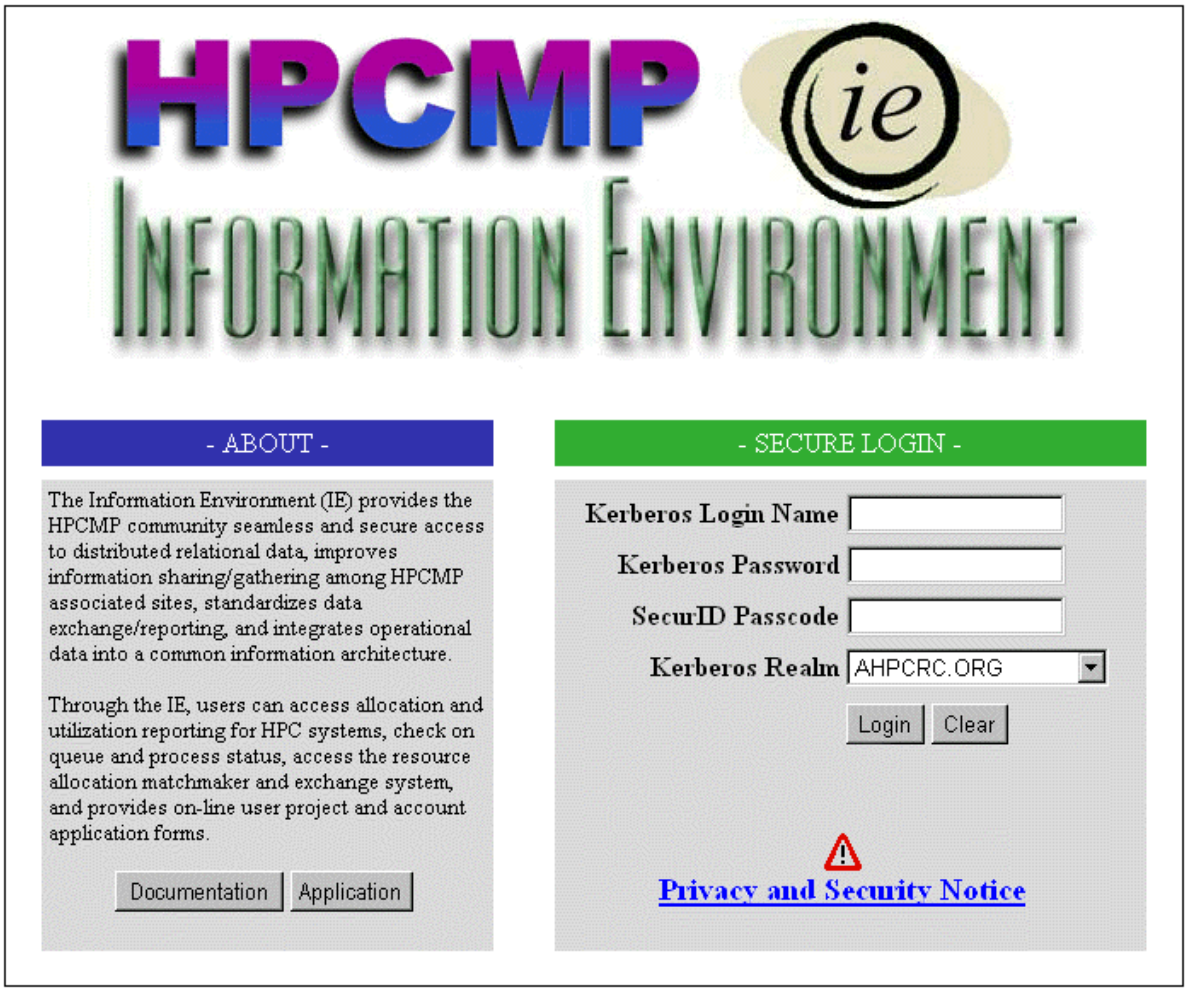
# Technical Proposal
## for a
# DoD High Performance Computing Modernization Program
# Information Environment
## (Solicitation 4TS-TT-01-0001)





**Submitted by**

**Network Computing Services, Inc.**
**1200 Washington Avenue South**
**Minneapolis, MN 55415**

## TABLE OF CONTENTS

# A. INTRODUCTION

This Network Computing Services, Inc. ("NetworkCS" or "The Contractor") proposal is for the development and implementation of an Information Environment (IE) that will enable the Department of Defense (DoD) High Performance Computing Modernization Program (HPCMP), Service Agency Approval Authorities (S/AAA), and users to have secure query and update access to user, allocation, and HPCMP high performance computing (HPC) system resource usage data. The proposed IE uses web technology to provide interactive access to an extensible and scalable database architecture and is fully compliant with DoD and HPCMP security requirements.

This proposed architecture relies on proven products: a web-based access sub-system with a user authentication and data encryption system that has already been evaluated by the HPCMP and found to meet or exceed HPCMP security requirements, and commercially proven third party commercial-off-the-shelf (COTS) software. The architecture is standards compliant.

The implementation of this architecture is a low risk investment by the HPCMP because:

1. NetworkCS, as the infrastructure support contractor for the Army High Performance Computing Research Center (AHPCRC) Distributed Center (DC) since 1989, fully understands the IE requirements of the HPCMP as stated in the Statement of Work (SOW).
2. NetworkCS has provided allocation based utilization controls on AHPCRC systems since 1991.
3. NetworkCS has previously developed and implemented relational database information environment tools to securely satisfy AHPCRC utilization, allocation and reporting requirements.
4. NetworkCS has provided web-based S/AAA access to usage and allocation information since 1998.

Based on this prior experience, NetworkCS is in a unique position to implement an IE that satisfies the performance and schedule requirements of the SOW.

NetworkCS is proposing that the IE server be deployed and supported at the AHPCRC, at least through the warranty period. This would facilitate the deployment of the IE and expedite problem resolution. HPCMP database administrators would still have network access to the IE from the HPCMO, yet not need to have to support systems operation on a 24 by 7 basis. A description of the support facility is provided in Section 6.0.

# B. TECHNICAL APPROACH

## 1.0 ARCHITECTURE

The NetworkCS architecture for the proposed IE is shown schematically in Figure 1. (1) (Numbers in () are cross reference to SOW requirements. An index is provided in Section 9). The IE consists of the following major sub-systems:

(a) The SRC Data Transfer Sub-system (SDTS), a sub-system implemented on a computer located at each major shared resource center (MSRC) or DC (hereafter referred to as "shared resource centers" or "SRCs") that securely communicates to the server hosting the IE database located at a central site. The computer is referred to as the SRC Data Transfer Computer (SDTC).

(b) The Internal Data Transfer Sub-system (IDTS), a sub-system on the server hosting the IE database that communicates with the SDTC and the IE database sub-system (IEDBS).

(c) The IE Database Sub-system (IEDBS), an Oracle database engine that hosts and relates data in Contractor defined data tables.

(d) The Identification and Authentication Sub-system (IAS), a facility that provides for strong identification and authentication of interactive users.

(e) The Interactive User Sub-system (IUS), a set of five tools running on an Apache

**Figure 1.**

IE Architecture Diagram

See file NetworkCS.Arch.vsd (for a VISIO format file of the Architecture Diagram or NetworkCS.Arch.doc for a Word version of the Architecture Diagram

web-server and using Allaire's ColdFusion COTS products to support web-based, interactive access by users to the IEDBS. Each of these sub-systems is described below in more detail.

### 1.1. SRC Data Transfer Sub-system

The SDTS is the facility located at each SRC that communicates with, and transfers data between that SRC and the centralized IEDBS server. The SDTS is implemented on an SDTC. Each SRC must designate and provide one computer, at its site, to be its SDTC. The SDTS can be supported on a personal computer-based server, so there is no requirement for this computer to be dedicated to the IE activity. System support and responsiveness of the SDTC are the responsibility of the SRC. The SDTCs are the only non-user computers permitted to transfer data to or from the IEDBS.

Data transferred from the SDTC to the IDTS includes utilization and metrics data, and other data identified in the SOW. This SRC provided data is required to update and populate the IEDB on a daily basis.

In addition, HPC system queue data is to be transferred by the SRC from the HPC resource accounting systems to the SDTC and subsequently to the IDTS at 10-minute intervals. Each SRC is responsible for all aspects of transferring the data from its HPC resource accounting systems to the SDTC in a timely manner.

Each SRC is responsible for converting its site specific HPC system accounting data into an XML format that conforms to the NetworkCS specified Document Type Definition (DTD). Each SRC is also responsible for initiating the transfer of this data from the SDTC to the IDTS.

NetworkCS will deliver a set of sample programs that illustrate how to convert data to and from XML format. NetworkCS will also deliver sample programs for the transfer of data between the SDTC and the server hosting the IEDBS. These sample programs will be tested by the Contractor to run under

RedHat Linux or Solaris. They may also run on other systems with little or no modification. The SRC has the option to use the provided programs as templates for its own specific requirements or to develop their own. Each SRC is ultimately responsible for correctly providing required data in XML format. (2)

All data transfers between the SRC and the IEDBS, whether uploads or downloads, are initiated by the SDTS. All data transfers will be in XML format, using Secure Shell (SSH) RSA for authentication, and SSH for encryption. The SRC is responsible for providing and installing secure shell (SSH) client software on the SDTC.

### 1.2. Internal Data Transfer Sub-system

The purpose of the IDTS is to support the secure transfer of data between the SDTC and the IEDBS.

SDTCs will transfer data to and from the IEDBS by connecting to the IDTS. The IDTS will be implemented as an SSH server. The IDTS will verify that the files were completely and accurately transferred before the data is loaded into the IEDBS. Only authorized SDTCs will be able to connect to the IDTS. Each SDTC will have its own account on the IDTS computer. Clients will be authenticated using RSA authentication. Full shell access will not be permitted and only the commands necessary to transfer data will be available. The IDTS design does not permit individual user access.

Allocation balances, and changes to user, project, and allocation amounts will be downloaded by the SDTCs from the IDTS daily.

### 1.3. Database Sub-system

After careful analysis, NetworkCS has elected to propose a centralized database for the IEDBS. A centralized IEDBS minimizes design, development, implementation, and operational costs. The cost savings in these areas more than offset the cost of providing for enhanced

availability through the use of redundancy in hardware at a single site.

NetworkCS is also proposing to use Oracle as the IE's database engine. Oracle was selected as it is the premier COTS database system. It is widely used by most large financial institutions and within highly classified DoD installations because of its built in security features, and its scalability and extensibility in highly demanding production environments. In addition, Oracle is a proven, stable product with demonstrated high availability. Oracle provides for tight control of access to data with the use of logins and passwords and administrator assigned privileges, which determine what data may be accessed and what kind of access is allowed per login.

Oracle employs an internal mechanism for locking modifications to tables while another user or process is trying to modify the same data. Oracle provides for user query access to data while the database is being updated. Hence users are able to access the prior data as a new day's information is being added to the database. However, the new information will not be available until the update is completed. (9)

Access to the data in the IEDBS is controlled by strong identification and authentication and need-to-know (NTK). The security policy and implementation is provided in the Security section of this proposal (see Section 3.0).

Data integrity is maintained in the IEDB through the implementation of integrity rules at the data field level. Constraints such as type of data and size are applied to every field. Keys are defined on tables and referential integrity is enforced. For example, the IEDBS will not allow a user to be added to a project unless the project already exists in the IEDBS. Additional constraints, such as range checks and list checks (i.e., a site code is not valid unless it is in a given list) are to be implemented, as reasonable and practicable.

The IEDBS is the central repository for the retention of all Information Environment data. It consists of Contractor defined data tables, relationships, and rules pertaining to IE data about people, resources, projects, and usage. The successful development of the IE is dependent upon a thorough understanding of the requirements and the ability of the IE developers to translate that knowledge into an efficient database design. NetworkCS, with its twelve year experience as the support contractor for the AHPCRC and its prior experience in developing AHPCRC Resource Accounting System, (ARAS) for the AHPCRC, is uniquely positioned to rapidly develop, implement and deploy an optimally designed IE database structure. In the following sections, NetworkCS details the major elements of its proposed database layout.

### *1.3.1. Person Data*

An important feature of the IE architecture proposed by NetworkCS is the establishment of a mechanism for uniquely identifying a user across SRCs and systems. This capability is important because, at present, an individual may have more than one "username" and "usernames" are not necessarily unique across all HPCMP resources. The implementation proposed by NetworkCS does not require the user to change his username and it does not require the user to enter any additional information. Rather, the IAS creates an implicit "PersonID" from information in the IE based on existing HPCMP requirements that an HPCMP user can have only one Kerberos username and be homed at only one HPCMP Kerberos Realm.

All the information about a person, such as contact information from Section II of the application form, Kerberos login, and username is related through the implicit PersonID. Figure 2 shows an example of the data elements related through use of the PersonID.

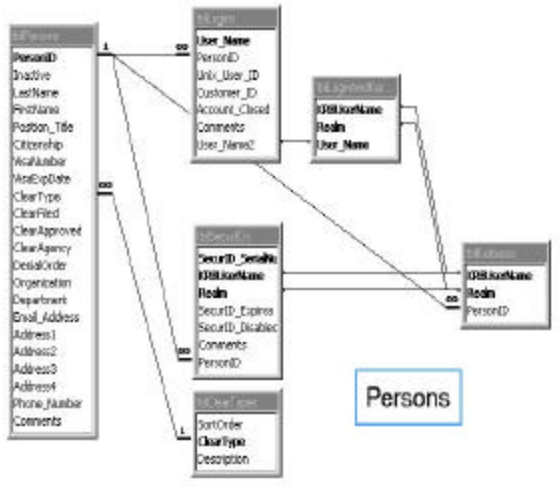



Figure 2. The NetworkCS proposed IE architecture creates a unique, implicit PersonID to link user data—even if the user has multiple usernames.

### *1.3.2. Projects and Rgroup Data Tables.*

Project data is information about HPCMP projects and includes the 13 digit project number and project information from Section I of the application form.

"Rgroup" data is information about the organizational relationships of the user, projects, and organizations within the HPCMP. It supports the creation of an unique tree structure per PersonID that defines the person's organizational relationships and is fundamentally important to generating the required DoD reports by project, organization, or service. It is also used to control access to IE data and services based on a person's NTK. Section 3.2 of this proposal provides additional information as to how Rgroup data tables are used to define the reporting tree structure and in enforcing NTK policy. Projects and Rgroup tables and relationships are pictured in Figure 3.

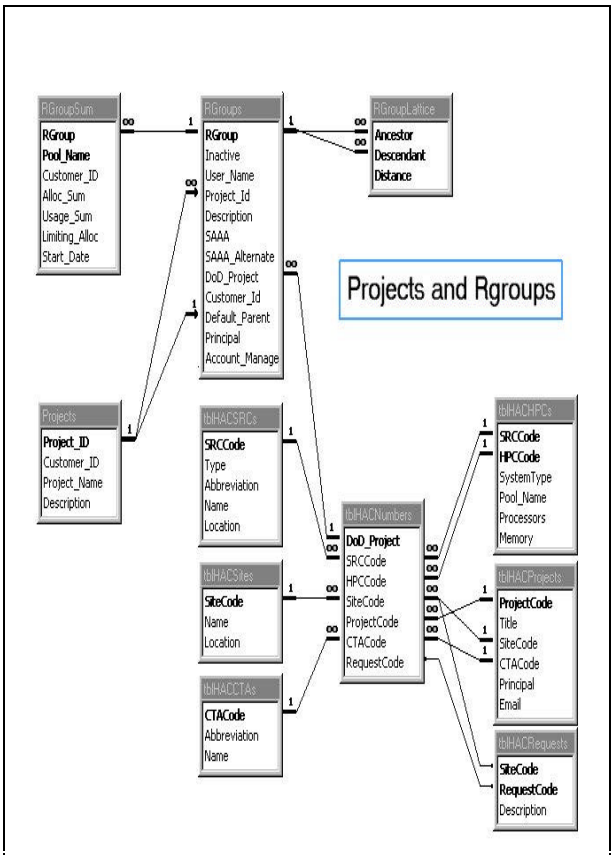



Figure 3. Projects and Rgroups data define all HPCMP projects and how they relate to users and organizations.

### *1.3.3. Usage, Allocation, Resource Data*

The resource data tables define and describe the HPC resources that are

available to the users. The allocation tables retain the original allocations per HPC resource and are updated daily to record the remaining allocation amounts. The usage tables maintain a record of when, how, and how much of each resource is used. Together, these tables provide the ability to produce the allocation and utilization reports required by the SOW including third party application software usage and expansion factor reports. The data tables and relationships for the usage, allocation, and resource data are shown in Figure 4.


Figure 4 – HPC resources are defined and their allocation and usage is recorded.

### *1.3.4. Holding Tables.*

The IEDBS has tables which contain pending Section I and Section II account applications awaiting S/AAA approval and a table for holding pending allocation exchange information from Tool 3. These tables provide for the tracking and modification of these transactions until the transactions are finalized. When transactions are finalized, the necessary data is transferred to tables previously discussed and to transaction history files. Then, the associated records are deleted from the holding tables.

### *1.3.5. Queue Status Tables.*

These tables contain current status of queues for each HPC system. This data is not stored long-term, but is overwritten with new data at each upload cycle.

### *1.3.6. Logging*

In addition to the data mentioned and shown in the tables above, every record in every table in the IEDBS will contain fields for tracking information about record

creation and modification. There will also be log tables to track IE transactions at a higher level (i.e., allocation, user fill-in, and account application management transactions). Reports may be generated from the fields in records or from the logs.

### 1.4. Identification and Authentication Sub-system (IAS)

The IAS is based on NetworkCS's Teraweb™ security module. The IAS provides for strong identification and authentication, based on SecurID and Kerberos, for access to the IE through web browsers. Teraweb was evaluated by the HPC Modernization Program Office (HPCMO) and meets HPCMP's requirements for data security and authentication. Additional information on the security implementation for the IAS and IE is provided in Section 3.0.

Other than a standard web browser (Netscape 4.7 or Microsoft Internet Explorer 5 or newer) with cookies and 128-bit encryption enabled, the NetworkCS design for the IE does not require any special or customized software or hardware on the user's desktop client. (48) Therefore, there are no operating system dependencies for client access, other than the ability to run a current web browser. (47)

Users gain access to the IE through the IE homepage. The IE homepage is publicly accessible on the World Wide Web. It displays the appropriate DoD notices regarding accessing Government web sites, acceptable use, and security and privacy information. An example of the homepage is shown in Figure 5. The homepage allows an individual to fill in a blank HPCMP account application form, or to log in as an authorized user.

To log into the IE, users are required to enter their Kerberos username, Kerberos password, SecurID passcode, and must select the appropriate HPCMP realm. All communication between the user's browser and the Teraweb authentication server is

encrypted with Secure Socket Layer (SSL). (13,45,46)


Figure 5. The IE homepage supports strong authentication for information access.

The IAS will store the user's Kerberos login information. The IAS communicates with the IEDBS to create a "PersonID". This information is used to provide the interactive tools and menus throughout the interactive session customized in accordance with user's NTK (Sections 1.5.1 and 3.2).

### 1.5. Interactive User Sub-system

Interactive tools are built on Allaire, Inc.'s ColdFusion product operating on an Apache SSL server. ColdFusion supports direct, real-time queries to the IEDBS for all user requested reports and information.

Based on the user's NTK, the IE provides to the user only those menus the user is authorized to use and only that data for which the user has authorized access. For example, as shown in Figure 6, after user "Wes Barris" successfully logs in to the IE, the IE displays a main menu page. The main menu page provides a "Welcome Wes Barris" confirmation note and displays the allocation and utilization summary for all "Wes Barris" accounts. In addition, it displays, in the upper left hand corner, "buttons" for available Tools. The buttons that are displayed are based on the person's NTK. So, for example, users who are S/AAAs or HPCMP management personnel see the management buttons shown on the main menu screen, but others do not.

The Interactive User Subsystem (IUS) uses the PersonID supplied to it by the IAS to control access to data in the IEDBS. Using this PersonID and information stored in the database, the IUS generates a tree of the "resource group" nodes to which the

person belongs or has access. Resource groups are entities such as DoD, Service and DoD Challenge Projects, Organization, Projects, and Users within projects. On the tree, a person is allowed read access to their ancestors and self, write access to their descendants, and look up access to their siblings. Additional information on the tree structure and its role in enforcing NTK is further described in the Security Section (Section 3.2).

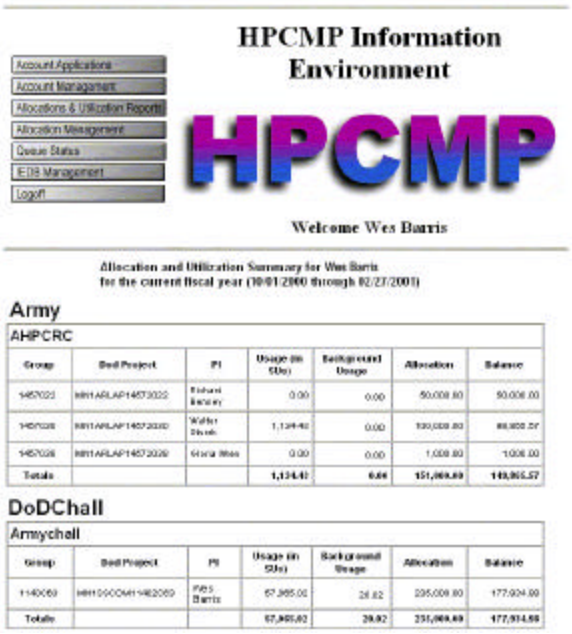



Figure 6 - The main menu provides quick access to the IE tools and allocation and usage information.

Figure 7 is an example of the DoD Challenge Projects tree available using the NetworkCS developed ARAS. Using this tree, the S/AAA with cognizance of DoD Challenge Projects is able to see the AHPCRC resources allocated and used by DoD Challenge Users. The tree is expandable and collapsible at the click of a button. So, by clicking on the DoD Challenge projects button, the S/AAA can see the next set of descendants (a list of Challenge Projects by Service/Agency). A click on any Challenge Project displays information on each of the users having sub-accounts on the Project. NetworkCS's proposed IE implementation provides the HPCMP with the same capability across all the SRCs included in the IE.

### *1.5.1. Tool 1: Allocation/Utilization*

The allocation/utilization tool provides users, PIs, S/AAAs, and HPCMO and SRC staff the ability to easily obtain information including project, allocation, utilization, and HPCMP utilization metrics. The same type

of tools were developed by NetworkCS for the AHPCRC environment and ARAS. For example, ARAS currently provides monthly allocation and usage reports by individual, project, organization, or service. Figure 8 is an ARAS allocation/usage query webpage. Usage is broken out by system and reportable for any given date range within the fiscal year. NetworkCS is able to demonstrate this tool in use at the AHPCRC to the HPCMP now. Building from this design, the HPCMP IE reports menu will have report choices and selection criteria available from a single page. (5)

Information from this Tool is limited by NTK criteria in accordance with the "Authority Rules" identified in Section 3 of this proposal. For example, S/AAAs are only able to obtain information on users and projects under their authority. Principal investigators (PI) are only able to obtain information on users in their projects. (13)

Allocation, utilization, user, project, and metrics information is available through

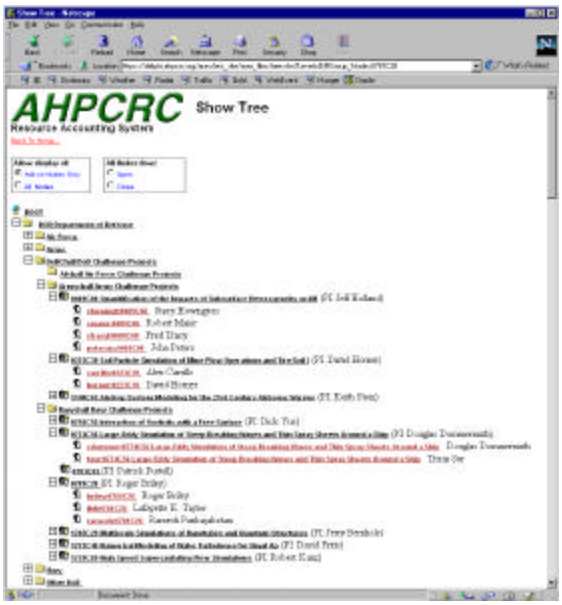



Figure 7. This view of the tree shows the relationship between users and Challenge Projects.

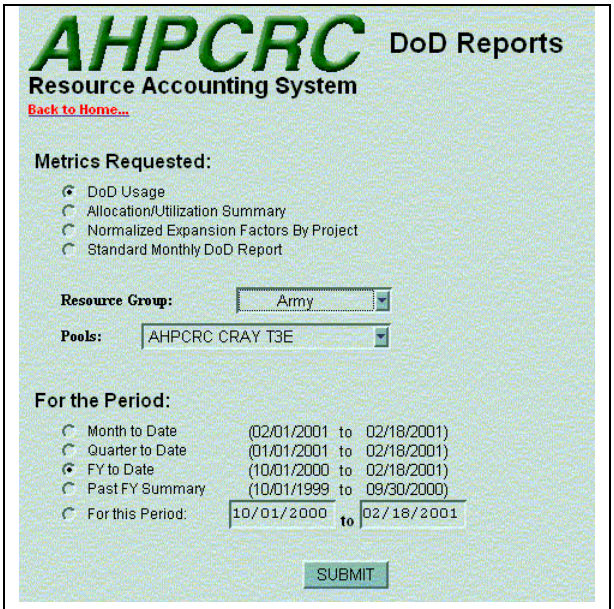



Figure 8. AHPCRC ARAS reports menu provides access to all reports in a single page.

Tool 1 for the current fiscal year and can be reported for year to date, month to date, and as a monthly summary, as well as by any

arbitrary date range within the fiscal year. Examples of Tool I type reports from ARAS showing, Expansion Factors and Utilization Metrics are provided in Figures 9 and 10. The IE is designed to archive detailed data three months after the close of the fiscal year, but continue to maintain summary information for an additional year. (11,12)

The IE provides reports on foreground and background utilization labeled by HPC system and by SRC.

The Allocation and Utilization tool also provides IE users with information about the HPC users and projects in the HPCMP. User contact information is provided to those with NTK. Allocation balances are calculated using foreground utilization only, but both foreground and background queue utilization is reported. Allocations and utilization are reported in processor hours and are labeled with the SRC and HPC system on which the utilization was generated. (7)

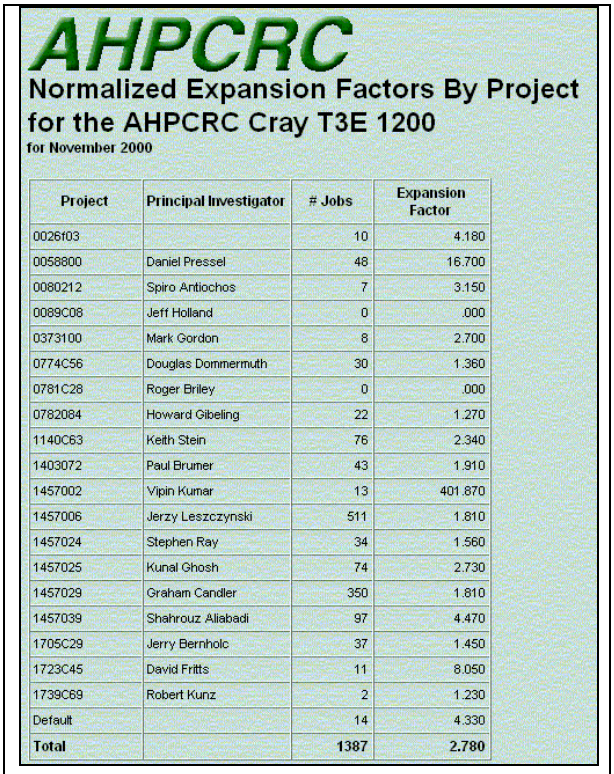
The ability to generate a variety of reports is provided in the IE. These include:

- Allocation/utilization reports for users and S/AAAs.
- Metrics reports including number of active users, number of cumulative users, un-normalized expansion factor, normalized expansion factors by queue and normalized expansion factors by challenge project.
- Application software usage reports including number of accesses to each program or library, CPU hours used on each COTS program, and number of load references for dynamic libraries.
- Standard utilization metrics report that all SRC send to the HPCMP monthly. (14-16)

The AHPCRC ARAS currently has the functionality to generate many of the reports requested in the SOW. This report generation capability was developed by NetworkCS for the AHPCRC to meet the reporting requirements of the HPCMP

An option is provided to users so that reports can be generated in a comma separated value (CSV) format that can be easily downloaded into a spreadsheet application. These reports are compliant with the requirements provided in the IE Utilization Metrics File Specification.

Users of the report generation facility are able to view reports by selecting the following options: Service/Agency; MSRCs only or DC; only; a specific SRC; a specific S/AAA; a project, a user; a HPC system; project type (Challenge, High Priority, Regular, Urgent, or Background); a CTA; and, foreground only or background only; utilization.



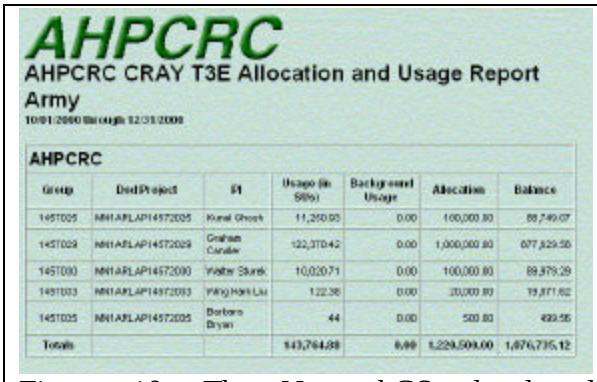
AHPCRC

Normalized Expansion Factors By Project for the AHPCRC Cray T3E 1200

for November 2000

| Project | Principal Investigator | # Jobs | Expansion Factor |
|---|---|---|---|
| 0026f03 | | 10 | 4.180 |
| 0058800 | Daniel Pressel | 48 | 16.700 |
| 0080212 | Spiro Antiochos | 7 | 3.150 |
| 0089C08 | Jeff Holland | 0 | .000 |
| 0373100 | Mark Gordon | 8 | 2.700 |
| 0774C56 | Douglas Dommermuth | 30 | 1.360 |
| 0781C28 | Roger Briley | 0 | .000 |
| 0782084 | Howard Gibeling | 22 | 1.270 |
| 1140C63 | Keith Stein | 76 | 2.340 |
| 1403072 | Paul Brumer | 43 | 1.910 |
| 1457002 | Vipin Kumar | 13 | 401.870 |
| 1457006 | Jerzy Leszczynski | 511 | 1.810 |
| 1457024 | Stephen Ray | 34 | 1.560 |
| 1457025 | Kunal Ghosh | 74 | 2.730 |
| 1457029 | Graham Candler | 350 | 1.810 |
| 1457039 | Shahrouz Aliabadi | 97 | 4.470 |
| 1705C29 | Jerry Bernholc | 37 | 1.450 |
| 1723C45 | David Fritts | 11 | 8.050 |
| 1739C69 | Robert Kunz | 2 | 1.230 |
| Default | | 14 | 4.330 |
| **Total** | | **1387** | **2.780** |

Figure 9. This report provides Normalized Expansion Factors organized by project.



AHPCRC

AHPCRC CRAY T3E Allocation and Usage Report

Army

10/01/2000 through 12/31/2000

AHPCRC

| Group | DodProject | PI | Usage (in SBUs) | Background Usage | Allocation | Balance |
|---|---|---|---|---|---|---|
| 1457025 | MHPCAP14572025 | Kunal Ghosh | 11,250.93 | 0.00 | 100,000.00 | 88,749.07 |
| 1457029 | MHPCAP14572029 | Graham Candler | 122,370.42 | 0.00 | 1,000,000.00 | 877,629.58 |
| 1457030 | MHPCAP14572030 | Walter Sturek | 10,020.71 | 0.00 | 100,000.00 | 89,979.29 |
| 1457033 | MHPCAP14572033 | Wing Hong Liu | 122.36 | 0.00 | 20,000.00 | 19,877.64 |
| 1457035 | MHPCAP14572035 | Barbara Bryan | 44 | 0.00 | 500.00 | 456.55 |
| Totals | | | 143,764.88 | 0.00 | 1,220,500.00 | 1,076,735.12 |

Figure 10. The NetworkCS developed ARAS already generates many of the reports requested in the SOW.

These options are posted on the web page in a pop-up menu and are available for all of the reports in the IE. (5,6)

Another menu allows the user to select various reporting periods such as: specific run date; or a range of dates within the current fiscal year; monthly summaries ; month-to-date; quarter to date; and, Fiscal Year-to-date (the default option). For all reports, the default is to show all options available to the requestor. (14-17)

Utilization and metrics information for an SRC is current as of the last daily upload from that SRC and is made available through Structured Query Language (SQL) queries issued by ColdFusion to the Oracle IEDB. User contact, project, and allocation information is available from Tool 1 as soon as it is confirmed by the S/AAA and changes are provided to the SRCs daily. (8,10)

The user contact information is searchable by first or last name, username, or by Kerberos login. An example of the user contact information page from the AHPCRC ARAS is shown in Figure 11.

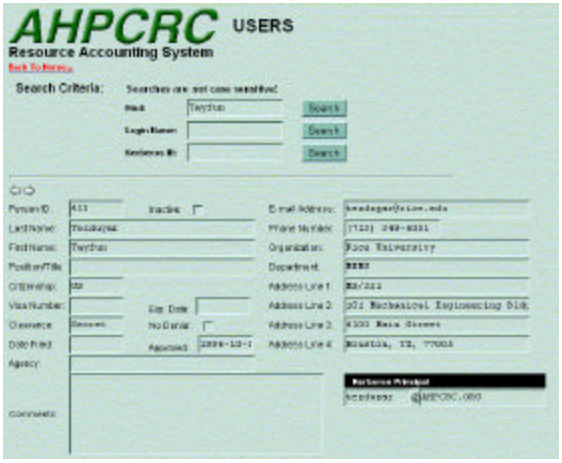


Figure 11. User information is searchable by name, username, or Kerberos login.

A pop-up menu is provided so that a user can select the system or systems on which the user wants queue status, queue structure, or hardware configuration. Options are provided to present the information by SRC, system, or type of system.

### *1.5.2. Tool 2: Queue Process Status*

The IE provides a web-based tool, Tool 2, to view queue information for any single system, all systems of the same type across the IE, or all systems at a specific SRC. Once the option is submitted, the queue information for all of the computers selected is displayed. (18, 19)

The current queue status information will be stored in the IEDBS so that it may be reported with the interactive tools. This data is considered to be temporary and each update will overwrite the previous data from that HPC system. The NetworkCS provided SDTS script provides updated queue status information approximately every 10 minutes. If an update fails, the information reported is from the last successful update.

Queue structure and hardware

configuration is considered to be resource data and therefore is stored in the database. SRCs provide information on changes to queue structure and hardware configuration by sending XML update files to the IEDBS. NetworkCS already provides queue status information for the AHPCRC through Teraweb. Figure 12 shows, for example, the current queue status for all five AHPCRC systems. This capability will be expanded in the HPCMP IE to include views by system type and views by SRC.

Figure 12. Summary or detailed queue information can be displayed.

The ability to see queue information on some or all HPCMP systems will be available to all authenticated users, but could also be limited by NTK, if required by the HPCMP. (20) The ability to see queue information for all HPC systems in the HPCMP program could help with load leveling use across the HPCMP systems.

### *1.5.3. Tool 3: Allocation Management.*

The Allocation Management Tool, Tool 3, provides a mechanism for S/AAAs to facilitate the exchange of allocations between organizations, and allows S/AAAs to reallocate resources among projects under their authority. (21)

In the IE, S/AAAs will be able to generate reports on the allocations and utilization of users under their authority from Tool 1. A link to the Tool 1 report is included in Tool 3 for convenience. (22) The IE will provide an allocation marketplace page (see Figure 13). Search capabilities will be included in the "marketplace" to allow S/AAAs to search available allocation exchange offers. (23,24) Tool 3 will provide a form (see Figure 14) for an S/AAA to post exchange offers including

number of hours, system, SRC, and organization initiating the offer. (23) S/AAAs are able to specify which other S/AAAs are to be notified via email when a new available allocation is posted. The email is sent automatically to the selected S/AAAs when the offer is posted. (25)

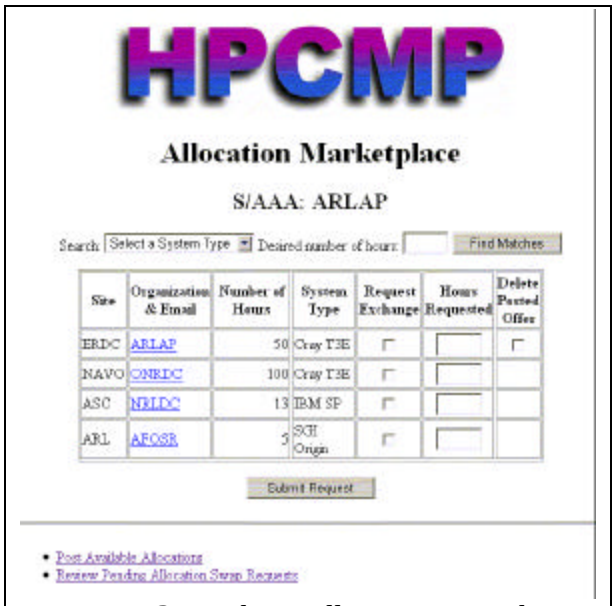



Figure 13. The allocation exchange marketplace allows S/AAAs to view and respond to any of the allocations available to be exchanged.

This offer then appears on the marketplace page. The S/AAAs have a delete button on their customized "marketplace" page that allows them to delete their posted offers, but not offers posted by other S/AAAs. Each

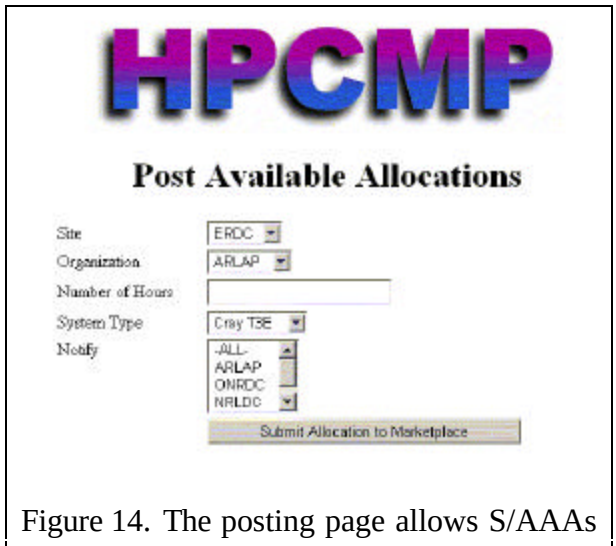



Figure 14. The posting page allows S/AAAs to send any of the other S/AAAs email notification of an exchange offer.

organization name listed on this page is a link to the S/AAA email address list for that organization. The IE also provides a web-form to allow S/AAAs to respond to exchange offers. When a response is submitted, the originating S/AAA is notified by email, and a response form is available from the marketplace page to view the offered exchange request. Acceptance and declination buttons are included for the originating S/AAA to confirm or decline the response. (21) The IE does not allow finalization of the trade until it is confirmed that there are sufficient allocations in the reserve accounts of both S/AAAs. (26, 29)

The S/AAA must place currently allocated hours into a reserve account before they can be exchanged. Each organization's S/AAA is given a unique reserve project in which to store allocations that have been assigned to the organization but have not been allocated to a particular project. This "project" is not able to accumulate utilization, but acts as reserve storage for allocations that are assigned to projects at a later date, or be traded to other organizations. (26)

At the beginning of the fiscal year allocation process, all allocations for the S/AAA's organization are put into the reserve project. S/AAAs are able to move those allocations into their projects as appropriate.

The IE will provide S/AAAs the ability to increment project allocations from their reserve projects to the user projects under their authority. This increment is allowed up to the amount of resources in the reserve project. They also have the ability to decrement allocations from existing projects at any time, up to the limit of the unused portion of the original allocation. This decremented allocation is automatically placed in the S/AAA's reserve project. However, only allocations in the reserve account are available for reallocation to other projects or for trade with other S/AAAs. When allocation time is moved in or out of any project, this information is sent to the SRCs where the allocated resources are located. (27, 29,30)

The S/AAA marketplace page will be made available to all IE users if requested by HPCMP management to facilitate allocation exchanges between S/AAAs and PIs. However, the action buttons on the page will only be available to S/AAAs. (28)

The IEDBS maintains a log of all allocation exchanges. A log of all requests and resource reallocations is also maintained. This can be queried by authorized users through the IE interface including generating exchange reports by

the criteria in SOW Requirement 34. (32, 34)

S/AAAs, HPCMO staff, and SRC management personnel are authorized to review the allocation histories. In general, HPC users do not have NTK access to allocation exchange logs. (33)

Changes resulting from allocation exchanges are reported back to the affected SRC via the IEDBS daily downloads and will be communicated to the SRC within 24 hours of S/AAA approval. (26, 31)

### *1.5.4. Tool 4: Account Fill-in.*

Using the IE web interface, an HPCMP user is able to generate the paperwork required to open an HPCMP account, including Sections I and II of the account application form. The Section III password receipt form is available from the IE, but since it requires a signature, it must be printed and faxed to the appropriate SRC.

The HPCMP account application form is available in two places in the IE. A blank account application form is available from the login web page of the IE and does not require Kerberos or SecurID for access, as new users typically do not have SecurID or Kerberos access yet. This form has a pull down menu for selecting the appropriate sponsoring organization for the application. It has a "send" button that emails the application to the sponsoring organization's S/AAA and stores the application information in the IE holding table. Once the S/AAA has approved the new application, a button within the Account Application Management Tool, "Tool 5" forwards all of the information to the appropriate SRC, assimilates the user and project information into the IEDBS, and logs the transaction. (35, 37)

The second instance of the application form is within the security perimeter of the IE. Current user and project information is displayed and S/AAAs and current users have access to their completed Section I and Section II forms for renewal or update of the information.

Each co-investigator on a project must fill out Section II of the application form. It provides user contact information, preferred logins, and Kerberos realm information. An example of a Section II fill-in form from the AHPCRC ARAS is shown Figure 15.

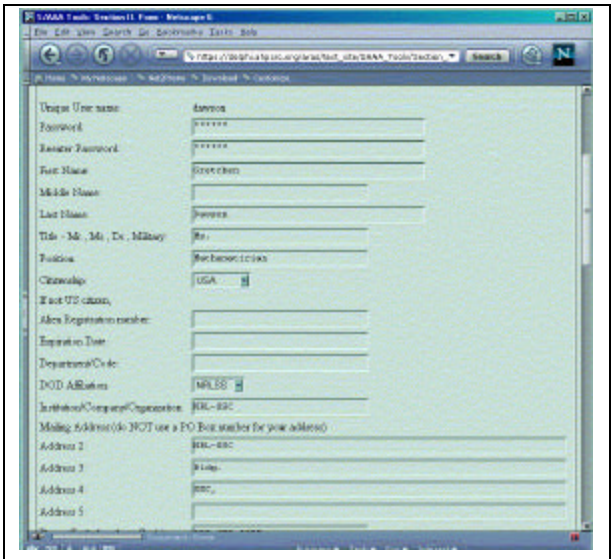


Figure 15. The Section II ARAS form features pull-down menus to assist the user.

An example Section I of the account application form for the HPCMP IE is shown in Figure 16. It includes a matrix of system availability that eases the allocation request process for users and the allocation approval process for S/AAAs. (35, 36)

The IE provides a pull down menu for selecting the appropriate sponsoring organization, and a send button that stores the user/project application information in the IE holding table, pending S/AAA approval with Tool 5. Tool 5 sends an email to the S/AAAs for the sponsoring organization informing them of the receipt.

All user application changes are logged and stored in a holding table pending S/AAA approval of the new applications, renewals, or information update requests. S/AAAs, HPCMO staff, and SRC management personnel are authorized to review the user fill-in log information. In general, regular HPC users do not have access to fill-in logs. (37, 38)

The proposed IE includes, “Tool 5”, an Account Application Management Tool for S/AAAs. It determines what allocation and project requests have been received from Tool 4 and sends email notification to

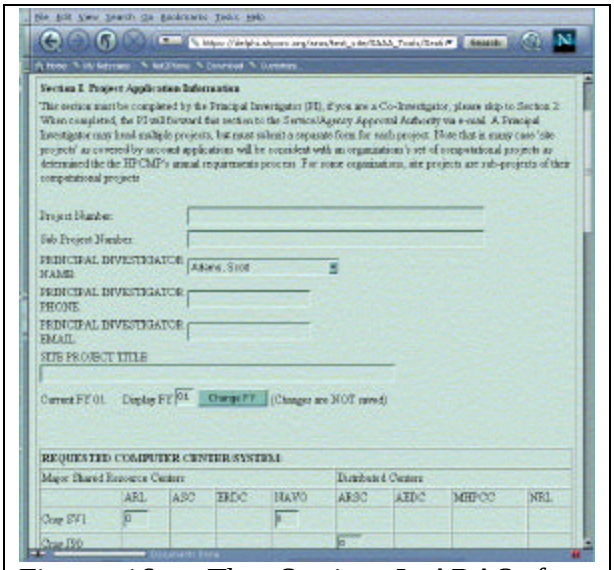


Figure 16. The Section I ARAS form provides a list of all HPCMP system to assist the applicant.

### *1.5.5. Tool 5: Account Application Management.*

the appropriate S/AAA of the receipt. (40)

The Tool provides a mechanism for an S/AAA to verify account/project applications, updates and renewals. Updated information is highlighted for ease of use and S/AAAs have full edit privileges on Application Form Sections I and II forms under their authority. S/AAAs also have the ability to add or modify the "S/AAA only" information at the bottom of each Section I and II. (39, 42)

The proposed IE will contain a Section I form that is a variant on the ARAS Section I form (Figure 17) to include a matrix of HPCMP systems and the SRCs at which they are available to conform with the prototype tool developed by NRL.

Allocation management forms in Tool 5 facilitate the allocation of resources, especially at the time of annual allocation renewal. These forms are based on functionality developed at the Naval Research Laboratory. When users submit their new or renewal allocation requests, they are stored in the IEDB holding tables. S/AAAs are able to view summaries of the allocation requests for all of the PIs under their authority sorted by PI, by system type, or by SRC. PI requests are shown in the forms, and S/AAAs are able to edit and adjust allocation amounts directly from the forms. Totals are shown in each form.

When the allocation process is complete, the S/AAA can click the “allocate” button and an application form is sent to each SRC

where the project has an allocation and the data is assimilated into the main tables of the IEDBS. The IE notes whether the application is a new or renewal request. If the request is new to the SRC, or if it includes new co-investigators, the IE sends a completed Section I along with a Section II for each co-investigator authorized for that SRC by email to the SRC. If the request is a renewal, the changes to user, project, and allocation are sent to the SRC via the daily download. (41)

Allocations can be made for future dates and will not be in effect until that future date is reached. This allows allocation for the new fiscal year before the October 1 effective date, for example. (39)

An example of the application management form in the AHPCRC ARAS is shown in Figure 18. It provides the S/AAA the ability to authorize account setup.

Account management actions are logged and stored in the IEDBS. (43) S/AAAs, HPCMO staff, and SRC management personnel are authorized to review the histories. In general, regular HPC users do not have access to account management logs. (44)

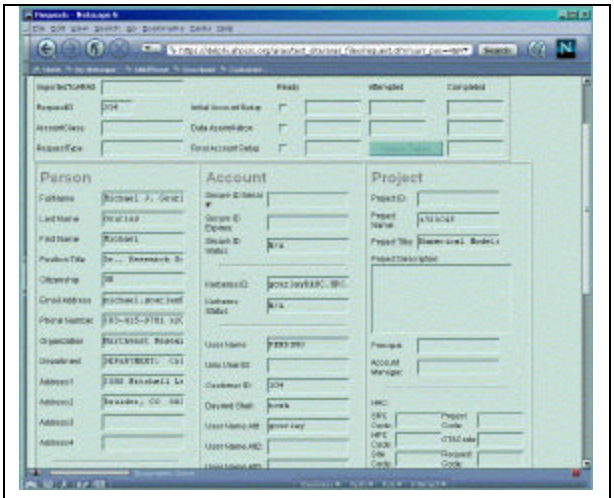


Figure 17. The ARAS application management form is used to set up projects and accounts.

### 1.6. Ease of Use

NetworkCS's proposal for the IE includes the following ease of use features: use of standard browsers and web-based interfaces, easy-to-use fill-ins for identification and authentication, customized menus, pop-up menus, online documentation, and email help contact. Each of these items is detailed below.

### *1.6.1. Standard Browsers and Web-Based Interfaces*

The NetworkCS proposed IE allows users to access IE data using a standard web browser. The NetworkCS design for the IAS and IE does not require any special or customized software or hardware on the user's desktop client. Hence, as far as the user is concerned, no installation of new software is required.

### *1.6.2. Fill-ins*

Web page forms are provided in the IE to guide users in entering data. The forms are clearly arranged to facilitate data entry and reduce errors. The NetworkCS proposed IE provides users with a form for entering identification and authentication information prompting users for Kerberos username and password, SecurID passcode, and HPCMP Kerberos Realm. The Kerberos Realm is selected from a pop-up menu.

### *1.6.3. Customized Menus*

Menus and options will be displayed according to the user's NTK. Once authenticated, the user sees only those menus and reports that are consistent with that user's authority (user, PI, or S/AAA) and NTK. This feature is thoroughly explained in Section 1.5, IUS.

### *1.6.4. Pop-up Menus.*

Pop-up menus will be implemented wherever possible to provide users easy access to lists of data such as user site codes, HPC systems, realms, and SRCs. This takes the "guessing" out of providing information and reduces errors.

### *1.6.5. On-line Documentation*

.

The proposed IE will provide online documentation on how to access and effectively use the Tools within the IE environment itself. Each page of the web interface will contain a link to a "Help" page. The "Help" page will contain a bulleted list of descriptions corresponding to each of the options available on that page.

(51)

### *1.6.6. Email Help Contact Forms*

A link included on each page allows the user to send data describing a problem or question to the IE administrators. When selected, the link will display a CGI-based web page form that the user will fill out describing the nature of the problem or question. The CGI program will also automatically collect and send hardware (system type), software (browser being used), and the URL of the page from which the user just came. This problem data will be stored in the IEDBS for the purpose of problem tracking and resolution. This page also provides a link to the IE administrator's email address so that a user also has the option of sending a free-format question if they desire. (51, 56)

## 2.0 TECHNICAL IMPLEMENTATION APPROACH

NetworkCS's proposed architecture for the HPCMP's IE uses, to the maximum extent possible, commercial-of-the-shelf products (COTS) that have been thoroughly tested and proven in demanding high transaction rate web and database applications. COTS products proposed to be included in the IE include Oracle, ColdFusion, Apache, and RedHat Linux. It also uses the IAS based on the security module in NetworkCS's Teraweb.

The ability of each of these products to handle the technical requirements for scalability, extensibility, portability, and reliability and maintainability of the HPCMP IE is addressed below.

### 2.1. Scalability and extensibility

The NetworkCS proposal for the IE is a fundamentally scalable and extensible design. (1) Scalability includes several factors:

- Ability of the software to handle significantly larger data sets.
- Ability of the infrastructure to handle more data flow.
- Scalability of the data architecture.
- Ease with which the IE can accommodate additional users, HPC

systems at existing SRCs and new SRCs, and/or remove existing users, HPC systems, and existing SRCs.

- Flexibility of the data architecture to extend to future capabilities.

These items are discussed below.

The software solutions chosen by NetworkCS for the IE are scalable to sizes much larger than the proposed IE. Oracle is used in the transaction processing industry with data sizes that are orders of magnitude larger than the HPCMP IE. Consequently, we are confident that Oracle can handle the current HPCMP user community and even one that is many times that size.

ColdFusion is a web application server that provides an excellent environment for database application development. It is also widely used to support transaction processing for large commercial information systems.

The Teraweb security module is unaffected by the number of users, or the size of the data being processed.

The infrastructure chosen for the IE server is a Linux server running Red Hat 7.0 Linux server software. Linux is increasingly the operating system of choice for e-commerce and database applications and supports configurations that are substantially larger than the IE requirements.

The standard LAN connection of at least 100 Mbits/second for the server with not less than 5 Mbits/second bandwidth to the DREN should provide sufficient server and network performance to handle the expected IE load at reasonable cost to the Government.

The proposed data architecture is designed to be extensible. Systems and SRCs are not hard-coded into the architecture, but are merely table entries that can be easily added or deleted. Utilization or metrics data entries have resource tags associated with them, and as such, can be associated with any resource. This design allows easy addition of new sites or systems, easy deletion of old sites and systems, and

easy accounting of new resources within new or existing systems. (60,61)

The IEDBS will be initially populated by SRCs sending user, project, utilization, allocation, SRC and resource information to the IEDBS in XML format. When new SRCs or new systems at existing SRCs are to be added to the IE, the SRC will email the data in XML format to the IE administrators for import into the IEDB.(3, 59)

The design of the proposed IEDB is an extension of the NetworkCS design for the ARAS database that accommodates daily uploads of utilization data and daily downloads of allocation balances from all 5 AHPCRC systems. These HPC systems are geographically remote and represent different vendors. Additionally, the AHPCRC database has capabilities for assimilating new and renewal users and projects from web-based forms or parsing text application forms. This process is also used for tracking users of the HPCMP corporate Kerberos realm. This basic design has shown itself to be both extensible and scalable, hence, providing confidence that the scalability and extensibility of NetworkCS's proposed design for the HPCMP IE will meet the Government's requirements.

### 2.2. Portability

The IE design proposed by NetworkCS is portable throughout. The IUS requires that no additional client software be installed on a user's workstation beyond standard configurations to access IE.

The software used in the IE, including Apache, Oracle, and ColdFusion are commercial or open source software products that run on many different versions of UNIX and proprietary server systems. Hence, the IE is not limited to a specific vendor's hardware.

The data architecture is designed using standard DBMS practices and standard SQL queries. If the HPCMP decides in the future to move the IE to a different DBMS system,

the tables and queries associated with the IEDBS should port readily.

XML provides a simple and elegant solution to data transfer. XML is an industry standard for data transfer and exchange. The use of XML provides support for data portability between the various HPC accounting data formats. As long as the data conforms to the XML DTD, it can be uploaded and downloaded from the IEDBS reliably, regardless of the hardware hosting the IEDBS. XML is an industry standard for data transfer and exchange. Use of XML provides for data portability. XML can be used with database programs such as Oracle and Microsoft Access to provide interoperability between those systems and the IE. (49,50) (4)

### 2.3. Reliability and Maintainability

To enhance maintainability, the IEDBS will adhere to good relational database practices in database architecture and relationships. This will enable the DBMS to enforce data integrity, thereby reducing time-wasting data problems.

Development of the IE adheres to good HTML, ColdFusion, and SQL coding practices. The code and SQL will be readable and documented. Standards are enforced throughout the coding process to maximize code reusability and minimize complexity.

The IE is to be well documented. In addition to the help pages within the web application and the comments within the code, design documents will be written for every major interface and procedure. (54)

## 3.0 SECURITY DESIGN AND IMPLEMENTATION

Figure 1 provides a detail view of the architecture of the IE. It shows the SDTS located on a computer at an SRC, the IE server, and a user client and the network interconnects. The security design for each of these major components and their sub-systems are described below.

### 3.1. System and Sub-system Security Implementation.

All of the components at the IE site run on a single IE server computer. Thus, the authentication module, web server, ColdFusion server, database, and IDTS all communicate through either shared address space, pipes, or local sockets. This provides for a simple, integrated architecture, which facilitates the security design review process and typically results in a more secure system.

Data transfers between the SDTCs and the IDTS are encrypted with SSH. The transfers are authenticated using RSA authentication, which is built into SSH.

Only authorized SRC SDTCs will be able to connect to the IDTS. Full shell access will not be permitted; only the commands necessary to transfer data will be available. This scheme will not allow normal users non-Kerberized access to HPCMP systems. Users have interactive access to the IE through a web browser. Interactive access includes viewing or modifying existing IE data, adding new data, and generating reports. The web server that supports these activities is Apache. Apache is a high-quality, open-source product that has become the most commonly used web server. Security updates for Apache are released on a regular basis. Connections between the browser and the web server are encrypted using 128-bit Secure Socket Layer encryption in accordance with HPCMP requirements. Access is authenticated by the IAS. The authentication module uses the same design as the Kerberos authentication module used in Teraweb. (45,62,63,65) Teraweb security was reviewed by an HPCMP security team led by R. Johnson, the HPC Information System Security Manager, and included K. Renard, H. Kash, and D. Butler. The HPCMP authorized the use of Teraweb on HPCMP shared resources and stated that it "meets or exceeds the HPCMO

requirements for authentication and data protection" (memo from Cray Henry dated 13 December 1999). (62)

The authentication mechanism in the IE is sufficiently flexible that a PKI authentication solution could be used instead of Kerberos tickets if the HPCMP moves to PKI as the standard authentication mechanism for its HPCMP systems (64).

The IE database engine, Oracle, is in use in many environments that require data security and integrity, such as financial institutions and government agencies. Oracle is known to have excellent, vendor supported security features.

Interactive access to information in the IE database is through ColdFusion. Security updates for ColdFusion are released on a regular basis.

Access to data in the database is controlled by the IUS using the PersonID supplied to it by the IE authentication module, which is described below. Using this PersonID and information stored in the database, the IUS creates a database table that contains a personal access tree. This personal access tree is used for the remainder of the user's session and provides the basis for enforcing NTK policy.

### 3.2. Need to Know Policy.

As previously mentioned, IE users log in to the IUS with a SecurID and Kerberos. Once authenticated, a user's Kerberos login is translated into a PersonID in the IEDBS. Each person will have one person record and therefore one PersonID in the database, even though they may have multiple usernames on multiple systems. Translating the Kerberos login to the PersonID enables the IEDBS to provide information to the person based on the person's "authority".

Figure 18 schematically shows the authority tree in the proposed IE. The parentheses indicate the authority at each level of the tree.

The levels of the authority tree correlate to the levels of a person's personal tree. For example, if a person is an S/AAA, that

person will have access to every node under the organization that that belongs to this person as an S/AAA.

IE users will be able to see the existence of parents and siblings in the tree, but not data details. They will have the authority to see data details and report details about their nodes and all descendents of their nodes of the tree. They will also have edit capability from Tool 4 for user, project, and allocation information for their nodes, or any descendent nodes including the ability to issue an account deletion request. Any Tool 4 changes must be verified and authorized by the S/AAA or above (using Tool 5) for the change to take effect.

Root (IE Administrators)

- DoD (HPCMO management)
  - Service (Service management)
    - Organization (S/AAA)
      - Project (PI)
        - Co-investigators (User)

**Figure 18. Authority Tree**

All users authenticated by the IE will have access to queue information for any HPC system in the IE.

Based on a person's highest authority, IUS menus will be customized to ensure that the person will be allowed access only to the tools, and therefore data, for which the person is authorized access. In addition, the IUS generates a tree of "resource group" nodes that the person has access to. Resource groups are entities such as ROOT (Level Zero), DoD (Level One), Army (the military services and DoD Challenge projects are Level Two), Organization (Level Three), Projects (Level Four), and Users within projects (Level Five). On the tree (see Figure 19), a person is allowed read access to their ancestors and self, write access to their descendants, and look up access to their siblings. This tree is used throughout the IUS to ensure that NTK access is enforced.

As an illustration, an example from ARAS, for the “person” named “Stein” is

shown. Stein is "PersonID" 401. Associated with PersonID 401 are two different usernames, seven projects, and two different "authorities" (PI and user on multiple projects).

The tree shown is a graphic representation of the nodes (and therefore, data) that Keith Stein has access to. (The AHPCRC node and the 1140000 node have been closed in this image in order to conserve space.) The underlined nodes are the nodes that "Stein" has either read or write access to. The nodes that are not underlined are siblings; "Stein" can merely see that they exist.

A "Person's" "personal tree" is destroyed when he logs out or after 10 hours have passed. It is recreated (implicitly) when it is needed by the IUS for the "Person" or whenever it already exists and an administrator modifies the master resource group tree. Only the "Person" and authorized administrators have access to a "Person's" tree.(45)

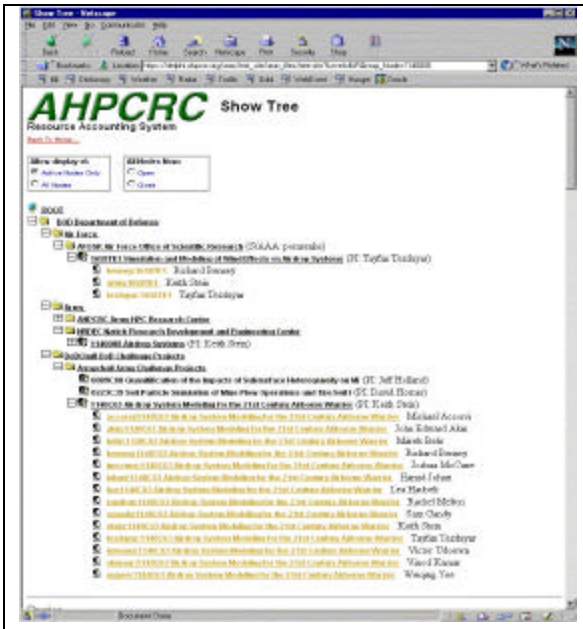



Figure 19. The personal tree for "Stein" shows the information nodes that Stein has access to.

## C. MANAGEMENT PLAN

### 4.0 IMPLEMENTATION PLAN

Four critical factors for the successful development and implementation of the IE are (1) understanding the customer's requirements, (2) thorough knowledge of the underlying technologies and experience, (3) correct personnel mix, and (4) the corporate management commitment of resources to get the job done. Sections 1.0 through 3.0 of this proposal clearly demonstrates excellence in each of these measures. Additional information is provided in this

section of the proposal to demonstrate the Contractor's unique capabilities to implement, on schedule and in conformance with the SOW, the HPCMP IE. These factors are addressed below.

### 4.1. Customer Requirements

NetworkCS, having been the infrastructure contractor for the AHPCRC and having served AHPCRC DoD customers on HPC systems since 1989, knows the HPCMP's requirements for allocation and utilization reporting, and account setup and management. NetworkCS has provided allocation based utilization controls on the HPCMP's AHPCRC systems since 1990 and has provided allocation and utilization reporting using relational database technology since 1995. Because of this prior experience and through planned meetings during the early phase of the IE contract, NetworkCS will be able to deliver the DTDs within the schedule required to achieve the implementation schedule.

Furthermore, NetworkCS has demonstrably strong skills and expertise in technical security implementation. As previously mentioned, NetworkCS deployed a web based tool, Teraweb, for accessing HPC systems at the AHPCRC in 1998. It was evaluated by a HPCMP security team to meet or exceed the HPCMP requirements for data security and authentication and was running in production at the AHPCRC SRC ever since. Again, this reduces risk to the Government, demonstrates that NetworkCS understands the customer's security requirement and insures that the aggressive implementation requirements of the solicitation can be met. This particular point can not be over emphasized. DoD is very concerned about the security of its system and NetworkCS has already demonstrated that it understands those requirements and can satisfy them. Security is a critical design element and NetworkCS has shown that it can deliver the products to satisfy those requirements.

### 4.2. Technical Knowledge and Experience.

NetworkCS is able to leverage the existing capabilities, skills, and experience gained through its work on AHPCRC's ARAS in its implementation of the HPCMP IE. NetworkCS recognizes that the IE is larger and more complicated than ARAS, but critical design issues have already been evaluated and addressed.

The NetworkCS developed ARAS includes the following features:

- Strong security authentication.
- A database (using Oracle) with daily uploads of utilization data from and daily downloads of allocation balances back to multiple remote AHPCRC HPC systems.
- An automated system for incorporating new and renewal user information into the database, both from a web-based application form and also from automated parsing of email application forms. This is also used to support the HPCMP Corporate Kerberos Realm.
- A mechanism for viewing the queue status of all AHPCRC systems from Teraweb.

This strong technology base will be leveraged for the development of the HPCMP IE.

### 4.3. Personnel Skill Mix.

NetworkCS is proposing to assign three senior staff members with over twenty years of experience with the AHPCRC SRC to the HPCMP IE project. On the average, their tenure with the AHPCRC equals the chronological age of the HPCMP. These three persons know and understand HPCMP operational and security procedures. In addition, they all have had extensive experience in software development. One has had applications development experience, two have operating systems experience, and one has database and compiler development experience. These three persons all have Secret clearances.

This team is augmented by additional NetworkCS personnel and consultants in database design from Greenbrier and Russel, Inc., (G&R) a database consulting firm with an annual revenue of over $100 million.

### 4.4. Corporate Commitment

NetworkCS is proposing a multi-phased approach to the implementation and deployment of the IE. This approach takes advantage of NetworkCS's long experience in HPC and its in-house resources to mitigate risk to the Government during the initial development and prototyping of the IE, a cautious and rationale plan for alpha and beta testing, and an aggressive plan for deployment of the full IE. Proposed activities under each of these phases is described below and in the Deployment Section (Section 5).

NetworkCS will, in conformance with the requirements of the SOW, use contractor owned facilities for the development and prototyping of the IE. This approach, coupled with the availability of in-house HPC systems, allows NetworkCS to maintain a separate development and prototype facility throughout the development process. NetworkCS believes that it is the only Contractor able to propose this capability.

### 4.5. Project Management/Implementation Management

NetworkCS's principal subcontractor, G&R, is a privately held software development and consulting company with over $100 million in annual revenue. G&R has developed a methodology (the "Guide") that focuses on providing a consistent and structured approach for the definition, development and implementation of business and technology solutions.

NetworkCS and G&R will use this Guide to insure that there is a clearly defined scope for the project, established project milestones and deliverables, an appropriate project organizational structure, appropriate project and quality control procedures, and an adequate risk analysis assessment.

This guide will be used throughout the project life cycle for assigning roles and responsibilities, establishing protocols for communication, issue and risk management, and change control. A project plan with detailed milestones for each Tool, including start and completion dates for each task, will be established. Scheduled reviews will be held with the HPCMP at the Contractor facility on the critical design issues such as DTDs and security design.

The software developed for the IE will be managed using RCS for revision control. Monthly status reports will be sent to HPCMP management as required in the SOW. They will include implementation status, and validation and testing status. NetworkCS and G&R, using the Guide, will provide the HPCMP with a Project Debriefing that will assess the various success factors in the project including staffing, project planning and management, communication, environment and documentation.

### 4.6. Implementation Schedule

An implementation schedule organized by task category showing days to completion from contract start date for each task is provided in Table 1.

**Table 1**

**Implementation Schedule**

| Task | Completion (elapsed days) |
|---|---|
| User authentication developed | 10 |
| Initial design of user interface | 10 |
| Test server setup | 14 |
| Complete initial design of IEDBS | 30 |
| Security design completed | 30 |
| Security design review | 30 |
| Technical design review | 30 |
| Tool 1: user info report developed | 30 |
| Tool 4: Section I form developed | 35 |
| Tool 4: Section II form developed | 50 |
| SDTS development | 75 |
| Write XML specs | 75 |
| Prototype Review | 90 |
| Tool 1: Forms and Reports | 90 |
| Tool 4: other forms developed | 90 |
| XML DoD review | 90 |
| JAVA Oracle upload interface | 100 |
| XML roll-out | 105 |
| Tool 2: queue status application | 110 |
| Tool 5: Section I form developed | 115 |
| Tool 5: Section II form developed | 120 |
| JAVA server written | 125 |
| Tool 3: allocation assignment | 130 |
| Upload libraries written | 130 |
| Tool 5: other forms developed | 140 |
| Tool 3: forms and reports | 150 |
| Tool 3: allocation trading interface | 150 |
| Beta Review | 180 |
| On-line problem tracking | 180 |
| Full Release Review | 300 |
| On-line help written | 300 |

## 4.7. Schedule Risk Analysis

The major implementation risk factors relate to the timely and complete specification of DTDs, the timely and successful completion of security reviews, availability of cleared personnel, continued availability of third party software, travel requirements, and award date. Each of these items are discussed below.

### *4.7.1. DTDs*

In order to meet the requirement to deploy a beta version of the IE at five sites within 180 days, it is necessary to start deployment no later than day 150. This, in turn, requires that DTDs be reviewed by the HPCMP, and approved by day 90. This is truly, an aggressive schedule.

The implementation schedule for the IE is aggressive. NetworkCS proposes to hold design meetings with HPCMP designated personnel with in the first 30 days after contract award to review the security design and the DTDs and secure HPCMP approval by day 90 for these critical elements. NetworkCS believes, based on its experience with the HPCMP, that this aggressive schedule can be met.

### *4.7.2. Security Reviews*

Appropriate security controls are a fundamental requirement and a fundamental design parameter of the IE. Security must be built in, not added on. In order to insure that the delivery schedule is met, the security design must be reviewed and accepted by the HPCMP within 45 days of the initiation of the contract. Again, based on NetworkCS's prior experience in implementing secure web based technology, the risk is minimal.

### *4.7.3. Third Party Software*

Apache, ColdFusion, Oracle, SSH, and SSL are third party applications. Successful completion of the project is dependent on the continued availability of this software. These products are, however, widely used and the probability of non-availability of

these products or suitable alternatives is considered minimal.

#### *4.7.4. Travel*

The development of the IE, will in accordance with the SOW, be performed at the Contractor site. Consequently, NetworkCS is proposing that all project reviews be performed at the Contractor site to minimize disruption of development activities.

#### *4.7.5. Award Date*

This implementation schedule risk is mitigated in the NetworkCS proposal by the extensive experience that NetworkCS has in the IE area. NetworkCS has extensive familiarity with the HPCMP user community and management requirements and experience in development of web technology, security systems and HPC accounting systems. This experience gives NetworkCS a clear understanding of the requirements and the knowledge and ability to develop a secure, web-based IE system.

### 4.8. Implementation Testing Plan

NetworkCS will employ a three phase testing plan during the implementation of the IE. The three phases are: (1) Sub-system Level testing on the Contractor's development/prototyping system; (2) System testing in the Contractor's non-Government HPC environment; and, (3) subject to Government approval, testing at the AHPCRC SRC as the first beta test site. Key points of each of these phases are discussed below.

#### *4.8.1. Sub-system Level Testing*

NetworkCS will conduct thorough reviews of the design documents IE subsystems during the development phase. For example, the Oracle IEDBS will undergo a design review with the Oracle consulting firm, G&R. It will be tested for its ability to accommodate the requirements in the SOW, for good database practices, and for the validity of the data being reported. (53)

NetworkCS technical security personnel will conduct a thorough review of the IE implementation to insure the integrity of the user authentication, verification, and data privacy and mechanisms at each stage of its development. NetworkCS will request a further review by the HPCMP and, if the HPCMP so desires, by the National Security Agency or other appropriate security agencies. Obviously, as stated elsewhere in this proposal, some of the key security elements of the proposed architecture have already been subject to exhaustive security review by the HPCMP.

Tests will be performed to verify the validity of the XML data transfers, the reliability of the transfer mechanism, and the operation of the interface to the IEDBS.

### *4.8.2. System Level Testing*

Once sub-system level testing is completed, NetworkCS will conduct alpha release system level tests (without SecurID) of the IE using the Contractor's development/prototyping system in conjunction with the Contractor's non-Government HPC facilities. Those resources includes, at present, a CRAY T3E-900, a CRAY C916/12512, SGI Origin 2000, Sun Microsystems, and cluster systems based on INTEL's Pentium architecture.. The ability of this Contractor to conduct alpha testing of the IE on its own systems in its own facilities substantially reduces risk to the Government. Again, we believe that no other Contractor is in a position to approach the IE development in this way. (52)

## 5.0 DEPLOYMENT PLAN

After the IE is fully tested in Network's commercial environment, NetworkCS proposes to implement the first beta release of the system on Government furnished equipment (GFE) and software in the AHPCRC SRC for additional testing prior to further distribution to an additional five SRCs as required in the SOW. The overall schedule for IE deployment is shown in Table 2.

### 5.1. Beta Test Phase

The Contractor proposes that the first HPCMP deployment during the beta test phase of the IE, in accordance with the SOW, be at the AHPCRC SRC using GFE and software. Contractor believes that the beta test phase, in accordance with the SOW, can only be accomplished on GFE and Government furnished networks operating in compliance with HPCMP security policy.

**Table 2.**
**Deployment Schedule**

| Tasks | Completion |
|---|---|
| Prototype- | |
| 3 tools partial functionality | 45 |
| 2 tools full and 2 tools partial functionality | 90 |
| Distribution of XML DTD | 105 |
| Beta Deployment | |
| Availability of GFE | 120 |
| At AHPCRC | 130 |
| SRC 1 | 154 |
| SRC 2 | 161 |
| SRC 3 | 168 |
| SRC 4 and SRC 5 | 175 |
| Full release | |
| To five Beta SRCs | 300 |
| Install/Integration. SRC 1 | 330 |
| Install/Integration. SRC 2 | 337 |
| Install/Integration. SRC 3 | 345 |
| Install/Integration. SRC 4 | 352 |
| Install/Integration. SRC 5 | 359 |
| Complete Installation/Integration | 365 |

Since the design for the IE uses a central server to support the HPCMP, it is clear that the central server must be installed and operational and meet HPCMP security requirements prior to beta testing with any SRC. Consequently, NetworkCS is proposing to use existing AHPCRC GFE to host the operational beta installation of the IE. The Government will need to provide, however, the appropriate Oracle DBMS and ColdFusion software licenses.

The proximity of the AHPCRC facilities to the IE developers makes this a cost effective choice for the first deployment site. It essentially allows for the side-by-side operation of the Contractor's development system and the IE. This enables developers to analyze and test out bug fixes on the Contractor's development system and then quickly install them on the operational IE server supporting the beta SRC sites. Although the development system and the operational IE server are located in the same facility, they are not on the same network

and are isolated from each other by firewalls and strong identification and authentication requirements.

After deployment at the AHPCRC, a beta release of the IE will be deployed at five additional SRCs to be determined in consultation with the HPCMP.

**5.2. Full Release.**

The full release of the IE will be completed no later than 300 days after contract award at the same six beta sites (AHPCRC and five others).

**5.3. Final Release**

The final release of the IE to at least five additional SRCs will be accomplished no later that 365 days after contract award. These will also be deployed at a rate of one per week to make ensure that issues related to additional deployments can be resolved.

**5.4. Installation and Integration.**

Complete implementation and maintenance documentation and user manuals will be made available to the Government 300 days from contact award. (54)

Installation and integration of the complete IE will be accomplished prior to day 365. NetworkCS is proposing that the installation and integration from beta deployment through final deployment be performed at the AHPCRC SRC on AHPCRC GFE (Oracle license to be provided by HPCMP). NetworkCS will, at the request of the HPCMO, re-install and test out the system for final delivery on GFE and software at an alternative site. The Government is requested to provide invitational travel orders to cover the travel costs associated with installation at an alternative site.

An "Acceptance Period" report will be delivered to the government at the end of the acceptance period. It will include lessons learned, and unforseen dependencies or anomolies observed. (54)

The contractor will provide usage, installation and maintenance training at its

facilities on one to two days per month from month 6 of the contract period through the end of the warranty period. The Contractor understands that from time to time the Government may wish to sponsor training at other locations. Contractor will support off-site training as part of the above commitment with the Government providing invitational travel orders. (55)

For a period of 6 months after final installation and integration NetworkCS will provide for resolution of critical problems that render the IE inoperable within 24 hours and non-critical problems/bugs within 72 hours. The Government or SRC hosting the IE server is responsible for support of GFE on a 24x7 basis. (57,58)

### 5.5. Deployment Testing

As previously mentioned, testing of the alpha release of the IE will be performed on NetworkCS's commercial HPC systems. Beta testing of the IE server and its subsystems (IEDBS, IUS, IAS, IDTS, and SDTS) will then be accomplished in the AHPCRC SRC before deployment to any other SRC. This testing will include data transfer upload and download operation and data integrity, security of the data transfer mechanisms, security of the user interface, access control to the data within the database, and functionality tests on the tool interfaces. This should reduce the testing needed in the later phases of deployment.

In the beta test phase, the IE will be tested with each SRC for data integrity, and for upload and download reliability and security. Beta SRCs will be encouraged to use the user feedback form provided in the user interface, and to work with the NetworkCS deployment coordinator on any issues arising from deployment at the SRC.

This process will be repeated with the full release and again with the deployment at the additional 5 SRC. (52)

### 5.6. Deployment Schedule Risk Analysis

The major deployment risk factors relate to the availability of cleared personnel,

firewall issues, availability of Government data, availability of GFE, location of IE server, and travel. Each of these items are discussed below.

### *5.6.1. Cleared Personnel*

Key NetworkCS staff proposed to work on this project are cleared at the Secret level. Other personnel assigned to the project either already have or will have submitted paperwork for a Position of Trust (NAC), at a minimum, thus mitigating this area of risk.

### *5.6.2. Firewall Issues*

It is recognized within the HPCMP that issues with Firewalls have, at times, restricted access to SRC systems. The Contractor believes that it is the responsibility of the Government to insure that Firewall configuration issues at SRCs do not effect communications between the IE server and the SDTCs. This is a moderate risk factor at a few SRCs.

### *5.6.3. Availability of Data*

The SRCs are responsible for providing usage, utilization, queue information and other data as specified in the SOW. It is necessary for the SRCs to make that information available to the IE on a schedule that is in conformance with the schedule proposed by the Contractor and approved by the HPCMP. This is a low risk issue for most SRCs, but could be a significant issue with a few SRCs.

### *5.6.4. Availability of GFE*

In order to meet the schedule for beta testing and implementation, the appropriate GFE, including software, must be made available to the Contractor. The Contractor is proposing that the IE Server be housed in the AHPCRC SRC. All the necessary GFE, including networking, to support the IE is already available at the AHPCRC SRC, except for the appropriate Oracle and ColdFusion licenses. The HPCMP would need to grant permission for Contractor to deploy the IE for beta test in the AHPCRC SRC within 115 days after the award of the contract. We believe this is a low risk item.

### *5.6.5. Location of IE Server*

Contractor has proposed the use of existing GFE equipment located at the AHPCRC SRC for the IE server. Pricing for the deployment, installation and support of the beta, full, and final releases assumes that the HPCMP concurs in the selection of the AHPCRC SRC to host the IE server. Location of the IE server at a different site will have an impact on price.

### *5.6.6. Travel*

NetworkCS is proposing that the GFE IE server be installed at the AHPCRC SRC, which is collocated in NetworkCS facilities; this further reduces disruption for travel.

### *5.6.7. SRC Accounts*

Since the transfer of data to the IE is the responsibility of the SRCs, NetworkCS personnel will not require accounts on any of the SRC systems (except for NetworkCS personnel in support of the AHPCRC SRC). Hence, delays in opening SRC accounts is not a risk factor.

## 5.7. Control and tracking

Project management will continue through deployment with schedule and resource management of the deployment phase. It will be included in the project plan with detailed milestones for each SRC including start and completion dates for beta and full release deployment.

The weekly project status meetings will continue in order to enable discussion of any deployment issues that arise and allow the deployment coordinator to work with the developers on problem resolution. The meetings will include management oversight.

Periodic reviews will be offered to the HPCMP for consultation on deployment issues and deployment status review.

The software developed for the IE will continue to be managed using RCS for revision control.

Monthly status reports will be sent to HPCMP management through the deployment phase as required in the SOW.

They will include implementation status, validation and testing status, and deployment status.

## 6.0 AHPCRC SRC

The AHPCRC SRC is housed in the facilities of NetworCS in Minneapolis, MN. The facility is a secure robust environment supporting 24 x 7 operation. The network and system performance is sufficient for supporting the HPCMP IE operations. (4)

The facility (see Figure 20) was designed to support HPC systems. It is a 200,000 square foot building with 18,000 square feet of raised computer room floor. The computing facility has limited access with 24 by 7 security guard service. Entry into the building is controlled through the use of a security card system and security guards.

Computer room (see Figure 21) access is limited through the use of the security card system to appropriately cleared authorized operations personnel Security, fire and smoke detection and suppression systems, UPS battery backup (See Figure 22), redundant chillers and a monitoring system insure high system availability and provide for the protect of critical resources. Diesel generator backup is also provided for the major systems such as the IE server.

Figure 20. AHPCRC systems are located in this state-of-the-art building specifically designed to protect and support HPC systems and operations.

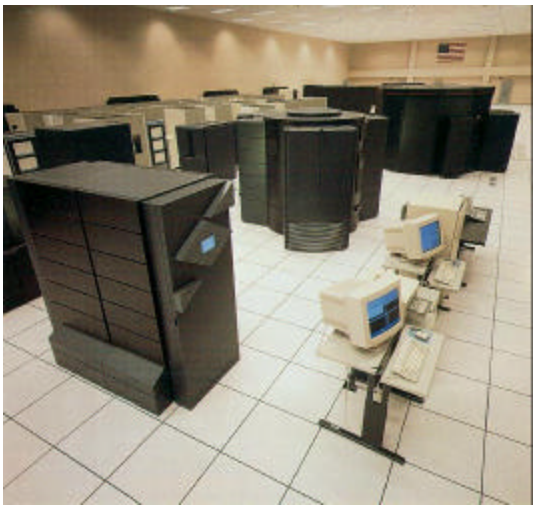


Figure 21. AHPCRC systems are located in this state of the art HPC computer room.

AHPCRC and HPCMP systems are connected to the DREN.

Root access is limited to operations personnel who are responsible for support of the system. These personnel are required to

Figure 22. Systems are on UPS with battery and three diesel generators.

AHPCRC and HPCMP systems are have secret clearances. Controls are in place to provide for data protection. Media disposal procedures are designed to insure the confidentiality of information. Regular backups are performed and offsite storage of vital records is provided. Data in the IE will be backed up for recovery. The HPCMP performs an annual ST&E or SAV of the site. The last SAV reported no "observations" of any kind. (4)

## 7.0 PERSONNEL PLAN

NetworkCS has assembled an experienced team for the IE effort. Barbara Bryan will be the project manager. Barbara is currently the NetworkCS Technical Manager for the AHPCRC and knows with the HPCMP requirements for utilization reporting, account setup, user requirements, and allocations management.

Paul Ewing will lead the security implementation team. Paul is the AHPCRC and NetworkCS computer security expert and is so recognized by the HPCMO.

Todd Rannow is one of the developers of ARAS. He has Oracle development and DBA experience and will oversee and implement the IEDBS and ColdFusion interface to the IEDBS.

For additional database experience, NetworkCS will add David Knutson from G&R to the IE team. David is an Oracle database developer and will be assigned

tasks on database implementation and provide oversight in database best practices, design, and optimization. He has 10 years experience in database development and information systems design.

Wes Barris will lead the team implementing the user interface. Wes is agraphics programmer and web developer and on the AHPCRC team since 1990.

## 7.1. Resumes of Key Program Personnel

### *7.1.1. BARBARA BRYAN, NetworkCS*

**Profile:** Barbara is the Technical Manager for the AHPCRC and manages 20 Center support staff and staff scientists. She has worked in customer support for the AHPCRC for 11 years and for Lawrence Livermore National Laboratory for 7 years. Her AHPCRC duties have included working with the DoD user community, supporting account management, teaching HPC programming, assisting HPC users with code optimization and efficient use of HPC resources, and performing the duties of an S/AAA. Her project management experience includes mnagement of the ARAS development project, management of the deployment of the AHPCRC computing environment including web-based tools, five HPC systems located at five sites, and management of the development of the AHPCRC environment including the deployment of AFS, remote management remote management HPC systems and workstations.

**Technical Skills:**

**Languages**: C, Fortran, HPF, MPI and PVM libraries, HTML; **Systems:** UNICOS, UNICOSmk, AIX, Windows NT, Windows;, IRIX, **DBMS:** ORACLE, MS ACCESS

### *7.1.2. PAUL EWING, NetworkCS*

**Profile:** Paul is the Senior Security Analyst for NetworkCS and the ISSO for the AHPCRC. His duties include security systems and network design, development and implementation. He is responsible for the overall security design for the AHPCRC networks supporting five sites and the

DREN connection including the installation and configuring of Firewall-1 software and Solaris firewalls, ruleset definitions and installation, and the AHPCRC implementation of Kerberos and SecurID. He is also responsible for the overall management support of the HPCMP Kerberos Corporate Realm. He was also the systems analyst responsible for the installation and administration of the AHPCRC's Thinking Machine Co. CM-5, IBM SPs, AFS file system and DNS servers. He has installed and configured Apache webservers, including SSL-enabled versions including troubleshooting system, network and software problems. Paul has developed software for security and system account management tools.

**Technical skills: Languages:** Perl, C, Python, Scheme, csh, HTML, SQL; **Network Technology:** TCP/IP, DNS, NIS/NFS, AFS; **Web-related:** HTTP, CGI, HTML, XML, Apache, SSL; **Security Systems:** Kerberos, SSH, SecurID, Firewall-1, ipchains, Nessus, Snort, Nmap, TCP Wrappers, PGP

### *7.1.3. TODD RANNOW, NetworkCS*

**Profile :** Todd has over eighteen years of experience in systems software, complier, and application design, development, and support. He also has six years of experience in UNIX system administration and two years of experience as a database administrator. Todd participated in the design and implementation of the current AHPCRC computing environment, AHPCRC ARAS, and provided technical leadership to a team of five people in the support and improvement of that environment.

**Technical Skills: Languages:** HTML, ColdFusion, Oracle PL/SQL, Visual Basic, Perl, shell scripts, C; **Operating Systems:** UNIX, MS Windows; **Databases:** MS Access, Oracle, Sybase; **Tools**: MS Office, SQL*PLUS, ColdFusion Studio.

### *7.1.4. DAVID KNUTSON, GREENBRIER AND RUSSEL, INC*

**Profile:** David has over 10 years of experience in the analysis, design, development and implementation of information technology. He has functioned as a programmer, designer, analyst, technical lead and consultant. David has also been involved in strategic information technology planning, software package selection and installation, customization, implementation and process improvement. David is currently specializing in Oracle Customizations and Applications.

**Technical skills:Languages:** BASIC, VISUAL BASIC, PL/SQL, SQL, UNIX SCRIPTING; Databases: ORACLE, MS ACCESS; Development Tools: ORACLE FORMS 4.5 SC/NCA, ORACLE REPORTS 2.5, Oracle Financials, Visual Basic, SQL*PLUS; Methodologies: OOP, standard Oracle customization practices; Other Tools: COLDFUSION

### *7.1.5. WES BARRIS, NetworkCS*

**Profile:** Wes has over 15 years of experience in system and graphics software development. Wes has extensive knowledge in web site administration and web site design including HTML, Perl/CGI, and Java programming. Wes is very experienced in computer animation, video production, image manipulation, and both analog and digital audio editing. Wes has a solid background in UNIX operating systems, UNIX system administration, and Windows operating systems.

**TECHNICAL SKILLS: Operating Systems:** UNIX (RedHat, FreeBSD, IRIX, UNICOS, UNICOSmk) Windows; **Languages:** Perl, HTML, JavaScript, UNIX-Shell, Tcl/Tk, Java, C, FORTRAN; **Graphics APIs**: X Window System, Motif, IRIS GL, OpenGL

## 8.0 PAST PERFORMANCE

### 8.1. Network Computing Services, Inc.

NetworkCS has been a provider of HPC services since 1982. NetworkCS provides HPC services in Fortune 500 companies in aerospace, finance, manufacturing and the petrochemical industries. It has installed

and operated approximately 30 HPC systems, including the DoD HPCMP's first terascale system. NetworkCS has been the infrastructure support contractor for the AHPCRC SRC since 1989.

Government contracts:

AHPCRC Support Infrastructure Contract (DAAH03-89-C-0008) (1995-2000) Army Research Laboratory
COTR Dr. Walter Sturek (Tel: 845-938-7689 or 845-938-4179)
Cost plus fixed fee
$31,545,953.

AHPCRC Support Infrastructure Contract (DASW01-01-C-0015)
COR: Tobin Gatto (703) 602-3705
COTR Charles Nietubicz (Tel 410-278-3691), Dr. Andrew Mark (Tel: 410-278-9761)
Cost plus fixed fee
$18,000,000

### 8.2. Greenbrier & Russel, Inc.

G&R is a privately held strategic information technology services firm headquartered in Schaumburg, Illinois. The company specializes in new and advanced technologies including web development and deployment, package selection and implementation and client/server integration. The company was founded in 1984 and now has nearly 700 employees. Strategic alliances with Oracle, Microsoft, Sybase and Sun have allowed G&R to bring clients an even greater depth of expertise and knowledge in the planning and development of these types of systems. G&R has made a significant investment in the development of a structured approach to project management called the Guide™. This unique approach, which includes a pre-project and a post-project evaluation and communication process, is the key to the successful delivery of all G&R project initiatives.

## 9.0 DELIVERABLES CROSS REFEFERENCE TABLE

**IE Integration**

| | |
|---|---|
| 1. Integrated architecture | 2 |
| 2. XML | 5 |
| 3. Additional sites | 27 |
| 4. Industry standards | 28,45,46 |

**Tool 1**

| | |
|---|---|
| 5. Information by system | 13,15 |
| 6. Information by site or by system | 15 |
| 7. Denote site and system | 14 |
| 8. Usage current as of midnight | 16 |
| 9. Data lockout | 6 |
| 10. User data current as midnight | 16 |
| 11. Data summaries | 14 |
| 12. Previous Fiscal Years | 14 |
| 13. Proper user access | 11,13 |
| 14. Allocation/utilization by criteria | 14,15 |
| 15. # of users and expansion factors | 14,15 |
| 16. COTS reports as listed | 14,15 |
| 17. Metrics reports | 15 |

**Tool 2**

| | |
|---|---|
| 18. Queue status | 16 |
| 19. Multiple views queue status | 16 |
| 20. Queue status, as listed | 17 |

**Tool 3**

| | |
|---|---|
| 21. Exchange of allocations | 17,18 |
| 22. Reports for the S/AAA | 17 |
| 23. Post allocations and advertise | 17,18 |
| 24. Search the posted allocations | 17 |
| 25. Notify of exchange | 18 |
| 26. Reserve account process | 18,19,20 |
| 27. Allocations among projects | 19 |
| 28. Allocations - PIs and S/AAAs | 19 |
| 29. Exchange hours in the reserve | 18,19 |
| 30. Allocations less utilization | 19 |
| 31. Effective in two business days | 20 |
| 32. Log of all transactions | 20 |
| 33. Review of the log | 20 |
| 34. Log reports by criteria | 20 |

**Tool 4**

| | |
|---|---|
| 35. Paperwork for HPCMP account | 20,21 |
| 36. Update contact information | 21 |
| 37. Log of all fill-in actions | 20,21 |
| 38. Review of fill-in actions | 21 |

**Tool 5**

| | |
|---|---|
| 39. Management of paperwork | 22,23 |
| 40. Determine requests received | 22 |
| 41. Assigning of resources | 23 |
| 42. Add "S/AAA only" information | 22 |
| 43. Log management actions | 23 |
| 44. Review management actions | 23 |

IE Interface

| | |
|---|---|
| 45. Access controls | 11,29,32 |
| 46. SSLv3/TLS | 11 |
| 47. Function fully and correctly | 10 |
| 48. Open standards | 10 |
| 49. Open standard interfaces | 28 |
| 50. Portable with different databases | 28 |

**Upgrades/Enhancements**

| | |
|---|---|
| 51. On-line help | 24,25 |
| 52. Validate the operation | 39,42 |
| 53. Validate the data integrity | 28,38 |
| 54. Documentation | 41 |
| 55. Provide training | 42 |
| 56. Problem tracking and reporting | 25 |
| 57. Resolution of critical problems | 42 |
| 58. Resolution of all other problems | 42 |

Scalability/Extensibility

| | |
|---|---|
| 59. Detecting resource status | 27 |
| 60. Adding and removing sites | 27 |
| 61. Optimized for extensibility | 27 |

**Security**

| | |
|---|---|
| 62. No compromise of security | 30 |
| 63. Kerberos tickets | 29 |
| 64. PKI certificates | 30 |
| 65. Kerberized access | 29 |

## 10.0 GLOSSARY

| | |
|---|---|
| AHPCRC | Army High Performance Computing Research Center |
| ARAS | AHPCRC Resource Accounting System |
| COTS | Commercial-off-the-shelf |
| CPU | Central Processing Unit |
| CSV | Comma Separated Value |
| CTA | Computational Technology Area |
| DBA | Database Administrator |
| DC | Distributed Center |
| DoD | Department of Defense |
| DREN | Defense Research and Engineering Network |
| DTD | Document Type Definition |
| GFE | Government Furnished Equipment |
| HPC | High Performance Computing |
| HPCMO | High Performance Computing Modernization Office |
| HPCMP | High Performance Computing Modernization Program |
| HTML | Hypertext Markup Language |
| IAS | Identification and Authentication Sub-system |
| IBM | International Business Machines Corporation |
| IDTS | Internal Data Transfer Sub-system |
| IE | Information Environment |
| IEDB | IE Database |
| IEDBS | IE Database Sub-system |
| IUS | Interactive User Sub-system |
| KDC | Kerberos Distribution Center |
| LAN | Local Area Network |
| MS | Microsoft |
| MSRC | Major Shared Resource Center |
| NCS | Network Computing Services, Inc. |
| NetworkCS | Network Computing Services, Inc. |
| NTK | Need to Know |
| OS | Operating System |
| PI | Principal Investigators |
| PKI | Public Key Infrastructure |
| RCS | Revision Control System |
| S/AAA | Service Agency Approval Authorities |
| SAV | Security Assist Visit |
| SDTC | SRC Data Transfer Computer |
| SDTS | SRC Data Transfer Sub-system |
| SGI | Silicon Graphics, Inc. |

| | |
|---|---|
| SOW | Statement of Work |
| SQL | Structured Query Language |
| SRC | Shared Resource Centers |
| SSH | Secure Shell |
| SSL | Secure Socket Layer |
| ST&E | Security Test and Evaluation |
| UPS | Uninterruptible Power Systems |
| XML | Extensible Markup Language |