George Myers
NASA/Information Power Grid

July 2001
Revised Sept 2001
Revised Dec 2001
Revised July 2002
Revised October 2002
Revised November 2002

Grid Constitution

Status of this Draft

This draft invites discussions and suggestions for improvements. The distribution of the document is unlimited. Last update on 11.28.2002.

Copyright Notice

1. Abstract

This document is targeted toward those forming a Grid computing environment and describes the basic principles and agreements among individuals and institutions that must be identified and addressed to compose or participate in a *specific* computational grid community. This document primarily addresses the issues related to overall organization and to resource providers within grid environments. The purpose, therefore, is to identify and outline in some detail the various areas and components that constitute a grid for which some form of agreement are necessary. The agreements may be formal or informal, for part or all of the areas identified. Formal agreements allow for a clearer understanding of the relationships and responsibilities that participating resource providers have and are therefore preferred, though in current practice this is not always the case.

The requirements primarily fall in to several areas that every computational organization has already dealt with, but will need to adjust for the grid environment. The primary areas include:

- Organization
- Infrastructure
- Resource sharing agreements
- Information Services
- Security
- Allocation
- Accounting
- User Support

This document serves as a template for institutions wishing to create or participate in a Grid as resource providers. A template with the structure and headings outlined in this document are included as the last section in this document. Documents defining policies, agreements, and methodologies developed by various GGF working groups and from other sources are referenced as appropriate in the various sections. Note that the documents that are suggested are expected to be dynamic and updated to reflect the evolving technologies, capabilities, and policies relevant to that evolution.

Acknowledgement: This document represents the efforts of many GGF contributors who have participated in the construction of this document. We wish to thank and acknowledge the significant contributions of John Towns, John Brooke, Mike Jones, Jon MacLaren, Stephen Pickles, Robin Pinning, Jim Ferguson, Nancy Wilkes-Diehr, Laura McGinnis, Esther Baldonado (including input from the Sandia Security team), Alistaire Mills, and William Johnston.

Table of Contents

1. Abstract 1 — Deleted: 1
2. Organization 5 — Deleted: 5
2.1. Mission Statement and Overview 5 — Deleted: 5
2.2. Governance 5 — Deleted: 5
2.3. Definition of Rights and Obligations 5 — Deleted: 5
2.4. Organizational Requirements 6 — Deleted: 5
3. Infrastructure 6 — Deleted: 6
3.1. Existing Infrastructure 6 — Deleted: 6
3.1.1. How will existing infrastructure be affected? 6 — Deleted: 6
3.2. Infrastructure Components 7 — Deleted: 7
3.2.1. Identify key low-level components 7 — Deleted: 7
3.2.2. Identify required application-level components 7 — Deleted: 7
3.2.3. What middleware is going to be used if required 7 — Deleted: 7
3.2.4. Authentication and Authorization 7 — Deleted: 7
3.2.5. Accounting 7 — Deleted: 7
3.2.6. Defining user environment components – commonality, differentiation across multiple resource providers, machines. 7 — Deleted: 7
3.2.7. Providing as close to a single source of information as possible 8 — Deleted: 7
3.2.8. Support systems 8 — Deleted: 8
3.2.9. Interoperability requirements 8 — Deleted: 8
3.2.10. The method of upgrading levels of key software components 8 — Deleted: 8
3.2.11. The method of reporting changes to the user community 8 — Deleted: 8
3.2.12. The method of scheduling periodic maintenance and other scheduled interruptions of key components of the grid, including networks, compute systems, data stores, instruments, and servers 8 — Deleted: 8
3.2.13. Method of reporting system, network, and software availability and reliability 9 — Deleted: 8
4. Resource Sharing Agreements 9 — Deleted: 9
4.1. Range of Resource Sharing Agreements 9 — Deleted: 9
5. Information Services 10 — Deleted: 10
5.1. The method(s) used to store information 10 — Deleted: 10
5.2. The method(s) used to disseminate information 10 — Deleted: 10
5.3. The method used to agree upon what, where, and how information is stored 10 — Deleted: 10
5.4. What information is required vs. optional 10 — Deleted: 10
5.5. The method(s) used for resource discovery 11 — Deleted: 11
6. Security 11 — Deleted: 11
6.1. Components of the Security Policy 11 — Deleted: 11

6.1.1. Registration policy 11

6.1.2. Credential protection policy 12

6.1.3. Revocation policy 12

6.1.4. Trust policy 12

6.1.5. Authorization policy 12

6.1.6. Data protection policy 12

6.1.7. Network connectivity and firewall policy 12

6.1.8. Policy on inter-grid accessibility 12

6.1.9. Policy and methodology of intrusion detection, and what to do about it 13

6.1.10. Policies of participating organizations that comprise this Grid Communit. 13

6.1.11. Agreement to conduct security audits 13

7. Allocation 13

7.1. Allocation of resources to grid projects 13

7.2. Allocation of users to grid projects 13

7.3. Request reviews 13

7.4. Allocation schedules 13

8. Accounting 13

8.1. Agree on what is going to be accounted for 14

8.2. Method of identification of an individual 14

8.3. Method of valuation of resource utilization 14

8.4. Method of reporting on accounting data 14

8.5. If a Grid Economy Model is used, a method of exchange 14

8.6. Administrative retention 14

9. User Support 14

9.1. Potential User Requirements 15

10. Conclusion 15

11. Grid Constitution Template 15

12. Security Considerations 17

13. Author Contact Information 17

14. Intellectual Property Statement 17

15. Full Copyright Notice 17

16. Appendix A: Governance Examples 18

16.1. TeraGrid Management Plan 18

16.1.1. Introduction 18

16.1.2. TeraGrid Project Summary 18

16.1.3. Institutional Roles and Commitments 20

16.1.4. Management Leadership 22

Deleted: 11

Deleted: 12

Deleted: 12

Deleted: 12

Deleted: 12

Deleted: 12

Deleted: 12

Deleted: 12

Deleted: 13

Deleted: 13

Deleted: 13

Deleted: 13

Deleted: 13

Deleted: 13

Deleted: 13

Deleted: 13

Deleted: 13

Deleted: 14

Deleted: 14

Deleted: 14

Deleted: 14

Deleted: 14

Deleted: 14

Deleted: 14

Deleted: 15

Deleted: 15

Deleted: 15

Deleted: 17

Deleted: 17

Deleted: 17

Deleted: 17

Deleted: 18

Deleted: 18

Deleted: 18

Deleted: 18

Deleted: 20

Deleted: 22

16.1.5. Meetings, Reviews, and Corrective Actions 26
17. Appendix B Sample Contract 27

Deleted: 26

Deleted: 27

2. Organization

The initial decision to construct or become part of a computational grid should be based on clear needs that a grid can fulfill. Most grids will span organizational boundaries, each of which will have some or all of the elements outlined in this document. Some common goals must be shared by, and motivate all of the participants if success is to be achieved, as any one of these areas can present insurmountable roadblocks.

2.1. Mission Statement and Overview

The mission statement describes the overall objective of the collection of participants in the particular Grid Community. The motivation for organizing the virtual organization is stated and high-level description of the organization is given. This section acts as an executive summary of the particular Grid Community.

2.2. Governance

This part of the constitution describes the overall organization of a single Grid Community. Included in this section is a description of the governing body and the management processes for the virtual organization. Within this section, there must be clear delineation of the areas of management responsibility for participating sites. This section should also describe what decision processes exist for making decisions affecting the overall virtual organization. In addition, this section should describe the processes to request and implement changes in the virtual organization. Methods should be defined for petitioning for changes to the constitution. A petition might come from the user base, a participating organization, or a candidate organization. The governing body might be empowered to determine who may become a member of the community. Having these processes in place will provide an easy method for growth and improvement.

As a clearly documented implementation of this, though certainly not the only implementation possible, included in Appendix A is a excerpt from the TeraGrid proposal – the successful response to the US NSF Distributed Terascale Facility Solicitation. This excerpt is the management plan that addresses a number of the issues indicated here in the establishment of a well-defined virtual organization.

If there are other documents addressing this area, we would appreciate getting a copy to include in the appendix.

2.3. Definition of Rights and Obligations

In many ways, the Grid Constitution resembles a contract. Contracts define the various rights and obligations of the parties involved. This includes the definition of terms, ownership of intellectual property rights, obligations of both parties, services provided, warranty, confidentiality, agreements for termination of the relationship, force majeure, duration of the contract, etc. As grids move into the commercial sector, these will become more important and more formal. A sample contract is included as appendix B. These issues will be particularly important for Resource Sharing Agreements, but will apply anywhere a service is provided. The disposition of Intellectual Property Rights of data and software developed as a result of collaboration with the grid community should be addressed. Included as Appendix C is an example of a document that defines the area of Intellectual Property Rights in the Alliance Grid which represents a collaboration of several distinct organizations. In addition the Open Source Working Group of the Global Grid Forum is addressing Intellectual Property in the development of Open Source.

2.4. Organizational Requirements

The following are questions to stimulate thinking about issues that deal with the overall organization of a grid.

- Will we be joining a single Grid, or must we allow for multiple Grids, with overlapping/conflicting software requirements? Even if we're joining one Grid now, there may be more Grids in the future.
- Are we joining an existing Grid? If so, this may determine many of the infrastructure decisions (for sake of consistency to the users). If not, we may be in a position to influence the infrastructure decisions.
- Are we free to decide what to do, or is there a committee that limits our decision making, e.g. by mandating that resource X may only become part of a single Grid?
- How can I simultaneously satisfy my responsibilities in all grids I participate in?
- Who are the partners in the Grid? What are responsibilities of partners? Who's responsible for providing what part?
- Will the Grid have centralized or distributed control?
- What else needs establishing? For example: helpdesk, web presence, policing? What resources do we need to provide all this?
- What agreements and contracts need to be set up. Will we have Service Level Agreements, and what will they look like (e.g. bilateral, multilateral)?
- What should a grid provide for users (see below)?
- Is there a Roadmap that can be given to the users?

3. Infrastructure

Infrastructure means the support structure that maintains the cohesive elements of the grid. This includes system administration where agreed upon levels of middleware, operating systems, and any other key software elements are maintained. Included in this are the support of various hardware and network elements that are critical to the functioning of the overall grid environment.

Before the infrastructure can be decided upon, the existing infrastructure needs to be thought about, as do requirements for the Grid (both organizational and user-driven).

3.1. Existing Infrastructure

What are the resources that are going to be put onto the Grid? Are these resources part of an existing infrastructure?

Before the formation/joining of the Grid, the resources may already be part of some existing facility. These schemes may already provide infrastructure such as helpdesk, web presence/information, training, support, system support, engineers, etc. There are other existing facilities that may be joining in, such as data/information service providers, experimental facilities, network providers, etc. And there will also be users who are already using these facilities. There will also be existing sources of funding (DTI, Research Councils, consortia of users), and perhaps some new ones for Grid-related funding.

3.1.1. How will existing infrastructure be affected?

To answer this question, the Service Provider needs to consider the following questions:

- What service am I expected to provide? To what level(s), e.g. 24/7 QoS SLA (Service Level Agreement). See also, the section on Resource Sharing Agreements
- Where will the boundaries of responsibility / accountability be? (So, who do users contact? What does helpdesk do/not do? What gets passed on? If something isn't done, who takes the blame?) See also the User Support Section.
- Who are my clients/customers/stakeholders? My registered users, my "guest" users (trusted/untrusted), my funding body, my corporation, my partners, etc.

Most Important: A Grid must not compromise existing standards of service on security policies, conditions of use (or changes to baseline service quality must be negotiated in advance).

3.2. Infrastructure Components

Components of the infrastructure that need to be agreed upon include:

3.2.1. Identify key low-level components

What Hardware, Operating System, Schedulers (e.g. NQE, LSF, SGE, PBS, Entropia, Condor) will be used?

3.2.2. Identify required application-level components

What Software and applications will be required on the Grid? How will licenses be managed (e.g. by the scheduler)?

What compilers, debuggers, development tools will be needed?

3.2.3. What middleware is going to be used if required

Middleware flavours? e.g. Globus, UNICORE, LEGION

3.2.4. Authentication and Authorization

What are the security policies that apply? [Reference the Security Policies Section of your document]

3.2.5. Accounting

Who has used my machines? Who should pay? Can we also meet the user's accounting requirements. See also, Accounting Section.

Can the accounting information be used as an input into capacity planning? Can users provide resources with predictions of their usage to assist in capacity planning?

Logging – will this be centralized or interlinked? Can we tell who ran this job?

3.2.6. Defining user environment components – commonality, differentiation across multiple resource providers, machines.

How consistent can the user environment be? It will never be possible to maintain all sites perfectly in sync with respect to software resources, so we must strive to:

- Plan changes/upgrades carefully and inform the users sensibly of changes
- Ensure compatibility across the Grid at all times, e.g. by providing environment variables which always point to the same thing on different resources.

3.2.7. Providing as close to a single source of information as possible

What information should be published?

- User guides and documents.
- Web pages.
- Meta-data information (e.g. MDS in Globus) about: resources, applications licenses; also resource/network monitoring. Maybe extend this to describe repository of client tools for end users.
- Conditions of use.
- Points of contact (helpdesk, etc.)
- [notification/dissemination, mailing list]
- data protection/privacy policy

How to publish? Want to provide as close to a single source of information as possible.

3.2.8. Support systems

Will there be a helpdesk? Will it have multiple entry-points, e.g. telephone (24/7?), e-mail? Will there be SLAs for turnaround time,etc?

Can the users use this as a single point of contact for anything that goes wrong in the Grid? If so, what will the procedures be for tracking and exchanging incidents? Must decide on how to arbitrate and demarcate problems. Also, who is responsible for what?

See also, User Support Section.

3.2.9. Interoperability requirements

Can all the chosen components interact with each other? If not, what do we do next?

This is particularly complex if a single resource is being part of more than one Grid, as this may mandate having different pieces of middleware doing similar tasks, or even running different versions of the same middleware. Can these pieces be made to interoperate?

3.2.10. The method of upgrading levels of key software components

Do we need to have an interim period where multiple versions are available? When do we change the default version? How do we notify users about this (see below)? Do we require downtime in Grid middleware, or even reboots?

3.2.11. The method of reporting changes to the user community

Can we provide a (regularly updated) roadmap? Will we run a mailing list? Or just put everything on a collection of web pages?

3.2.12. The method of scheduling periodic maintenance and other scheduled interruptions of key components of the grid, including networks, compute systems, data stores, instruments, and servers

How will this work be coordinated across the Grid? Can we ensure that some parts of the Grid are always available? How do we report this to users (see below)?

3.2.13. Method of reporting system, network, and software availability and reliability

How do we publish these statistics? Can they be made accessible in machine readable form (e.g. through a Web Service) as well as human-readable (Web page)? Will we publish quarterly reports for the service?

4. Resource Sharing Agreements

Resource Sharing Agreements (RSA's) are, at their core, simply bartering arrangements between two or more parties to share what resources they control with the other party or parties. One current widespread use of RSA's can be found among the libraries of the world. Most have RSA's with multiple groups of libraries, committing to share resources and costs associated with shipping materials to each other to satisfy that sharing. There are many other examples.

RSA's are not to be confused with Service Level Agreements (SLA's). SLA's, as the name suggests, refers to the level of service to be provided from a resource. If your institution is sharing a 64-node Linux cluster, for instance, you will likely not want to share it 365 days a year, but some fraction of that time. RSA's can (and in most cases should) point to separately written SLA's for each resource shared. This includes human support of hardware, software, etc.

RSA's between computing centers will necessarily be more complex than those between libraries, for example, given that there are many types of resources to share. An agreement between two parties (or among a consortium) must specify many things, including hardware available, long-term and short-term storage available, network connection expected, software available, etc. Consortia need to fully delve into expectations from each party involved and (hopefully) have some mechanism of RSA compliance. For example, if each site is expected to maintain a license and install the latest commercial computational fluid dynamics code, then that needs to be spelled out in the RSA.

One of the trickiest things to be worked out is in the accounting of usage. Each party to the agreement will either need to adopt one method of accounting for usage of resources, or each site must agree to learn and understand the accounting methods employed at all the other sites. This is critical in order to insure fairness of compliance of the agreement by all parties.

RSA's should contain language that demands a periodic review of the requirements from each site. A consortium will likely expect each site to keep upgrading their hardware, both computational and data storage, plus perhaps keep upgrading their network connections. Unless you can see into the future, a periodic review of requirements will be needed.

Some work has been done in the Enforcement area of this problem, mainly aimed at checking compliance of commercial vendors in their contracts to deliver applications or other resources to a client. One paper by Tao Zhao and Vijay Karamcheti at http://www.cs.nyu.edu/vijayk/papers/agreements-ipdps02.pdf details a way to enforce RSA's. The paper also contains references to further work on this subject.

4.1. Range of Resource Sharing Agreements

Given the above definition of RSA's, the following is a list of some of the areas that an RSA might address:

- Definition of Overall Grid Environment
- Overall Quality of Service Agreements - Is it practical to define a level of quality of service?
- Hardware environment and service level agreement. Level of support by local organization. Set expectation of availability. Define how much resource is available. How are the resources allocated for use. All resources should be addressed: compute resources; mass storage; networks; others. Longevity of resource.
- Software environment and service level agreement. Advertise software that is available on a resource. May include details of licensing, versions, where it is located, etc, as appropriate. Longevity of software and possibly versions, old, current, and new.
- Environment and service level agreement. Data retention policy, whose responsibility is it to maintain data. Level of User Support provided by local sites.

5. Information Services

This section of the Grid Constitution describes the method and format for storing and disseminating global and local information that is required to inter-operate. An information service provides vital information used by other grid services for the purpose of job management, or grid monitoring.

Information Service is being addressed by the Grid Information Services (GIS) Area of the Global Grid Forum (GGF). In many cases, members of a specific Grid community will agree on the middleware to be used and this will determine how information will be stored and disseminated. Several documents describing various topics addressing Information Services are under construction in the Grid Information Services Area. See these documents in the GIS Web Pages at: http://www.ggf.org for more information.

Participation in the development of specifications and standard for Information Services can be achieved by participation in the Grid Information Services Area of the Global Grid Forum or by proposing a new area of investigation.

The following sections outline areas where agreements may be necessary.

5.1. The method(s) used to store information

How will the information be stored for later retrieval? Examples might be a database, and LDAP server, or a service that hides the storage medium.

5.2. The method(s) used to disseminate information

Whichever method is used to store data, methods must be provided and agreed upon to extract information.

5.3. The method used to agree upon what, where, and how information is stored

From a users perspective the information service should provide a consistent view of the resources. Therefore, agreements on what information is stored are required. Agreements on where specific kinds of information are stored may be required if more than one information repository is provided. Agreements on how data is represented may also be necessary to distinguish between "grid wide" and "site specific" use of a term to eliminate ambiguity.

5.4. What information is required vs. optional

The above agreement might be refined to define what data is required vs. optional.

5.5. The method(s) used for resource discovery

One of the more common tasks performed in a grid environment is the determination of what resources are available to the user. Agreements may be necessary to provide consistent information about resources and simplified methods to access it.

6. Security

The cornerstone, perhaps the foundation, of establishing a grid is a well-defined security policy and implementation. Any organization with expensive equipment and sensitive data, whether it is government sensitive, or company private data, has security policies in place to protect that data, both physically, and electronically. You will seldom find two organizations that are identical in security policy, or in the way they carry it out Most grid middleware accommodates a security infrastructure. Some (like DCE and Legion) provide part of the infrastructure. Other middleware (globus toolkit) sit on top of a site's existing PKI or Kerberos security infrastructure.

In order to participate in a grid community you need to be able to adapt your policy so that it can be accommodated / enforced by the Grid security services. Both your security policy and the security policy of the grid community you wish to join need to be well defined.

Several areas should be described in the Security Policy. One such area is authentication of individuals and entities. How do you know this person is who they say they are? What organization do you trust as sufficient to verify identity? Another area is authorization. Ok, I trust you are who you say you are. You have the right stamp of identification, but how do I know you are authorized to use a particular resource, or access particular data or equipment? What means is used to ensure the privacy and security of data? What are the physical precautions used to ensure physical access to data and resources are limited to authorized personnel and electronic access?

There are several security standards that can be used. Using a standard security methodology (PKI, Kerberos, DCE, etc.) is necessary to allow diverse organizations to interact without overly complex interfaces. This standard security methodology will be a set of security policies that represent the common denominators among the participating organizations. In order to become a member, an organization wishing to participate will have to evaluate whether these policies are sufficient to satisfy their own requirements. And in turn, the grid community will have to evaluate the policies of the petitioning organization to determine whether their policies are sufficient to become a member of the grid community.

6.1. Components of the Security Policy

(some of these may come from the overarching organization or agency to which you belong)

The three policies below are often defined by references to standard policy guidelines. In the PKI world there are organizations that define general "Certificate Policy" statements, and a site's local policy may refer to such a statement. The GGF has a working group that is developing such a document for use by the Global Grid community. These policies may be backed up by detailed, auditable practice statements. In some cases, there may be policy requiring formal inter-site agreements before one site is allowed to trust a security provider (CA, KDC, Domain Controller, DCE cell, etc.) from another site or organization.

6.1.1. Registration policy

This policy defines how an authentication provider assures that they issue initial identity certificates and/or keys appropriately. In high-assurance environments this may involve in-person registration and assurance that a name on a certificate matches a person's passport, drivers license, or government issued badge.

6.1.2. Credential protection policy.

This policy defines how an authentication provider issues and protects credentials (i.e., certificates and keys.) It may include policy on how key servers or key escrow systems protect keys, in addition to how users are required to protect their own keys (and/or passphrases, smartcards, cryptocards, etc.). A high-assurance policy may require that an identity private key exist only on a smartcard.

6.1.3. Revocation policy.

This policy defines how an authentication provider assures that accounts and credentials are disabled or revoked appropriately. A long-lived credential like a PKI certificate and key may need to be revoked by publishing a "certificate revocation list", making that list publicly available as a high-assurance service.

The following policies apply to users and to administrators of grid resources.

6.1.4. Trust policy

This policy defines what is required in order to allow a user or resource to trust an authentication or authorization credential from some authority (CA , KDC, Domain, etc). In high-assurance environments, this policy may require that the user or resource only trust sites that have inter-site trust (cross-certified CA keys, or inter-realm KDC trust relationships) with their local security provider. In other cases a user or resource owner may be allowed to directly trust a foreign security provider.

6.1.5. Authorization policy.

This policy defines what is required before a resource administrator may allow a given subject (entity/user/role represented by a trusted credential) access to a given resource. In the simplest cases, this policy defines how a global identity may be mapped into a local identity (such as a Unix user and group ID). In many cases, the global identity and perhaps an associated attribute certificate is mapped into roles or groups that are used by site-local access control mechanisms.

6.1.6. Data protection policy

This policy is typically defined by the data resource owner, and specifies what type of integrity and/or privacy protection is required on data, especially data in-transit over public networks. Some high assurance sites may require that all sensitive data in transit be encrypted using a specific algorithm from a specifically approved encryption library. Some data (e.g., security libraries) may require high integrity protection, but little or no privacy protection.

6.1.7. Network connectivity and firewall policy

This policy generally defines ports, addresses, and protocols that are allowed to pass into and out of a site or organization's network. It may include requirements for proxying, network address translation, network address hiding, and intrusion detection, -- any of which could have a serious impact on whether or not a grid service can operate over the site's network.

6.1.8. Policy on inter-grid accessibility

If this grid community wishes to allow interaction and cross grid activity, there should be a policy that describes the security requirements for accessibility. This may be as simple as a statement that requires the use of some commonly known authority.

6.1.9. Policy and methodology of intrusion detection, and what to do about it

Intrusion detection is more an activity, however, a policy might state that it must be performed, and outline a set of basic tools or techniques that should be employed.

6.1.10. Policies of participating organizations that comprise this Grid Communit.

This is a collection of the policies of all of the participating organizations. Having such a repository will make it much easier for potential participants to review both the individual policies and all of the agreements of the current participants.

6.1.11. Agreement to conduct security audits

This would involve agreeing on an outside organization, or a select team of internal security experts to perform periodic audits to ensure that security policy is being enforced.

7. Allocation

Grid allocation means two different things: how much of a resource does a stakeholder make available to grid users and how do grid users request and receive access to grid resources. Research into current practices (see “Current Practices in Accounting”, ***[put URL here]***) shows that one commonality across all sites is some level of request review before projects are granted access to HPC resources. It is unlikely that participating organizations and funding agencies, for example, will be willing to relinquish control, at least initially, to self-allocating implementations. Therefore, allocations issues should be addressed at the constitutional level.

7.1. Allocation of resources to grid projects

Resource providers need to decide how much of their resource will be made available for grid projects. This should consider how much of a resource is made available, when it will be available, and how grid users will be made aware that the resource is available (e.g. resource discovery).

7.2. Allocation of users to grid projects

The resource providers need to agree on how users and resources will be connected, through some sort of allocation process, or via some other agreed-upon methodology.

7.3. Request reviews

It is rare that users have unrestricted access to computing resources without completing some sort of application process, often involving some oversight or review.

7.4. Allocation schedules

If request review and allocation will not be an ongoing activity, the resource providers and users need to agree on the application and review schedule and the allocation start and end date guidelines. Issues of request extensions, renewals and supplemental allocations and their timing should also be enumerated.

8. Accounting

Most large computational centers have some form of accounting. Accounting is not built into many modern operating systems, however, most large computational centers have a local accounting system that provides some degree of capability. Generally, these accounting systems are based on system usage records, but tend to aggregate resource utilization differently, depending on the needs of the organization. Accounting acts as both a method of identification and as a method of tracking usage. In order to be accountable for utilization some measurement methodology must be agreed upon. This must be well defined. Most accounting systems have a method of measuring usage. What is needed in the grid environment is a way to compare resources of diverse architectures.

The following sections describe the components of accounting that need to be agreed upon.

8.1. Agree on what is going to be accounted for

8.2. Method of identification of an individual

While security defines the requirements for obtaining an account, this element of accounting describes how the organization ensures that each individual is uniquely identified. This is important from an accounting perspective for sites that need to be able to map usage back to a specific person, at least when the resources are being used

8.3. Method of valuation of resource utilization

If the resources contributed to the grid are not free of charge, a method of exchange needs to be determined to fairly compensate the participating organization for resources used. This valuation might not only be determined by the raw capability of the resource, but might also take into consideration the demand for the resource. Several ideas are being explored and discussed by the GGF Accounting Working Group.

8.4. Method of reporting on accounting data

This document or section of the accounting document describes how accounting information is reported.

8.5. If a Grid Economy Model is used, a method of exchange

A section must describe how equalization is achieved, or how and what is exchanged for imbalances in utilization. The GGF Accounting Working Group is developing scenarios and responses for a variety of economic models that could be used by grid projects.

8.6. Administrative retention

This section should enumerate the various types of relevant administrative data (usage records, identity mappings, e.g.), how long the data will be retained, and which entities will be responsible for retention and purging.

[Might want to include reference to User Records WG work here.]

9. User Support

Users are the reason for a grid. Supporting them is more difficult in a grid environment for many reasons, not the least of which is the geographically distributed nature of grids. In the "Grid User Services Common Practices" document we have defined the common practices for user support in a grid environment (insert URL). That document can assist an aspiring grid community to define their support model. In the context of this document, these practices need to be spelled out as an agreement between the participating organizations.

Components of user support that need to be agreed upon:

- The overall support model
- Methods of dissemination of user information

- Service level agreements in the context of user support, i.e. level of support.
- Method and form of education and training
- Problem reporting and resolution procedures
- Method of dissemination of support staff information
- Methods of measurement of success
- Policies for the creation of a User Forum

9.1. Potential User Requirements

What will your prospective users want/expect from a Grid?

- Single sign-on/credentials – what's accepted, how to get them, how maintained?
- Resources that can authenticate themselves to users.
- Remote job submission/monitor(heartbeat)/retrieval – nice tools for doing these things, when mobile.
- Information about resources (local/remote) – available everywhere. Information for resource discovery. Physical info – computers – memory, connectivity, devices. Information about how to access and conditions of use. See also, Information Services.
- Unified conditions of use in a Grid.
- Persistence, always meeting SLA. Consistence – notification of environment changes.
- Support. Single point of contact.
- Debugging. Being able to track failures, obtain trace and log information.
- Accounting. What am I being charged? What resources did I use?
- Authorization. More power/control to user, automatic access to new Grid resources.
- Plug-and-play resources (service perspective?).
- Watertight SLA. Contracts, but transparent.
- Confidentiality/privacy/data protection.
- Protection against malicious use.

Overall, they want the Grid to Make Life Easier!

10. Conclusion

A Grid Constitution provides cohesion within a specific grid community by defining the policies and procedures for which agreement is essential. . The implication here is that the level of complexity that Grid Communities entail require agreements in many key areas in order to function. This document outlines these key areas. What we have been describing are the minimal components and agreements that are necessary to ensure a smooth functioning grid environment. These agreements may take the form of a set of Memorandums of Understanding, or a more formal contract that the participating organizations of a grid community compose and sign. The details of each section will be dependent upon the organizations forming the grid.

11. Grid Constitution Template

This section provides a template of the areas covered above that can be used to construct constitutions--or agreement statements--for current and prospective grid communities. An alternative would be to use the ten sections above as the template.

1.0 Abstract

[Brief description of the document.]

2.0 Organization

[Description of common goals and overall structure of community/]

2.1 Mission Statement and Overview

2.2 Governance

2.3 Definition of Rights and Obligations

2.4 Organizational Requirements

3.0 Infrastructure

[The details of the underlying support and organization for hardware and software that constitutes the organization.]

3.1 Existing Infrastructure

3.2 Infrastructure Components

4.0 Resource Sharing Agreements

[Descrition of how resources will be shared between the various organizations that comprise this grid community.]

4.1 Range of Resource Sharing Agreement

5.0 Information Services

[Description of how information on grid resources is handled.]

5.1 The method(s) used to store information

5.2 The method(s) used to disseminate information

5.3 The method used to agree upon what, where, and how information is stored

5.4 What information is required vs. optional

5.5 The method(s) used for resource discovery

6.0 Security

[Description of the security policies that apply to this grid community.]

6.1 Components of the Security Policy

7.0 Allocation

[Description of how resources are allocated within this grid community.]

7.1 Allocation of resources to grid projects

7.2 Allocation of users to grid projects

7.3 Request reviews

7.4 Allocation schedules

8.0 Accounting

[Description of how usage is accounted for between the organizations comprising this grid community.]

8.1 Agree on what is going to be accounted for

8.2 Method of identification of an individual

8.3 Method of valuation of resource utilization

8.4 Method of reporting on accounting data

8.5 If a Grid Economy Model is used, a method of exchange

8.6 Administrative retention

9.0 User Support

[Description of how users will be supported in this grid community.]

9.1 Potential User Requirements

12. Security Considerations

Security issues are not discussed in this document.

13. Author Contact Information

George Myers
NASA/Information Power Grid
gmyers@nas.nasa.gov

14. Intellectual Property Statement

The GGF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the GGF Secretariat.

The GGF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this recommendation. Please address the information to the GGF Executive Director.

15. Full Copyright Notice

16. Appendix A: Governance Examples

As documented implementations of many of the issues raised in Section 2.2, though certainly not the only implementations possible, included below is the management plans for some virtual organizations establishing grid environments.

Deleted: 2.2

16.1. TeraGrid Management Plan

Below is the management plan for the TeraGrid project – the successful response to the US NSF Distributed Terascale Facilty solicitation. This plan addresses a number of the issues in the establishment of a well-defined virtual organization.

Here we include an excerpt from the Project Management Plan for the NSF fundeded project The TeraGrid: Cyberinfrastructure for 21st Century Science and Engineering. More complete information about this project is available at www.teragrid.org.

16.1.1. Introduction

This document presents the management plan, schedule, and resource allocations for the "TeraGrid: Cyberinfrastructure for 21st Century Science and Engineering" project, hereafter referred to as the "TeraGrid," submitted in accordance with National Science Foundation (NSF) solicitation NSF 01-51 for a distributed terascale facility (DTF). This project will acquire, deploy, test, and make operational a DTF among four major institutions, NCSA, SDSC, UC/ANL and Caltech, based on large-scale Linux clusters, data archives, and high-performance networks.

The DTF TeraGrid will have broad impact on the computational science community, advancing discovery by making available to academic researchers next generation information technologies that are an order of magnitude more capable than those now generally available. These computing resources will allow more complex and complete simulation, more thorough analysis of large datasets, higher resolution visualization, and contributions to the body of scientific knowledge.

This document describes the organization, systems, and plan via which the project participants will manage the TeraGrid project. This plan will be reviewed and revised, as required, to incorporate lessons learned, changes in baselines (technical scope, cost, and schedule), and new project development and/or other arrangements among the participants. Revisions, as they are issued, will be acknowledged by all participants, and will supersede in their entirety previous versions. New information on requirements will assist the project participants in determining the order to undertake the development and deployment efforts in the plan, managing risk, and ensuring the integration effort meets its objectives and deliverable schedule.

16.1.2. TeraGrid Project Summary

Collaboratories and scientific consortia are conducting simulations of fundamental phenomena (e.g., weather and climate, physics and biochemistry) at unprecedented scale. Moreover, diverse disciplines are now developing observatories, experiments and sensor networks (e.g., astronomy, ecology and physics) that will generate torrents of new data. Disciplinary scientists in these projects recognize that a distributed computing, communications, and information infrastructure, a large-scale Grid, is the primary catalyst for scientific breakthroughs, enabling extraction of insights from the torrent of new data and testing of theories via simulations. At the dawn of the Digital Millennium, it is time to deploy a sustainable national cyberinfrastructure in support of these activities.

In partnership with IBM, Intel, Qwest, Oracle and SUN, the National Center for Supercomputing Applications (NCSA), the San Diego Supercomputer Center (SDSC), University of Chicago (including Argonne National Laboratory) (UC/ANL), and the California Institute of Technology (Caltech) will create a DTF based on multiple terascale Linux clusters and Intel's next-generation McKinley microprocessor, as well as large-scale storage archives and data management software; a 40 Gb/s optical mesh will interconnect the DTF's components. The DTF will increase PACI computing, storage and communication capability by an order of magnitude, transforming academic high-performance computing.

The DTF hardware will be integrated, using Globus and other PACI Grid technologies, to create a powerful TeraGrid, with an aggregate of 13.5 TF of computing capability and roughly 600 TB of disk storage, that supports terascale computing (6.1 TF and 120 TB at NCSA, with FY02 PACI funding proposed to augment this to 8 TF and 283 TB), distributed data management (4.1 TF and 225 TB at SDSC), remote rendering and visualization (1 TF and 25 TB at UC/ANL), and data-intensive scientific application analysis (0.4 TF and 86 TB at Caltech). Figure 1 shows the overall architecture of the DTF clusters with vendor labels and capacities.

This DTF TeraGrid will be the largest coordinated infrastructure ever deployed for open scientific research. As a comprehensive computing, data management, and networking environment of unprecedented capability, the TeraGrid will be the enabling cyberinfrastructure for 21st century U.S. scientific research. Operating as a distributed resource that can be co-allocated and scheduled, the TeraGrid will support traditional scientific computing and emerging disciplinary scientific groups. A unified TeraGrid Operations Center will coordinate management, user support, and access.

The two PACI partnerships will spearhead deployment of the proposed TeraGrid. From the beginning, these two groups have been at the center of information technology revolution, developing the flexible Grid toolkits, commodity cluster computing systems, and data management and mining tools that can transform 21st century scientific endeavors. Indeed, PACI technology is at the heart of both disciplinary (GriPhyN, NEES, PPDG, and Telescience) and agency (NSF, DOE, DOD, and NASA) Grid deployments, participating in over 90 percent of the NSF Major Research Equipment projects. As such, *the proposed DTF TeraGrid is the culmination of a decade of research, development, and deployment by NCSA, SDSC,UC/ANL, Caltech, and their partner institutions.*

To maximize scientific return on the DTF, the PACI partnerships will optimize "community application codes"—those codes and toolkits that promise to transform science and engineering via the TeraGrid. In consultation with the national community, these codes will be drawn from NSF-sponsored centers (e.g., NCAR, NOAO, and NRAO), MRE projects (e.g., NEES, NEON, Earthscope, and ALMA), major existing PACI users and other collaborations.

Additionally, this multifaceted TeraGrid will enable the creation and support of a national and international Grid of partner and satellite clusters and storage archives, leveraging PACI community building for Grid and cluster software. The result will be a unified national computing and data fabric, with the PACI TeraGrid anchoring a national cyberinfrastructure. Moreover, via technology evolution, the DTF TeraGrid can evolve naturally to 30-50 teraflops, 2-4 petabytes, and 80 Gb/s wide-area networks in 2-3 years. In less than ten years, it will scale to petaflops, tens of petabytes, and terabit networks. This DTF extensibility means partnerships with NSF Major Research Equipment (MRE) and other projects can enhance DTF resources, extending the TeraGrid for the national and international user base.

The DTF represents the largest single investment in NSF's history for computing infrastructure. This investment is complemented by at least $32.2 million in Illinois and California financial commitments to high-performance networking, facilities, and operations, plus an estimated $106 million in new IT buildings for faculty and staff at NCSA and the University of Illinois. By engaging vendors, application researchers, computing experts, and government collaborators in a partnership that leverages the explosive growth of Grid technology, open source software, and high-performance commodity hardware, we can deploy a cyberinfrastructure far more powerful and flexible than any single supercomputing system, catalyzing scientific discovery across broad disciplines.

16.1.3. Institutional Roles and Commitments

Each of the four partner sites fills an important, complementary role, and the hardware configurations at NCSA, SDSC, UC/ANL, and Caltech reflect the diversity of these roles. Concretely, NCSA and SDSC will lead the compute-intensive and data-intensive foci, respectively, drawing on their experience deploying large Linux clusters and data archives. In turn, UC/ANL will support remote visualization and software development, as well as managing deployment of the DTF wide-area network, and Caltech will support application community outreach and data serving.

The sites and the principals are committed to the Grid because they believe it is the future of high-performance computing. Moreover, the co-PIs and the participating institutions have a long history of collaboration that is independent of the PACI program. We have set concrete performance milestones that must be met by each of the four teams. The Project Director and Project Manager will hold each organization responsible for meeting its milestones.

National Center for Supercomputing Applications (NCSA)

NCSA will lead support for compute-intensive applications by deploying the 5+ TF compute-intensive system requested by the DTF solicitation. The storage configuration of the NCSA cluster is based on the same node building blocks with connected Fibre Channel SAN disks. This hardware commonality is intended to reduce software complexity and allow the storage components to be applied to compute-intensive applications when desired. Moreover, large storage archives at NCSA provide an alternate site for hosting discipline data archives, a potential data mirror site for SDSC, and data set storage for computing intensive applications.

This deployment builds on NCSA and the Alliance’s strength and experience building and supporting compute-intensive systems from commodity components, beginning with deployment of RISC clusters and a succession of Windows and Linux clusters. This experience with commodity hardware and open source software has led to new tools for cluster communication (e.g., VMI), cluster performance tuning and configuration, and large-scale operations.

NCSA is also one of the national leaders of an industry, national laboratory, and vendor consortium (OSCAR) to package and test cluster software on vendor platforms. The OSCAR initiative, along with the Alliance “cluster in a box” effort, is intended to foster use of open source cluster software on commodity platforms by reducing the effort required to deploy clusters. Finally, NCSA brings over two years of experience assisting users in code porting and tuning for commodity clusters.

Finally, the compute-intensive deployment will leverage 18 months of collaborative installation, integration, and deployment experience with IBM on the 1 TF, 1,024-processor Pentium III Linux cluster and the 320-processor Intel 64-bit Itanium cluster. Installation experience with the IA-32 cluster has already provided valuable insights into physical connection, Myrinet NIC testing and quality assurance, and node software cloning and distribution.

Although the processor architectures of the 1 TF IA-32 cluster and the 6.1 TF (8 TF with Cooperative Agreement augmentation) IA-64 DTF clusters differ, most of the physical installation and testing issues are similar. Indeed, there are fewer network components and nodes in the 8 TF DTF cluster than in the 1 TF IA-32 cluster, suggesting that we will have gained insights into some, though certainly not all, of the scaling issues associated with initial deployment. Deployment of the two 1 TF clusters will provide a year to test Linux and system software configurations, test IA-64 compilers, and continue working with compute-intensive application developers to optimize their codes.

In addition, NCSA and UC/ANL are leading an effort to build and deploy reconfigurable Grid infrastructure. The Alliance “Grid in a Box” software distribution builds on the “Cluster in a box” by adding the requisite software and documentation to “Grid enable” clusters. The Grid in a Box goal is enabling users and institutions to rapidly build and deploy functional Grids for application development and execution. This effort is jointly led by NCSA and UC/ANL and will be applied to achieve TeraGrid objectives.

San Diego Supercomputer Center (SDSC)

SDSC will lead data management for the TeraGrid by deploying a 4.1 TF data-intensive compute cluster, a large commercial-grade database-optimized SMP for data management and mining support, a 220 TB network disk storage, and a 900 TB archival storage system, all joined with other TeraGrid platforms via a high-performance WAN. SDSC will lead in the support of data management services, including collections management, collections replication, and the housing of specific collections including 2MASS, PDB, NVO, CMS, LIGO, BIRN, and NSDL. This deployment builds upon SDSC's experience developing open source cluster management tools (NPACI Rocks) and operating an existing 10 TB SAN, based on Sun storage and Brocade switches. Like NCSA, SDSC is likely to deploy 2-processor McKinley nodes if they become available.

The metadata management system will be deployed on a 72-processor Sun Starcat and will house all TeraGrid metadata information. The system will have 144 GB shared memory, eight 1 Gb Ethernet adapters, and sixteen 2 Gb/s fiber channel interfaces attached to SDSC's 220 TB SAN. The Sun Starcat represents Sun's next generation flagship SMP system. The system's primary function will be to run the Storage Resource Broker and the Oracle relational database. The metadata management tools will allow it to broker 3rd party data transfers among TeraGrid resources

This infrastructure allows SDSC to focus on data-intensive computing, very large-scale distributed collections management and data mining. This all leverages and extends SDSC's current activities in each of these areas. This tightly coupled and integrated storage-centric infrastructure will support data-intensive applications in ways impossible at other sites. SDSC also brings expertise and experience working with application scientists to understand their data (rather than just their application codes and/or algorithms), and will use this understanding to better model the domain data. This enables collaboration among scientists and data sharing among multiple tools.

SDSC's digital library experience has been demonstrated in applications ranging from Digital Sky and Digital Embryo to PPDG, along with integrating data from disparate disciplines for comparison and analysis. In addition to the data modeling and integration, SDSC has a unique combination of high performance database and data mining skills. For example, the SDSC data intensive group is working closely with the Alliance for Cellular Signaling (AfCS) group to enable high performance, high throughput analysis of micro-array data. Similar efforts are being planned for the NIH Biomedical Information Research Network (BIRN) project, and are anticipated with the Joint Centers for Structural Genomics (JCSG) and Protein Data Bank (PDB) initiative as well.

University of Chicago (including Argonne National Laboratory) (UC/ANL)

UC/ANL will concentrate on developing visualization capabilities for the TeraGrid. This work will involve deployment of a 1 TF cluster that will be configured to support three functions: 1) remote visualization (graphics accelerators and balanced I/O), 2) early testing and deployment of IA-64 cluster software (math libraries, scalable systems software (MPI and PVFS), and grid software infrastructure (IA-64 Globus Services), and 3) a general co-schedulable application cycle and I/O server for the TeraGrid.

UC/ANL has considerable experience in research and development areas critical for the success of the TeraGrid, notably libraries for computational mathematics and solutions of PDEs (e.g., PETSc), communication and parallel I/O libraries (e.g. MPICH and ROMIO), Linux cluster systems management and operations (e.g., Chiba City tools), Grid software tools (e.g., Globus), advanced networking and network engineering (I-WIRE, Star TAP, MREN, Starlight), and remote visualization and collaboration software (e.g. CorridorOne and the Access Grid). UC/ANL has considerable existing software development capability and will be providing critical software components for the DTF and TeraGrid.

UC/ANL will be the lead site for development and deployment of TeraGrid remote visualization services, parallel networking software interfaces to the clusters, and open source parallel and remote I/O infrastructure. UC/ANL has been the lead institution in the State of Illinois I-WIRE fiber infrastructure project and led the DTF network design and bandwidth vendor evaluation and negotiation, leading to the Qwest partnership. UC/ANL will lead a team of staff from UC/ANL, NCSA, Caltech, SDSC, Qwest, Internet2 and Indiana University to evaluate, select, and deploy transmission (DWDM), switching, and routing equipment to create a production network infrastructure. In addition, UC/ANL will work closely with NCSA to test high-performance parallel networking between clusters at the two sites; with the goal of staying ahead of the production WAN networking deployment plans.

California Institute of Technology (CIT)

Caltech will focus on application capabilities for effectively exploiting the compute-intensive cluster at NCSA with the data-intensive resources at SDSC, providing a prototype environment integrating scientific data serving, storage, and analysis. Caltech will deploy a data-intensive McKinley cluster configuration with 0.5 TF peak speed, 0.4 TB of memory, and 22 TB of local disk. A further 64 TB of disk will provide a data cache for on-line access to substantial scientific data collections from projects such as LIGO, LHC, and NVO. Caltech's HPSS archival storage system will be enhanced to provide higher I/O (through more tape drives and a much larger HPSS-managed disk cache) and more capacity.

The Caltech TeraGrid node will be available for the entire PACI community but will work particularly closely with several major projects that require both data-intensive and distributed analyses, namely LIGO, LHC, and NVO. Caltech's Center for Advanced Computing Research (CACR) has been collaborating with all of these projects for several years and has contributed substantially to mapping out their simulation, data analysis, and data storage directions.

CACR staff members have been actively involved in Grid development and deployment (e.g., CASA gigabit network testbed and SF Express), in data-intensive applications (Digital Sky), in putting applications on the Grid (Digital Puglia and VirtualSky), and in deploying applications on parallel computers and Beowulf clusters. CACR has deployed several Beowulf clusters based on Linux and won a Gordon bell prize in 1997 for the most cost-effective computing. Thomas Sterling, the inventor of Beowulf clusters, will participate in the TeraGrid and has already led the design of the proposed CACR data cache.

CACR has a long history of working with application groups to exploit new computing technologies, including Linux clusters and grids, and its ongoing collaboration with a number of projects will facilitate the deployment of their applications on the TeraGrid.

16.1.4. Management Leadership

As Figure 2 shows, the TeraGrid management team will be drawn from the current PACI leadership, complemented by additional advisory groups, technical managers, and professional staff.

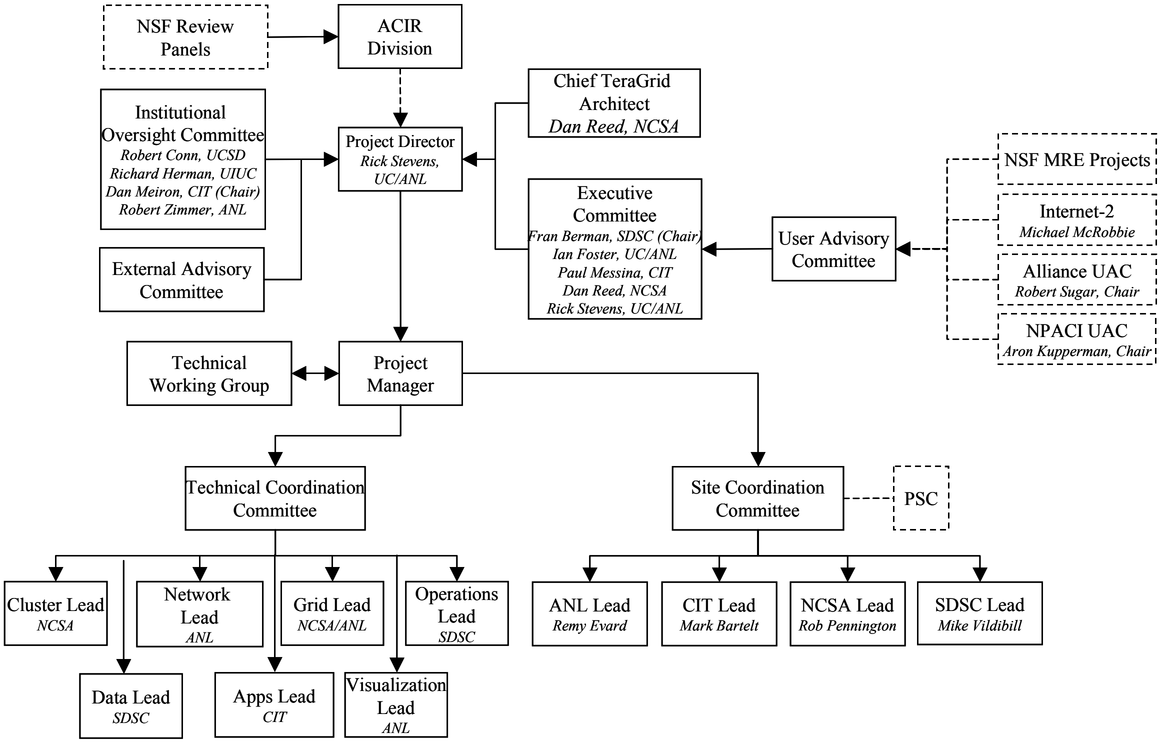
TeraGrid Project Manager

The Executive Committee and Project Director will recruit a full-time TeraGrid Project Manager (TPM). As an essential component of the TeraGrid management team, the TPM will report directly to the Project Director and have responsibility for day-to-day management and oversight of the distributed TeraGrid project. This responsibility will be realized through the implementation of the high-level project plans for the DTF TeraGrid, articulated to include specific implementation steps and time lines. The TPM also acts as chair of the Site Coordination Committee, composed of the TeraGrid Site Leads and the technical area leads (TALs); see below.

The TPM will report weekly progress to the Project Director and the Executive Committee via either teleconference or the Access Grid. The TPM will have general oversight and coordination responsibility for all key personnel supporting the project, regardless of their physical location. Support for the TPM will be provided via a dedicated full time administrative assistant.

Finally, a technical working group (TWG) will provide additional technical expertise to the TPM. These technical leaders (e.g., from both PACI and related Grid, cluster, and data management projects) will provide a longer timescale and independent perspective for the continued development of the components in the TeraGrid. In addition, the TPM will work directly with the technical leads via the Technical Coordination Committee.

The members of the TWG will be intimately familiar with the on-going research and development activities at the PACI sites – some will be drawn from PACI researchers and the DTF proposal senior personnel. The TWG will meet regularly with the TPM and the site leads during at least the first 18 months of the project and more frequently if the TPM deems necessary. Once the TeraGrid is operational, the TWG will review major planned changes to ensure that the best



available technologies are incorporated and to identify potential negative impacts.

Site Leads

Each partner site has identified and permanently assigned a TeraGrid Site Lead (TSL); see Figure 2. The TSL will oversee the activities (development and deployment) on site. Together, the four TSLs will constitute the site coordination committee, which will act as the leadership team of the TeraGrid Operations Center (TOC). These staff have been identified in each case based on a history of leadership within their sites as well as in the national community.

The coordination committee will identify the contents of new versions of the DTF software and hardware configuration. The software aspects of the TeraGrid will be under strict version control and a test and evaluation team will be formed populated by staff not part of the development efforts. Moreover, the TSLs will cooperate with PSC and TCS-1 to help ensure effective interoperation between the TeraGrid and TCS-1.

The TSLs will manage integrated software prototype deployment, with a period of friendly user testing prior to production deployment. This is the same strategy SDSC and NCSA use for deploying new compilers, tools, and other software – production versions remain in place during testing, with replacement only after a verification period.

All TSLs will meet weekly via teleconference or Access Grid with the TPM, and will update the principal investigator quarterly in writing on their progress. Due to the highly collaborative nature of the proposal, TSLs are also anticipated to have regular and frequent contact among one another via email, collaborative tools, and face-to-face meetings when necessary. The test results and other insights gained from the use of the TeraGrid systems will be conveyed to developers and users through workshops that will rotate among each of the DTF institutions.

Technical Area Leads

The project wide technical area leads (TALs) are charged with coordinating and deploying a consistent infrastructure across all four sites, in their specific technical domain (applications, clusters, networking, data management, visualization, Grids, and operations). Collectively, they report to the TPM as the Technical Coordinating Committee and coordinate their activities with the four site leads. As we move forward we will fill the TAL roles, either selecting members of our DTF senior personnel team, existing staff, or new staff recruited specifically for a given area.[1]

The TSLs and the TALs will work in a matrix management arrangement. The TSLs will be responsible for overseeing the development and deployment activities at their own sites and managing the operation of their TeraGrid node; in turn, the TALs will map the DTF-wide strategy, and work with the site leads to formulate the implementation plan. The implementation plan will be updated at least once a year and will include milestones and resources for each activity.

Through the TALs we will have clear lines of responsibility for each of the major activities in the DTF (applications, clusters, networking, data management, visualization, Grids, and operations). The TSLs make one person at each site responsible for realizing the implementation plan activities at that site, cutting across all the major activities.

Acting as the lead in a specific area, the TALs will work with the other leads and with technical staff at each organization to provide the best possible solutions. Specifically, the Cluster Lead works directly with the software and hardware specification and configuration of the computational cluster components at the sites. This will include working with the sites and the vendors to evaluate the available components and the site computational requirements as part of the DTF. In turn, the Data Lead works on the storage aspects common to all of the sites,

[1] Where multiple institutions are shown in Figure 2, we expect to jointly manage the technical area via experts from multiple institutions.

including secondary and tertiary storage components and software, as well as integration with the computational and Grid components. The Networking Lead is responsible for the overall networking design across the sites and for evaluating the plans for each site to interface to the TeraGrid network.

The Applications Lead works with application scientists to match their applications to the capabilities among and between the sites and to provide essential application feedback to the DTF deployment teams as applications exercise the capabilities of the TeraGrid. The Grid Lead coordinates deployment and extension of Grid software, as well as ensuring that TeraGrid software remains compatible with other Grids being deployed.

The Visualization Lead manages deployment of large-scale visualization and rendering hardware, as well as interoperable visualization and remote data access software at each of the sites. Finally, the Operations Lead coordinates the TeraGrid Operations Center, a joint activity of the four sites staffed primarily by SDSC and NCSA; see §**Error! Reference source not found.** for details on the TOC.

Deleted: Error! Reference source not found.

Project Oversight

The National Science Foundation, the Executive Committee, an Institutional Oversight Committee, the Chief TeraGrid Architect, and the External Advisory Committee will provide direct input to the Project Director.

Project Director

The construction and operation of the TeraGrid will be under the direction and supervision of a single Project Director, Rick Stevens, from University of Chicago/Argonne National Laboratory, who will manage and oversee the flow and distribution of resources for the entire project. The Project Director is expected to serve as the direct point of contact with NSF Officials for financial and management issues pertaining to the TeraGrid project.

Chief TeraGrid Architect

The Chief TeraGrid Architect, Dan Reed, will work with and advise the Project Director on strategic technologies, infrastructure, and approaches critical to successful deployment of the TeraGrid. In this role, he will focus on cluster hardware and software, Grid infrastructure, and the advanced networking technologies needed to support emerging Grid users and applications.

Executive Committee

An Executive Committee has been established for the project, consisting of the project co-investigators: Fran Berman (chair), SDSC; Ian Foster, UC/ANL; Paul Messina, CIT; Rick Stevens, UC/ANL; and Dan Reed, NCSA. This committee will provide advice to the project director on overall direction and strategy and make recommendations regarding high-level resource allocation in its advisory role.

Fran Berman, SDSC/NPACI director, has over 20 years of research leadership in parallel computing and computational Grids. Paul Messina, the NPACI chief architect, is known internationally for spearheading multidisciplinary high-performance computing projects, including the DOE Accelerated Strategic Computing Initiative. Ian Foster is one of the pioneers in computational Grid research, and, with Carl Kesselman, has led development of a series of releases of the widely used Globus Toolkit. Rick Stevens, the Alliance chief architect, has overseen generations of high-performance systems at UC/ANL and spearheaded Alliance work in Linux and open source software. Dan Reed has spearheaded development of performance tools for large-scale parallel systems as well as participated in collaborative projects with national Grid, parallel computing, and application groups.

External Advisory Committee

The DTF External Advisory Committee will be composed of leading national figures in the area of computer and computational science from both the public and private sector. The EAC will meet semi-annually to review the progress of the project and help identify future long-term technology and application thrusts for the project. This committee will be populated, in part, from advisory committee members for the Alliance and NPACI.

Institutional Oversight Committee

Member sites in the DTF proposal will establish an institutional oversight committee composed of Richard Herman, Provost, University of Illinois at Urbana-Champaign; Robert Conn, Dean, University of California at San Diego; Dan Meiron (initial chair), Associate Provost for Information & Information Technology, California Institute of Technology; and Robert Zimmer, Vice President for Research at Argonne National Laboratory, University of Chicago. The chair of the committee will rotate from Caltech to Illinois and then to UCSD on an annual basis. The committee will help resolve any institutional issues that arise in an expedited manner.

User Advisory Committee

The Executive Committee will establish a User Advisory Committee to provide guidance on desired DTF functionality. Membership will be drawn from the major NSF MRE sites, Internet 2, the Chairs of the Alliance and NPACI User Advisory Committee, and traditional supercomputing users and related projects from DOE and NIH.

The TeraGrid principals already have strong connections with projects such as GriPhyN, NEES, NVO, SDSS, ATLAS, CMS, and ASC. These groups and other communities have committed their staff to work with the DTF staff (a) to define the DTF software environment and operational policies, (b) to adapt their applications to take advantage of the TeraGrid environment, and (c) to test and evaluate the capabilities as they are installed on the TeraGrid. These commitments are documented in a number of the letters of support that were enclosed in the original proposal and as well as additional letters attached. We have found over many years of work that the structured and long-term engagement of advanced user communities such as these is a highly effective mechanism for determining real user requirements.

16.1.5. Meetings, Reviews, and Corrective Actions

Internal management meetings will occur on a weekly basis during the term of this project. The purpose of these meetings is to monitor project performance and to identify as early as possible any changes in risk profiles or other aspects that might require a change in the technical, cost or schedule baselines. Given the distributed nature of the TeraGrid participants, we will use the PACI Access Grid and video teleconferencing technologies to support remote participation in management functions. Both NPACI and the Alliance currently have such weekly meetings of the high-level management team. These meetings have proved to be extremely successful distributed management mechanisms.

Internal management meetings include:

- Management team meetings, conducted by the TeraGrid Project Director and involving the Executive Committee and TeraGrid Chief Architect,
- Site Coordination Committee meetings conducted by the Project Manager, and

- Overall Technical and Site Coordination Committee meetings, conducted by the TeraGrid Project Manager (TPM) and involving both the technical area leads (TALs: applications, cluster, networking, data, visualization, Grid, and operations) and technical site leads (TSLs: NCSA, SDSC, UC/ANL, and CIT).

External meetings include

- External Advisory Committee meetings, which will be semi-annually
- User Advisory Committee meetings, which will also be semi-annually, held in conjunction with the Alliance and NPACI UAC meetings.

In all areas of software development or TeraGrid components with high technological risk, walkthroughs will be performed sufficiently early in the systems integration process to ensure that no project failure modes exist. Such early walkthrough meetings will be one of the most important mechanisms for creating the baseline risk assessments.

The performance of all project technical and management teams will be measured by their meeting approved milestones according to the agreed upon timelines and within the allocated budgets. In addition, the Project Manager will monitor progress toward milestones, and evaluate on a monthly basis if any project components are at risk. The Project Manager will present this assessment to the Project Director and Executive Committee for discussion and action, if appropriate.

17. Appendix B Sample Contract

Contractor Service Agreement

Contractor Name and address:

____

____

____

(hereinafter referred to as "CONTRACTOR") contracts to provide services (hereinafter referred to as "the Service(s)") and COMPANY/ORGANIZATION, (hereinafter referred to as "RECIPIENT") by its acceptance and execution hereof, contracts to furnish the Services as specified on Schedule A.

This Agreement becomes affective on the date it is executed by CONTRACTOR and RECIPIENT.

The parties agree as follows:

PART-1 SERVICE TO BE PROVIDED

1. SERVICES AND PAYMENT

CONTRACTOR agrees to perform the Services described on Schedule A. As consideration for CONTRACTOR's Services, RECIPIENT agrees to pay CONTRACTOR the amounts set forth on

Schedule B, at the times and in the manner set forth on Schedule B. The total value of the Agreement is specified on Schedule A. No work in excess of this amount will be paid for by RECIPIENT without the prior written approval of a duly authorised representative of RECIPIENT.

2. TERM

The term of the Agreement shall be a specified on Schedule A, subject to the termination provisions of Article 13. It may be extended beyond this term subject to the consent of both parties.

3. LOCATION OF WORK

The location of the work shall be a specified on Schedule A.

RECIPIENT shall inform all CONTRACTOR personnel carrying out work at its premises of all relevant procedures relating to security, discipline, fire, and health and safety. CONTRACTOR shall ensure that its personnel observe such procedures.

4. OBLIGATIONS OF CONTRACTOR

CONTRACTOR undertakes to provide the following during the course of the Agreement:

- Carry out the Services specified on Schedule A;
- Provide a nominated Manager to oversee the Services;
- Prepare reports on a regular basis as specified on Schedule A, including a final report to be prepared on conclusion of the Services;
- Return to RECIPIENT, either prior to or on termination of the Agreement, all manuals, equipment, materials or other property furnished by RECIPIENT;
- Carry out additional obligations (if appropriate) as specified on Schedule A.

Personnel assigned by CONTRACTOR to perform the Service shall be CONTRACTOR employees and shall be suitable qualified for the work to be carried out; CONTRACTOR shall assume all applicable employer responsibilities and the Agreement shall not be deemed to imply any employer-employee relationship between RECIPIENT and such personnel. This Agreement will not prevent CONTRACTOR from performing similar Services for others.

In the event the CONTRACTOR wishes to change the personnel assigned to the delivery of the Services, CONTRACTOR will at all times give RECIPIENT reasonable notice of such changes and shall make all reasonable endeavour to keep the duration and impact of such changes to a minimum. CONTRACTOR personnel shall be entitled to take annual leave entitlement in accordance with CONTRACTOR's standard policies. RECIPIENT will be given reasonable notice of any absences due to annual leave or other foreseen circumstances.

5. OBLIGATIONS OF RECIPIENT

For Services to be provided at RECIPIENT premises, RECIPIENT agrees to provide free of charge adequate working conditions for CONTRACTOR personnel. This includes:

- sufficient office space and office furniture, including a telephone for business use;
- at least a lockable cabinet for storing CONTRACTOR proprietary or confidential information, such as documentation, computer listings and magnetic media (tapes, disk cartridges, etc.);
- appropriate equipment to access the appropriate computer systems;
- reasonable and sufficient amount of access to appropriate computer systems. This time will be used by CONTRACTOR personnel to perform task related to the Services. The amount and periods of such access will be mutually agreed upon between CONTRACTOR and RECIPIENT.

RECIPIENT undertakes to provide the following during the course of this Agreement:

- provide a nominated manager to receive reports and to act as a point of contact for all technical questions;
- provide adequate technical information, standards and timing information at start and completion of Services, as specified in Schedule A;
- sign a Completion of Services' Notification promptly on completion of the Services;
- carry out addition obligations (if appropriate) as specified on Schedule A.

6. OWNERSHIP OF INTELLECTUAL PROPERTY RIGHTS

All original written material including programs, tapes, listings, and other programming documentation originated and prepared for RECIPIENT pursuant to this Agreement shall belong exclusively to RECIPIENT. The ideas, concepts, or techniques relating to data processing developed in the performance of this Agreement by CONTRACTOR personnel or jointly by CONTRACTOR and RECIPIENT personnel can be used by either party in any way it may deem appropriate. Each invention, discovery, or improvement which includes ideas, concepts, or techniques relating to data processing developed pursuant to this Agreement shall be treated as follows:

- if made by RECIPIENT personnel, it shall be the property of RECIPIENT;

- if made by CONTRACTOR personnel, it shall be the property of CONTRACTOR, however CONTRACTOR grants to RECIPIENT a non-exclusive, irrevocable, and royalty-free licence throughout the world;

- if made jointly by RECIPIENT and CONTRACTOR personnel, it shall be jointly owned by each party without accounting to the other party.

Notwithstanding the above, any written material (including programs, tapes, listings, and other programming documentation), invention, discovery, improvements, idea, concept, or techniques which include any portion of RECIPIENT or Cray Research Inc software shall remain the property of its owners and is not licensed to CONTRACTOR. This Agreement shall not preclude RECIPIENT from developing materials which are competitive, irrespective of their similarity to material which might be delivered by CONTRACTOR pursuant to the Agreement.

7. CONTRACTOR WARRANTY

CONTRACTOR warrants that it will make diligent efforts to provide the Services in accordance with the terms and conditions of this Agreement.

Except as otherwise required by law, the express warranty set forth above is the exclusive warranty and is in lieu of all implied warranties of fitness for a particular purpose and merchantability.

The total of CONTRACTOR'S liabilities under or in conjunction with this Agreement and whether arising from negligence or contract of howsoever is limited in respect of each event or series of connected events as follows:

- for damage to physical property the sum $250,000 plus the obligation to make good by repair or replacement any equipment damaged by the negligent act or default of RECIPIENT, its servants or agents;

- for all other events (excluding injury to or the death of any person to which no limit applies) the sum of $50,000.

8 RECIPIENT WARRANTY

When any computer program material to which rights are owned by a third party are to be disclosed to CONTRACTOR in connection with the Services by RECIPIENT, RECIPIENT warrants that it has any necessary permission, express or otherwise, to enable it to disclose it to CONTRACTOR, or otherwise use such computer programs, without infringing said third party's rights and agrees to indemnify and hold CONTRACTOR harmless from all liability in connection therewith.

Recognising that RECIPIENT will make many choices of application and users without control by or knowledge of CONTRACTOR, RECIPIENT agrees to indemnify and hold CONTRACTOR harmless in respect of any and all claims or liability to third parties arising from the use of any software developed or modified under the terms of this Agreement.

PART 2 - GENERAL CONDITIONS

9. CONFIDENTIALITY

The parties recognise that in the course of performance of this Agreement each may be exposed to or come into possession of confidential or proprietary material of the other. When such material is in illustrated or written form, marked as confidential or proprietary, or when it is disclosed orally, identified at the time as confidential, and identified as confidential or proprietary in writing to the receiving party with twenty (20) days after disclosure, then the material shall be protected and held as confidential by the receiving party to the same extent that party protects its own confidential or proprietary material.

This obligation shall continue for a period of five (5) years following receipt of the material and shall survive any termination of this Agreement, but it shall not cover any information which:

- is disclosed to a third party, by the disclosing party, without restriction on disclosure;

- has been or is developed independently by the receiving party without violation of obligations of confidentiality is rightly in the possession of the receiving party at the time of disclosure by the disclosing party.

Provided, however, that RECIPIENT shall be obligated to maintain software proprietary to CONTRACTOR, documentation therefor, and concepts and information contained therein in confidence (in accordance with terms of the licence agreement covering such software) and that such obligation of confidentiality shall not end after the above-mention five (5) year period but shall continue thereafter and shall survive and continue after any termination of this Agreement.

10. FORCE MAJEURE

Neither party shall be liable to the other for any failures to observe any of the conditions of this agreement, expect as expressly provided to the contrary herein, if the party can show that the cause is beyond its reasonable control and without its fault or negligence, provided that the party promptly notifies the other party of any failure or anticipated failure as soon as it is known and resumes performance as soon as possible thereafter.

11. INVOICES AND PAYMENT

Invoices will be issued as specified in Schedule B and will be due and payable within thirty (30) days from date of invoice.

12. ADDITIONAL CHARGES

In addition to charges provided for elsewhere in the Agreement, all taxes including but not limited to Value Added Tax, however designated (exclusive of income taxes), and amounts levied in lieu thereof, based on or measure by the charges set forth in the Agreement for the Services provided herein, now or hereafter imposed by any Government authority, will be invoiced to and paid by RECIPIENT as they are accrued and incurred.

13. TERMINATION

This Agreement and the obligations of the parties hereunder, except for the provisions of Articles 6 and 9, will terminate upon the earliest completion of the Services by CONTRACTOR or

(a) if RECIPIENT suffers distress or execution or commits an act of bankruptcy or a petition is presented or a resolution is passed to wind up RECIPIENT (other than for purposes of reconstruction or amalgamation) or if a receiver is appointed over any part of RECIPIENT business or

(b) default by RECIPIENT in payment of any sum due under this Agreement and failure of RECIPIENT to sure such default within ten (10) days after written notice to RECIPIENT of such default or

(c) failure of RECIPIENT to fulfil any material obligation under this Agreement.

Termination of this Agreement by CONTRACTOR shall be without prejudice to any other remedies CONTRACTOR may have, including, without limitation, all remedies with respect to the unperformed obligations of RECIPIENT, including its obligation to pay all accrued charges due as of the date of termination.

Additionally it may at any time be terminated on 90 (ninety) days advance written notice subject to the consent of both parties. In the event of such early termination RECIPIENT will be invoiced for and will pay for all Services carried out by CONTRACTOR up to and including the date of termination as well as for all commitments entered into before the notice of termination was agreed.

14. ASSIGNMENT

Neither party may assign this Agreement in whole or in part, without the written consent of the other party. Such consent shall not be unreasonable withheld.

15. APPLICABLE LAW

This Agreement is governed by the laws of England, and any legal action instituted in connection with it shall be subject to English law. No action, regardless of form, including but not limited to claims in contract, tort or breach of warranty, arising out of or in connection with the transactions under this Agreement, may be brought by either party more than two (2) years after the cause of action has accrued.

16. NOTICES

Any notice required or permitted hereunder shall be effective when received in writing by the party to be charged with notice, and shall be sent to the person and address designated on the signature page of this Agreement or such other person or address as may have been furnished to CONTRACTOR or RECIPIENT, according to this article.

17. ENTIRE AGREEMENT

The provisions stated herein, including Schedules A and B, constitute the complete and exclusive statement of the Agreement between CONTRACTOR and RECIPIENT, and shall supersede all prior oral and written statements of any kind whatsoever made by wither party or their representatives including any order from CONTRACTOR or RECIPIENT. No statement or writing purporting to modify or add to the provisions hereof shall be binding unless consented to in writing by duly authorised representatives of CONTRACTOR and RECIPIENT. All references to figures, schedules, and attachments refer to the most recent amendments thereof; any notice of new prices or changes by CONTRACTOR under terms hereof shall for these purposes by deemed an amendment of the precious price list, schedule, or attachment. Failure to enforce any provision of this Agreement will not be deemed a waiver of such provision.

18. Appendix C - Article XVII - Rights in Data and Intellectual Property

18.1. A. Definitions

For the purposes of this Article XVII, “NSF-Funded Alliance Partner(s)” refer only to those institutions, nonprofit research organizations or consortiums receiving NSF funding under Cooperative Agreement No. ASC97-40300. The University of Illinois may also be an NSF-Funded Alliance Partner.

18.2. B. Rights in Data

Original data and records of research projects funded under this Subaward Agreement shall belong to the NSF-Funded Alliance Partner(s) that created it. Original data and records of research projects will be retained by the NSF-Funded Alliance Partner for a period of three (3) years after termination of each research project that generated it. Copies will be furnished to the University upon request. The University shall have the unrestricted right to use all data which is delivered to the University by the NSF-Funded Alliance Partner for non-commercial purposes, unless more restrictive rights are otherwise specified in writing on a case-by-case basis.

18.3. C. Sharing of Findings, Data, and Other Research Products

In order to facilitate collaboration within the Alliance, University and NSF-Funded Alliance Partner agree that sharing of findings, data and other research products from research projects funded under this Subaward Agreement shall be in accordance with Article 36, Sharing of Findings, Data and Other Research Products, of GC-1, and GPM Section 734, Dissemination and Sharing of Research Results.

18.4. D. Protection of Confidential Information

Prior to disclosure by the University or NSF-Funded Alliance Partner of its confidential information required for the performance of an Alliance-funded research project, it is the responsibility of the owner of such confidential information to secure a written non-disclosure agreement with those persons who have a "need to know" such confidential information (or the institution that employs such persons, if applicable).

18.5. E. Rights to New Intellectual Property Created Under This Subaward Agreement

1. For purposes of this Subaward Agreement, "Intellectual Property" shall mean inventions, patents, copyrights, software (whether protected by copyright and/or patent), trademarks, trade secrets and other forms of intellectual property subject to statutory protection.

2. Ownership of Copyrightable Material

The subset of Intellectual Property that is copyrightable material (i.e., "subject writings" as defined in Article 18 of GC-1) created in the performance of research projects funded under this Subaward Agreement shall be subject to Article 18, Copyrightable Material, of GC-1, and Section GPM Section 732, Copyright. Such copyrightable material shall be owned by the University or the NSF-Funded Alliance Partner or their employee(s) that created it, in accordance with the employer's policies. Copyrightable works created jointly by employees from more than one institution shall be jointly owned.

3. Ownership of Inventions and Patents

The subset of Intellectual Property that is inventions and patents resulting from the performance of research projects funded under this Subaward Agreement shall be subject to Article 21, Patent Rights, of GC-1 and GPM Section 731.3, Standard Patent Rights Clause. This subset includes software inventions that are eligible for patent protection. Ownership of inventions and patents resulting from collaborative efforts between employees of more than one institution shall be determined in accordance with the U.S. laws of inventorship, i.e.: inventions and patents made solely by employee(s) of the University or an NSF-Funded Alliance Partner shall be owned by the employing institution; inventions and patents made jointly by employees of more than one institution shall be jointly owned by the employing institutions.

4. Ownership of Other Intellectual Property

All Intellectual Property resulting from the performance of research projects funded under this Subaward Agreement that is not subject to Article XVII E.2 or XVII E.3 above shall be owned by the employee(s) that created it or their employing institution(s), in accordance with the employer's policies.

5. Minimum License Rights for the Alliance

Due to the collaborative nature of research projects under the Alliance, the parties agree that, unless otherwise agreed to by the parties in writing, all Intellectual Property resulting from the performance of research projects funded under this Subaward Agreement shall be provided by the owner(s) to the University and to the other NSF-Funded Alliance Partners with a minimum non-exclusive, royalty-free license to use such Intellectual Property for academic and research purposes of the Alliance Program, but not for commercial purposes. The owner(s) of such Intellectual Property may provide such Intellectual Property with greater than minimum rights on a case-by-case basis, at the owner(s)' discretion.

6. Greater Than Minimum License Rights

Commercial license rights to Intellectual Property resulting from the performance of research projects funded under this Subaward Agreement, and the right to sublicense or distribute such Intellectual Property to third parties who are not NSF-Funded Alliance Partners, shall be controlled by the owner(s) of the Intellectual Property. Except for the license rights provided in Article XVII E.5 above, neither the University nor the NSF-Funded Alliance Partner shall have any right to use the Intellectual Property of another NSF-Funded Alliance Partner for any other purpose without the express written permission of the owner(s) of such Intellectual Property.

7. Commercial Exploitation of Jointly Owned Intellectual Property

University and NSF-Funded Alliance Partner acknowledge the collaborative nature of research projects in the Alliance and the organization of Alliance Teams to accomplish mutual goals and objectives. Due to such collaboration, the parties recognize the potential for joint development or joint creation of Intellectual Property that will be co-owned by the more than one institution. University and NSF-Funded Alliance Partner agree that inter-institutional cooperation, whether between University and NSF-Funded Alliance Partner or between NSF-Funded Alliance Partner and other institution(s), is necessary in order to protect such jointly owned Intellectual Property in a timely manner and to facilitate commercial development and marketing. University and NSF-Funded Alliance Partner agree to use reasonable efforts to undertake the disclosure, protection and commercial development of any such jointly owned Intellectual Property, as further specified in *Attachment 1, Protection and Licensing of Jointly Owned Intellectual Property* (attached hereto and incorporated herein).

18.6. F. Background Intellectual Property

1. For purposes of this Subaward Agreement, "Background Intellectual Property" shall mean Intellectual Property that was created or developed prior to this Subaward Agreement by employees of the University or an NSF-Funded Alliance Partner, or that is developed independently by employees of the University or an NSF-Funded Alliance Partner during the term of this Subaward Agreement without funding under the Subaward Agreement, or that is owned or controlled by a third party, but which is needed by the University or NSF-Funded Alliance Partner(s) in the performance of research projects funded under this Subaward Agreement.

2. University and NSF-Funded Alliance Partner acknowledge that Background Intellectual Property may be owned by either party, their respective employee(s) and/or assigns, or third parties, and/or that such Background Intellectual Property may currently be (or during the term of this Subaward Agreement, may become) subject to licenses to third parties that restrict use of such Background Intellectual Property without the express consent of the licensee.

3. It is the responsibility of the University or NSF-Funded Alliance Partner performing an Alliance-funded research project to assure that it has cleared the rights and permissions sufficient to use Background Intellectual Property with the party(ies) that control such rights, prior to use of such Background Intellectual Property by its employee(s).

18.7. G. Institutional Contacts for Intellectual Property

The Institutional Contacts for Intellectual Property of the University and the NSF-Funded Alliance Partner for issues related to identification, protection and licensing of Intellectual Property are specified in *Attachment 2, Intellectual Property Contact Information* (attached hereto and incorporated herein).

Attachment 1

Protection and Licensing of Jointly Owned Intellectual Property

1. Intellectual Property: For purposes of this Subaward Agreement, "Intellectual Property" shall mean inventions, patents, copyrights, software (whether protected by copyright and/or patent), trademarks, trade secrets and other forms of intellectual property subject to statutory protection.

2. Cooperation for Management of Jointly-Owned Intellectual Property:

The Alliance research program involves scientists working in inter-institutional Teams where each Team member may be employed by a separate, independently governed organization or institution. Therefore, due to the application orientation of the research program and the high degree of networking and collaboration among Alliance Team members, it is likely that Intellectual Property will arise from Alliance-funded research projects that is created or developed jointly by employees of more than one NSF-Funded Alliance Partner and/or the University. In accordance with Article XVII of the Subaward Agreement, such Intellectual Property will be jointly owned by two or more entities.

U.S. patent law entitles each owner of a joint invention to independently exercise its rights as if it were a sole owner. Further, under U.S. copyright law, co-owners of jointly owned works have an independent right to use or license the use of the work, subject to a duty of accounting to the other co-owners for any profits. In practice, the independent management by one co-owner of jointly owned Intellectual Property generally precludes exclusive licensing, which could be a barrier to effective and timely commercial development.

In order to facilitate the goals of the Alliance and NSF, the University and the NSF-Funded Alliance Partners agree to cooperate to facilitate timely and efficient disclosure, evaluation, protection and commercialization or other public use of jointly-owned Intellectual Property.

The University will maintain an electronically accessible database of Institutional Contacts for Intellectual Property, as specified *in Attachment 2, Intellectual Property Contact Information.*

3. Disclosure of Intellectual Property

A. It is the responsibility of participating researchers on each funded project to disclose Intellectual Property to the designated Principal Investigator of the project. It is the responsibility of the Principal Investigator to disclose Intellectual Property to the Institutional Contact for Intellectual Property at his/her institution as follows:

- When such Intellectual Property results from an Alliance-funded research project under the direction of the Principal Investigator; and

- When such Intellectual Property results from collaboration with one or more NSF-Funded Alliance Partners and/or the University.

The disclosure should identify all known co-inventors or co-authors and their institutional affiliations.

B. As the default, the institution that employs the Principal Investigator under whose Alliance-funded research project the Intellectual Property was made will take the lead in administering the disclosed Intellectual Property ("Lead Institution"), and the Institutional Contact for Intellectual Property at the Lead Institution will coordinate follow-up with the other institutions who are believed to be co-owners of the Intellectual Property. However, in the event the Principal Investigator's institution does not want to assume lead institution responsibilities, it shall promptly notify the other institutions believed to be co-owners, who shall collectively select an alternate institution from among them to act as the lead institution on their behalf.

(1) The Lead Institution will forward a copy of the disclosure to the Institutional Contact(s) of the other identified co-inventors or co-authors, who shall in turn notify the employee(s) at their own institution.

(2) For the subset of Intellectual Property that is inventions and patents, unless otherwise agreed, the Lead Institution shall be responsible for disclosing the invention to the NSF, and for notifying the NSF regarding the decision whether or not to elect title, and providing copies of resulting patents and the confirmatory license, and compliance with the other terms of Article 21, Patent Rights, of GC-1, on behalf of all institutions that are co-owners of the invention. Copies of correspondence between the Lead Institution and NSF shall be provided by the Lead Institution to the Institutional Contacts of the other co-owning institutions.

(3) It is the responsibility of each institution to secure the rights from its own employees who are co-inventors or co-authors of a jointly-owned Intellectual Property sufficient to meet the requirements of the Alliance and NSF Cooperative Agreement No. ASC 97-40300. The Institutional Contacts will facilitate execution of paperwork required for protection and/or licensing of jointly-owned Intellectual Property from its own employees and/or authorized institutional representatives, as needed.

(4) The Lead Institution will report such information to the University regarding the jointly-owned Intellectual Property as may be required by Article II(B), Reporting, of the Subaward Agreement.

4. Protection and Commercial Development of Jointly-Owned Intellectual Property

The Institutional Contact at the Lead Institution will consult with the Institutional Contacts of the other co-owners of the jointly-owned Intellectual Property for the purposes of determining decisions related to evaluation, protection and commercialization of such Intellectual Property. The parties shall negotiate the issues, in good faith, including but not limited to the following:

- Evaluation of the commercial potential of such Intellectual Property.
- Review of the Intellectual Property to accurately identify all persons who made intellectual contributions to the creation or development of the Intellectual Property, and what such contributions are, including but not limited to identification of all legal inventors. For all persons so identified, notify their Institutional Contact for Intellectual Property.
- For potentially patentable inventions, whether or not to seek patent protection and, if affirmative, in what countries.
- Identification of counsel to handle the patent filing and prosecution or other protection (e.g., copyright or trademark registration), if applicable, and the co-owners' review rights and access to copies of paperwork and information associated with intellectual property protection.
- Sharing of expenses related to protection of the jointly-owned Intellectual Property.
- Development of a collaborative strategy for commercial development of the jointly-owned Intellectual Property, if warranted. May involve designation of a lead entity (which may be different than the Lead Institution) from among the group of co-owners to act on their behalf collectively in implementing the commercialization plan.
- Sharing of revenue and/or equity received from commercialization of the jointly-owned Intellectual Property, which may include reimbursement of expenses associated with protection and commercialization efforts.
- Such other terms and conditions as may be needed on a case-by-case basis.

The parties agree to reduce such mutual understandings to writing, in a document that will be signed by an authorized representative at each co-owning institution.

Attachment 2

Intellectual Property Contact Information

The principal role of the Institutional Contact for Intellectual Property is to act as the point of contact to work with the Institutional Contacts at other institutions for matters related to disclosure, evaluation, protection and commercialization of jointly-owned Intellectual Property, and to provide information on Intellectual Property required for the University's database.

Institution: Board of Trustees, University of Illinois

Institutional Contact for Intellectual Property:

Name: Sharon Tipsword

Title:

Address: Assistant Vice Chancellor for Research

Research and Technology Management Offic

4th Floor Swanlund, MC-304

Champaign , IL , 61820

2173337862

Telephone:

2172443716

Fax:

stipswor@uiuc.edu

Email: