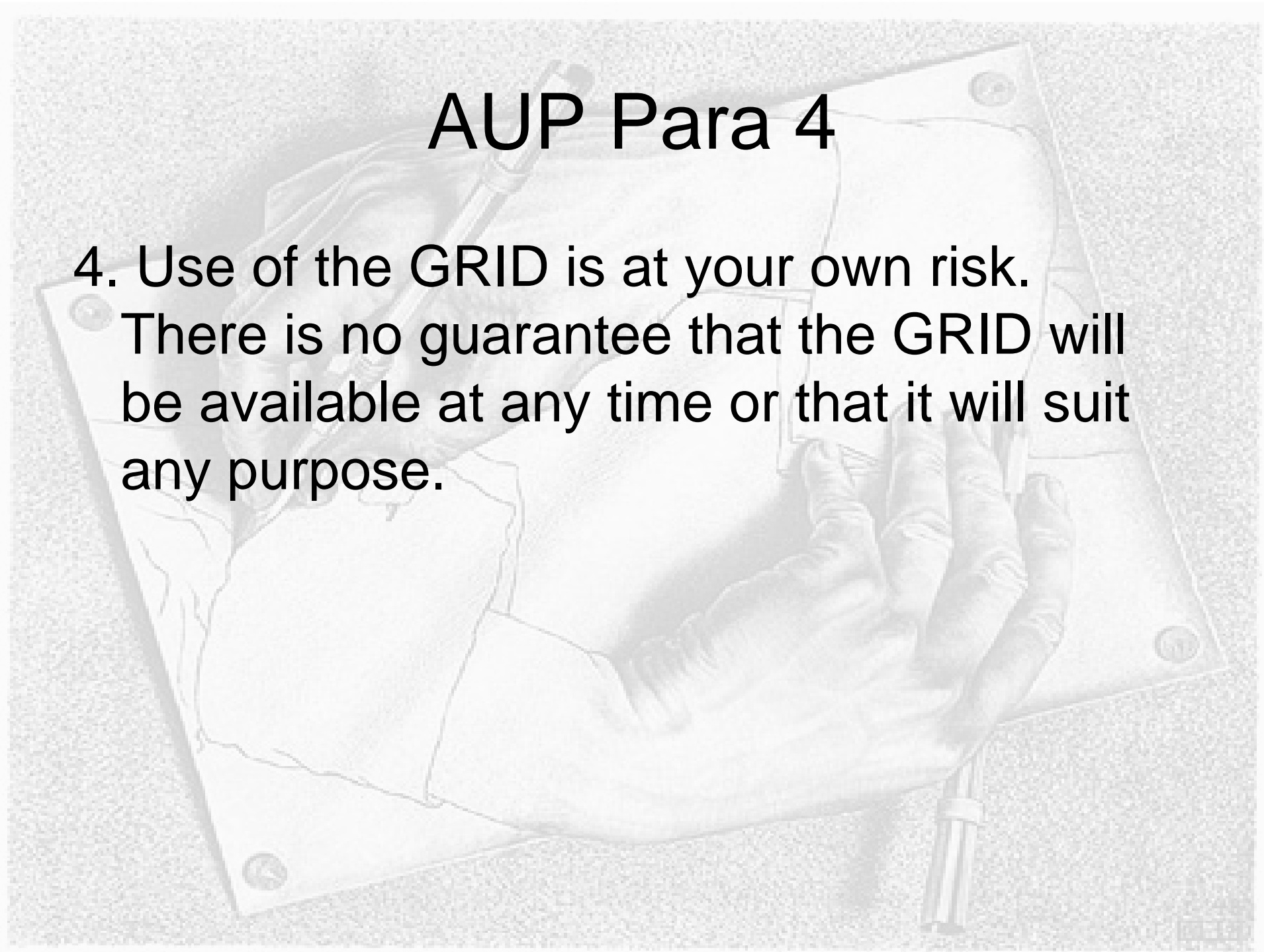
2. You shall not use the GRID for any unlawful purposes and not (attempt to) breach or circumvent any GRID administrative or security controls. You shall respect copyright and confidentiality agreements and protect your GRID credentials (e.g. private keys, passwords), sensitive data and files.

# AUP Para 3

3. You shall immediately report any known or suspected security breach or misuse of the GRID or GRID credentials to the incident reporting locations specified by the relevant VO(s) and to the relevant credential issuing authorities.

# AUP Para 4

4. Use of the GRID is at your own risk. There is no guarantee that the GRID will be available at any time or that it will suit any purpose.



## AUP Para 5

5. Logged information, including information provided by you for registration purposes, shall be used for administrative, operational, accounting, monitoring and security purposes only. This information may be disclosed to other organizations anywhere in the world for these purposes. Although efforts are made to maintain confidentiality, no guarantees are given.

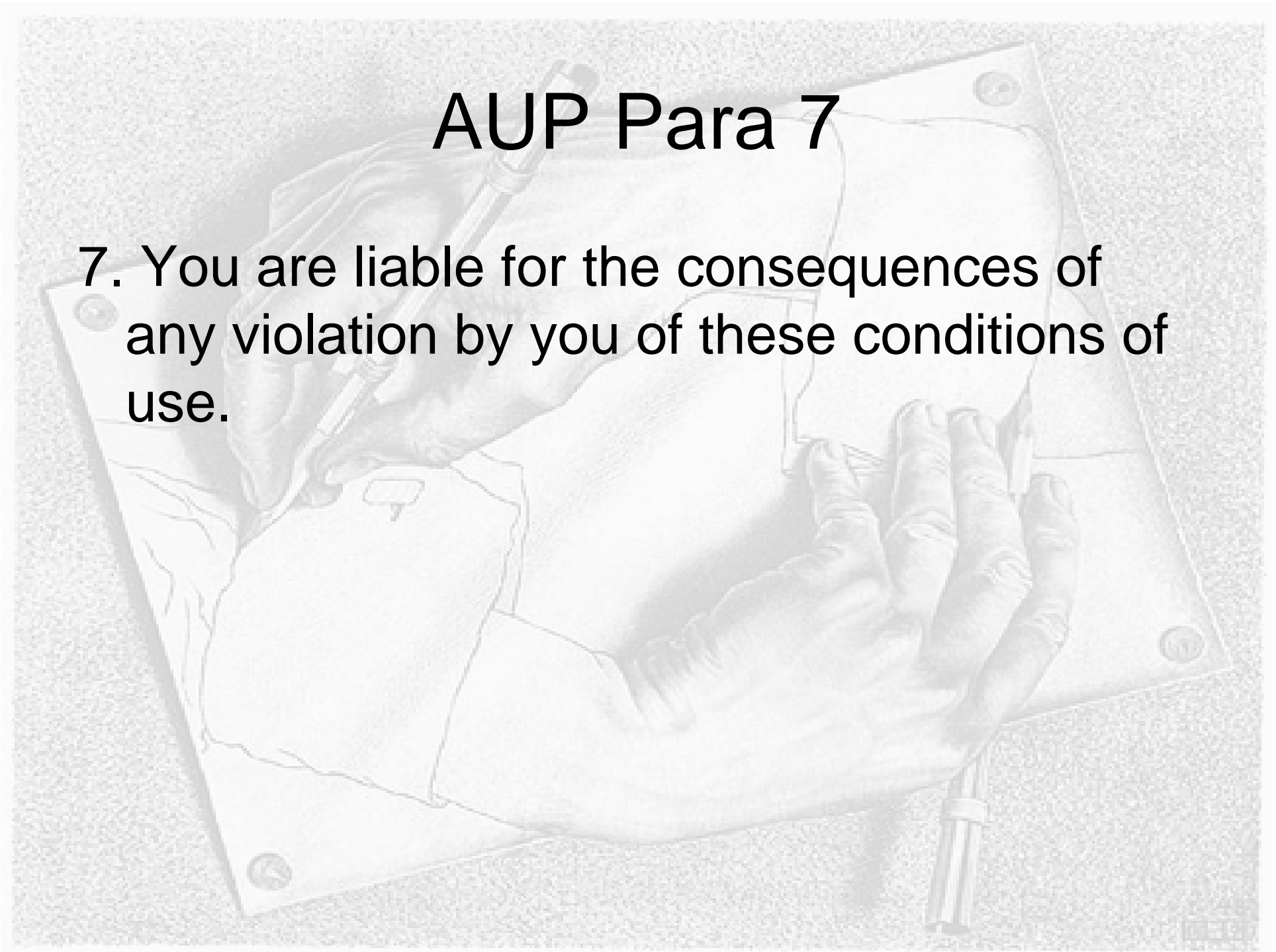
## New AUP Para 6

6. The Resource Providers, the VO and the GRID operators are entitled to regulate and terminate access for administrative, operational and security purposes and you shall immediately comply with their instructions.



# AUP Para 7

7. You are liable for the consequences of any violation by you of these conditions of use.



# VO Registration

- Define purpose
- Supply contact information
- Location of servers
- Certify all users have accepted grid AUP
- Responsive to complaints
- Mutual acceptance between VOs and Resource Providers

# Service Agreement

- Advertise services accurately, make limitations known. Do not try to circumvent controls.
- Not interfere with other resources. If problem, investigate & resolve
- Responsible for selecting appropriate VOs to offer resources to
- Take reasonable care with entrusted credentials.
- Participate in incident response activities.
- <http://osg-docdb.opensciencegrid.org/0000/000087/004/OSG-ServiceAUP-V104.pdf>

# OSG Security People

- Don Petravick in Facility:
  - OSG Facility Security Officer.
- Bob Cowles in Extensions:
  - Responsibilities to GGF, TAGPMA,
  - New Security CS developments for SciDAC-2
  - EGEE middleware meetings etc.

# OSG Draft Security Plan

- Additions to what we have been doing in OSG to date:
- An OSG Facility (OSGF) security cyclical process including:
  - Enumeration of OSGF assets
  - Consideration of threats to them, and vulnerabilities.
  - Implementation of controls to reduce risk to acceptable level,
  - Monitoring the controls to assess their effectiveness.
- Will be reading EGEE documents for input.

# Security Infrastructure

- Security infrastructure improvements of interest:
  - Better handling of CRL functionality
  - Respond expeditiously to identified VDT vulnerabilities
  - Think about how to do some spot audits
  - Deployment of glide-in and pilot jobs –
    - Certificate delegation & identity control more important.
    - Compatible use of glExec with EGEE

# JIT Workload Management

- ATLAS (PanDA) and CDF (GlideCAF) submit “pilot jobs” on OSG with an “administrator” rather than a “user” credential.
- Once the pilot is launched in a site’s batch slot, it pulls a workload according to VO priorities at launch time.
- This violates the security policies at sites that require knowledge & control over who runs arbitrary user code at their site.
  - CDF agreed with FNAL to find solution by August 2006

# Solution – Minimal Proposal

- VO Responsibility:
  - Pilot job calls “home” to obtain user credential for job to run.
  - Pilot job presents user credential to site service.
  - Pilot job does NOT directly run user jobs
- Site Responsibility:
  - Trust VO to play by the rules.
  - Allow VO to call “home” in a secure way (i.e. VO admin credentials available to pilot job).
  - Site service accessible to pilot job from all worker nodes.
  - Site service interfaced with OSG authz infrastructure.
  - Site service switch UID context to prevent user apps access to VO admin credentials



# Security for Open Science Center for Enabling Technology

Lead PI - Deb Agarwal, Lawrence Berkeley National Laboratory

-

Lawrence Berkeley National Laboratory - Brian Tierney, Mary  
Thompson

Argonne National Laboratory - Frank Siebenlist, Ian Foster

Pacific Northwest National Laboratory - Jeff Mauth, Deb Frincke

University of Illinois, NCSA - Von Welch, Jim Basney

University of Virginia - Marty Humphrey

University of Wisconsin - Miron Livny, Bart Miller

National Energy Research Scientific Computing Center - Howard  
Walter

Energy Science Network - Michael Helm

University of Delaware – Martin Swany

# Topic Areas

- Auditing and forensics
  - Services to enable sites, communities, and application scientists to determine precisely *who did what, where and when*.
- Dynamic ports in firewalls
  - Services to open and close ports dynamically for applications while enforcing site policy.
- Identity management
  - Services to seamlessly manage identity and access control across sites and collaborations, and to allow for rapid response to security incidents.
- Secure middleware
  - Services to proactively find and fix software vulnerabilities and guarantee deployed security software is current and correctly configured.

# Auditing/Forensics

- High-Level Approach:
  - An end-to-end auditing infrastructure which uses a policy language to allow resource (both systems and data) owners specify where auditing information may be published and who may access the audit logs.
- Components
  - Logging software (instrumentation) - Applications call easy-to-use libraries to log events with detailed information.
  - Normalizers – Agents transform existing logs so that they can be incorporated into the common schema of the audit system.
  - Collection sub-system (forwarder) – Audit logs are collected by a dependable, secure collection system.
  - Repository (database, publisher) – Audit logs are sent over the network, normalized, and archived. Then they are made available through a query interface.
  - Forensic tools (analysis) – Forensic tools query and process the audit data to find problems and answer questions.

# Firewall Ports

- High-level Approach:
  - Tools and services to dynamically open and close ports needed by applications and middleware based on authentication and authorization
- Components
  - *Configuration Broker* maintains the overall state of the firewall configuration for the site, validates user credentials, and verifies that requested actions are consistent with site policy restrictions.
  - *Firewall Agent* interacts with the existing site firewall systems, receiving direction from the Configuration Broker.
  - The *Validation Service* receives information about the completed firewall changes and continually analyzes network traffic to insure there are no errors in the firewall configuration.
  - The *Programming API* is the mechanism for software to make requests to the broker.

# Identity Management

- Near Term Approach:
  - Build on existing solutions:
    - VOMS, CAS, GUMS, MyProxy, GSI, OCSP
  - Integrate and deploy, e.g.
    - Deploy OCSP service; client support in GT, MyProxy, etc.
    - VOMS support in GridFTP, MyProxy
    - GUMS callout into GT, MyProxy
- Longer term:
  - XKMS support to ease configuration management
  - Integrate data access control policy with work on semantic workflows
  - PKCS 11 support
  - Ubiquitous hooks in middleware for site security integration
    - E.g. Kerberos, auditing,

# Secure Middleware

- Problem
  - Grid middleware has become essential to science
  - Security of this infrastructure is an essential consideration
- Approach - steps
  - *Architectural analysis* to understand the system level view of a middleware component and its external interactions
  - *Identify trust boundaries/threat model* to understand the dependencies and areas of concern
  - *Component and system analysis* of the particular software to understand vulnerabilities
  - *Disclosure of results* process is handled carefully to allow time for mitigation efforts
  - *Mitigation mechanisms* to provide means of patching or mitigating the potential security vulnerability

Discussion?

