EOSDIS User Registration System (URS) - Phase I Operations Concept and Requirements
Scope

This document covers the Operations Concepts and Requirements for Phase 1 of the EOSDIS User Registration System (URS). The Phase 1 system establishes the initial presence of the URS system including:

- High-Availability/High-Reliability hardware and software
- An LDAP-based authentication system
- Web pages for user registration and user profile administration
- An API for data center applications to access all URS capabilities
- Enhanced metrics collection and reporting to provide data centers with additional fidelity in the reporting of data and service access patterns of users. These reports can be used by the data centers to provide notification of changes to EOSDIS data and services directly to those users that are affected by the change.

For Phase 1, the URS will be integrated with Earth Observing System (EOS) Clearinghouse (ECHO) system and the Land Atmosphere Near real-time Capability for EOS (LANCE) system for user registration, profile maintenance, authentication, and enhanced metrics and reporting. Integration of LPDAAC’s DAR Tool will be accomplished via its use of the ECHO authentication service. Similarly, GCMD’s DocBuilder will be integrated as the LANCE system is transitioned to URS. Phase 1 provides the framework that will support additional capabilities in subsequent phases including:

- enhancing our understanding of user access patterns and providing insight into additional services to optimize the use of EOSDIS data
- enabling enhanced user notifications
- tailoring of the user experience
- providing a platform for Single Sign-On and authorization of access to data and services.

Introduction
As EOSDIS systems have evolved over the years, most of the EOSDIS data are now available to users via anonymous on-line access. Although the changes have improved the dissemination efficiency of earth science data, the anonymous access has also made it more difficult to notify users of critical system status changes, characterize users, capture metrics on the value of EOSDIS and provide customized services that benefit users. Additionally, data centers have implemented their own user registration systems, and provided new tools and interfaces for their registered users. This has led to the current implementation of independent data center registration systems for ordering or accessing data and interacting with online tools and services. The user profile information maintained by each of these registration systems is not consistent and the registration enforcement varies by data center as well. A consolidation of registration systems into an EOSDIS wide User Registration System (URS) presents an opportunity to improve the user experience through simplification of user registration and profile management. Users will be able to register once at a central location and gain basic access to publicly available EOSDIS data or services hosted at each of the data centers.

The EOSDIS URS will enable EMS to collect and analyze data on the usage of delivered products and services at an increased level of detail. This will help the EOSDIS program to better understand the user demographics and access patterns, to support planning for new value-added features and customized services that can be directed to specific users or user groups resulting in better user experience.

The EOSDIS URS will also provide a platform for notifying users of significant status changes across the EOSDIS data centers. This platform will allow the data centers to uniformly disseminate notifications of changes in the availability of data or services to the affected members of the EOSDIS user community.

Operations Concept

The primary goals of the User Registration System (URS) are to:

- Provide a uniform mechanism for registering and authenticating users for access to EOSDIS data so information about these accesses can be provided to EMS. EMS can then be used by the Data Centers to report statistics about user interests and access patterns including the number of users, type and amount of data archived, type and amount of data distributed, and other related information.

- Enable status change notifications to users regarding availability of EOSDIS data and services. By combining the user information gathered by URS and the data and service usage metrics gathered by EMS, the data centers can direct notifications to those subsets of user that may be affected by a change to data or services. For Phase 1, the access information will be generated by URS & EMS in static reports for ECHO and LANCE. Full ad-hoc reports will be provided in a subsequent phases.
• Establish a framework for future capabilities such as user tailoring of customized views, saved queries and enhanced order management.

The URS will provide user registration and authentication services and a common set of user information to all EOSDIS data centers in a manner that will permit the data center to integrate their additional requirements with the URS services and information. URS services will cover the following areas:

• **User Registration.** The URS will offer a web interface that permits users to register with EOSDIS. The user will be able to create a user identification of their choice provided that this identifier has not yet been taken, and choose a password. They will then be prompted to provide additional information such as name, affiliation, country and an e-mail address. The user can be directed to the EOSDIS user registration web page from data center applications and web sites. Users who are not yet registered with EOSDIS and thus cannot be authenticated may also be referred to the http://Earthdata.nasa.gov website when attempting to access EOSDIS data via ECHO or LANCE, and will be referred back to the original application after the registration has been completed successfully. Alternatively, an API to the URS system will also be provided for Data Center applications to register and authenticate their users without requiring the user to access the URS web pages. There will be a transition process that will migrate existing user profile information to the URS which will include provisions to identify multiple profiles for the same user and reconcile profiles that have colliding user identifications.

• **User Authentication.** The URS will offer an authentication service that will be integrated with ECHO and LANCE Authentication services in lieu of their existing registration mechanisms. This will result in the automated migration to URS by some data center applications, such as the LPDAAC DAR Tool, which currently use the ECHO authentication API. Each application will be expected to obtain authentication information from the data access requestor, pass this information to a URS authentication interface, and receive a response from the URS which indicates successful or failed authentication. For each application the URS will maintain a record of authentication frequency and last authentication. EOSDIS data is also accessed by external portals which themselves serve a large user community. In Phase 1, the URS will provide authenticated access to EOSDIS data by portals which will be registered, authenticated, and tracked as if they were a user.

• **User Profile and Password Expiration and Renewal.** The URS will not expire passwords. However, the URS will automatically flag user accounts as expired if they have not been used for a configurable amount of time. The expired status is primarily for filtering reports, and will not be used to deny access to data or services. These accounts are considered inactive, but they will not be removed from the URS database. They can be reactivated by administrative staff and will be reactivated automatically if a successful user authentication takes place.
For active profiles, the URS will also ask users to review the information in their profile and confirm its correctness after a globally configurable amount of time since the profile was created, last updated, or last confirmed (the method for prompting the user to do so will need additional data center feedback and remains an issue). Users who forget their user identification can request that it be revealed to them by providing their e-mail address. They can also request that a new one-time password be sent to their URS e-mail address in case they forgot their current password. These requests are automated and will complete without human intervention.

- **User Profile Maintenance.** Users will be able to update their profile at any time by returning to the EOSDIS URS registration page and logging in. All of the user profile attributes are subject to update except for the user identification. The URS also provides for the role of a User Profile Administrator, who has the same update privileges. Users will be notified via e-mail of changes to their profile, whether performed by the user, a User Profile Administrator, or a member of the URS Operations Support Team.

- **User Profile Access.** User Profile Administrators will be able to search and retrieve user profiles, for example, so they can investigate problem reports or to populate e-mail lists. The URS will also offer an efficient bulk export capability to provide user profiles for user and profile related reporting. To distribute and simplify User Profile Administration, the URS will support User Groups. A User Group is a named collection of URS users. A person with Group Administration privileges for a Group will be able to perform User Profile Administration activities for members of the group. For example, we may establish an ECHO User Group which will contain all of the URS users who were migrated from the ECHO system during the Phase 1 transition. This would allow the existing ECHO Administrators to continue to provide profile support to their users.
User Scenarios

This section provides a description of the URS operations concepts in the following scenarios:

Scenario 1 (User Registration):

Scenario 2 (User Data Access):

Scenario 3 (Password Reset):

Scenario 4 (URS Profile Administration):
  A. Single User Profile Update
  B. Bulk Export of New User Profiles – Non-partitioned
  C. Bulk Export of New User Profiles – Partitioned by Group

Scenario 1 (User Registration):

A. Web based registration from EOSDIS web site (Earthdata.NASA.gov)
   1. The user employs a web link available on the EOSDIS web site to register for EOSDIS data access
   2. The URS registration interface provides a web interface that allows the user to select a user identification and a password or pass phrase, and complete the user profile information.
   3. The URS validates the profile information and will prompt the user for corrections if it finds errors. [Validation details are TBD by design.]
   4. The URS saves the user profile in a persistent repository. In the case of a distributed implementation, this includes replicating the change among the other URS servers.
   5. The URS sends a confirmation e-mail to the user. The e-mail includes a validation link that refers back to the URS.
   6. The user clicks on the registration validation link, thereby confirming the correctness of the e-mail address and completing the registration.

B. Web based registration with referral from an Application (ECHO or LANCE).
   1. The user employs a web link available on the Application’s GUI to register for EOSDIS data access. The link leads to the URS registration page as in Scenario 1A.
   2. The user registers using the URS registration page as in Scenario 1A, Steps 2-4.
   3. The URS sends a confirmation e-mail to the user. The e-mail includes a validation link that refers back to the URS.
4. The user clicks on the registration validation link, thereby confirming the correctness of the e-mail address and completing the registration.

5. The URS updates the most recent authentication date and result for that user and application.

6. The URS reverts control back to the target page of the Application, including selected attributes of the user’s profile.

Scenario 2 Authenticated User Data Access:

A. ECHO Data Access via the URS API

1. The user accesses a ECHO user interface (e.g., Reverb) and logs into ECHO.

2. ECHO employs the URS API to provide the login information to the URS.

3. The URS matches the login information with a user profile.

4. In case of a match, the URS returns the required user profile information together with a confirmation of successful authentication to ECHO.

5. The URS updates the most recent authentication date and result for that user and site.

6. ECHO caches the successful authentication for the duration of the user session, together with the user identification and any other relevant profile information.

7. ECHO/Reverb confirms the successful login to the user.

8. The user performs a search and creates and submits a data order.

9. ECHO submits the necessary data order(s) to the data providers. Since ECHO already authenticated the user, further authentication by the data center application is not necessary. Rather, ECHO/Reverb provides all the requisite URS and ECHO user profile information as part of the order.

10. ECHO logs the order for EMS reporting (including any required user information provided by URS).

The user logs out of ECHO. ECHO removes the user information from its cache.

B. External Application using the ECHO Authentication API (e.g., DAR Tool)

1. The user accesses the External Application’s interface to log in.

2. The External Application employs the ECHO authentication API to provide the login information to ECHO.
3. ECHO employs the URS authentication API to provide the login information to the URS.
4. The URS matches the login information with a user profile.
5. In case of a match, the URS returns the required user profile information together with a confirmation of successful authentication to ECHO.
6. The URS updates the most recent authentication date and result for that user and site.
7. ECHO confirms the successful authentication to the External Application.

C User Data Access via LANCE:

1. The user accesses the LANCE FTP (or http, scp, etc.) server using the credentials of their previously created URS account.
2. The LANCE FTP server authenticates the user by performing an LDAP query to the URS LDAP server.
3. The URS LDAP server authenticates the user and logs the authentication request (or failure).
4. The URS LDAP server returns the successful authentication information to the LANCE FTP server.
5. The LANCE FTP server provides the user with access to the data.

Scenario 3 (Password Reset):

1. A user attempts to access EOSDIS data via ECHO or LANCE (or their client applications), but cannot recall the password or user identification.
2. The user clicks on an “I forgot…” button in the ECHO or LANCE application web page that refers the user to the URS web page.
3. Responding to a URS prompt, the user provides his/her e-mail address.
4. The URS finds the matching user profile, generates a temporary password, sends it to the user via e-mail.
5. The user retrieves the e-mail, logs into the URS using the temporary password and enters a new password.
6. The URS refers the user back to the application confirming successful authentication and providing the required user profile information.

Scenario 4 (URS Profile Administration):

A. User Updates Their Profile
1. A user goes to the URS profile update page either directly through the EOSDIS website (Earthdata.NASA.gov) or indirectly by selecting profile edit in the ECHO gui. In either case, the user will be authenticated before access to the profile is granted.

2. The user updates the user profile information.

3. The URS logs the update and sends an e-mail to the e-mail address on file to inform the user of the update. If the e-mail address itself changed, the e-mail is also sent to the old e-mail address.

B. Profile Administrator Updates Profile for a User

1. A URS Profile Administrator has a need to perform a single profile update for a user who is identifiable by either their name, e-mail address, or URS user name.

2. An administrator logs into the URS web page as a User Profile Administrator.

3. The administrator accesses the URS administrative functions.

4. The administrator searches the user profiles for a particular user identification or e-mail address or user name and displays the result.

5. The administrator updates the user profile information, confirming the update by entering his/her password once more.

6. The URS logs the update and sends an e-mail to the e-mail address on file to inform the user of the update. If the e-mail address itself changed, the e-mail is also sent to the old e-mail address.

C. Group Administrator Updates Profile for a User

7. A URS Group Administrator has a need to perform a single profile update for a user who is identifiable by either their name, e-mail address, or URS user name.

8. An administrator logs into the URS web page as a Group Administrator.

9. The administrator accesses the URS administrative functions.

10. The administrator searches the user profiles for a particular user identification or e-mail address or user name and displays the result. [Note that search results are limited to users who are members of the Group.]

11. The administrator updates the user profile information, confirming the update by entering his/her password once more.

12. The URS logs the update and sends an e-mail to the e-mail address on file to inform the user of the update. If the e-mail address itself changed, the e-mail is also sent to the old e-mail address.

D. Bulk Export of New User Profiles – Non-partitioned

1. A user logs into the URS web page as a User Profile Administrator.

2. The administrator accesses the URS administrative functions.
3. The administrator accesses the URS bulk export functions and selects the function to export selected user profiles to a file. The URS retrieves the active user profiles and places them into a file.

4. The administrator ships the file via ftp (or scp) to the data center that requested the information.

**E. Bulk Export of New User Profiles – Partitioned by Group**

1. User logs in as User Profile or Group Administrator and accesses the URS administrative functions.

2. The administrator accesses the URS bulk export functions and selects the function to export all active user profiles to a file.

3. The URS retrieves the active user profiles that are applicable to that Group and places them into a file.

**Scenario 5 (User Notification of New ECHO Service Availability -- Phase 1):**

1. ECHO’s URS Group Administrator has a need to notify all ECHO users of a new service to be provided by ECHO.

2. The administrator logs into the URS web page as a Group Administrator.

3. The administrator accesses the URS administrative functions.

4. The administrator searches for all email addresses of users in the ECHO application group.

5. The administrator filters the list to only include unexpired users.

6. The administrator exports the email addresses to a file.

7. The administrator sends an email announcing the new service to all of the exported email addresses.
Updated Business Requirements

This section provides the business requirements for the URS. The requirements are grouped into the following eight categories:

1. User Registration,
2. User Profile Maintenance,
3. User Authentication,
4. User Profile Administration,
5. URS Administration,
6. Performance,
7. Availability,
8. Security and Privacy,
9. User Notifications,
10. Browsers

Wherever applicable, the source(s) for the requirement update are provided within square brackets at the end of the corresponding requirement text.

3.1 User Registration

1. The URS shall allow users to request a new account for registered EOSDIS access.

2. The URS shall allow the user to enter user profile information during registration.

3. The URS shall provide for the following user profile information:

- User identification
- Password
- First name [source: SDPS, prototype]
- Middle Initial [source: SDPS]
- Last Name [source: SDPS, prototype]
- E-mail address [source: SDPS]
• Affiliation [source: prototype]
• Organization
• Primary Study Area
• Type of User
• Country [Note that the URS will use the same approved country list as ECHO]
• Telephone number [source: interviews]
• Fax number [source: interviews]
• Mailing address [source: interviews]
• Portal Name
• List of Contacts for Portal

4. The URS shall support user profiles for portal applications that act on behalf of users [source: interviews].

5. The URS shall allow a user to choose a user identification and password.

6. The URS shall verify user profile information against validation rules, including the following:
   • The following information items shall be mandatory [source: prototype]: User identification, password, first name, last name, e-mail address, affiliation, country.
     ○ Note: A list of predefined affiliations shall be available and offered to the user for selection, but the user may enter a different affiliation [source: prototype].
   • The user identification shall be case insensitive and must be unique [source: prototype].
   • The rules governing password composition shall be configurable.
   • The e-mail address shall be a syntactically correct internet e-mail address and must be unique within the URS [source: prototype].
   • The country shall be selected from a predefined list [source: prototype].

7. The URS shall verify the correctness of a user’s e-mail address before activating the user’s account by sending an e-mail to the specified e-mail address with a link the user must select to activate the account [source: interviews]

8. The URS shall include provisions that defend against user registration by an automated mechanism (e.g., a CAPTCHA mechanism) and provide accessibility options that are 508 compliant.
9. The URS shall expire a user registration session after a configurable amount of time [source: prototype].

10. The URS shall capture registration web metrics using EMS (e.g. Unica NetInsight page tagging). [source: prototype]

11. The URS shall be able to engage a user in a user registration session after redirection from another application.

12. If engaging in a user registration session after redirection from another application, the URS shall record the registered application from which the registration originated.

13. If engaging in a user registration session after redirection from another application, the URS shall return the user to the landing page specified by the re-directing application [source: interviews].

14. The URS shall provide a secure API and web interface to authenticate registered EOSDIS users. [source: KJM comments]

3.2 User Profile Maintenance

15. The URS shall allow users to update their profile information, including password and email address but excluding the user identification (the URS may also generate a unique internal identifier such as a UUID to identify user accounts).

   a) NOTE: The URS will not allow the same email address to appear more than once in the database

16. The URS shall expire user accounts that have not been used for a configurable amount of time; however, expired accounts shall not be removed from the URS except through explicit action by a URS administrator.

   a) Purpose of profile expiration will have diverse input from stakeholders. For the URS it is only an attribute value. We will not ‘lock’ expired accounts for example.

17. The URS shall renew an expired user account automatically when a successful authentication for that user occurs (the URS may request confirmation of the profile information on that occasion) [source: interviews].
18. The URS shall allow users to request a password via e-mail to their current e-mail address that provides them with a one-time ability to update their account information (e.g., provide a new password) [source: interviews].

19. The URS shall allow users to request that their user identification be revealed to them via email [source: interviews].

20. The URS shall ask a user of an active account for confirmation of the profile information after a configurable amount of time since the profile was established, last updated, or last confirmed, for example, during the next authentication or via e-mail [source: interviews].

21. The URS shall authenticate users before allowing them to change their account information.

22. The URS shall inform a user via e-mail each time the user’s profile was changed, using the old and new e-mail in case of e-mail address changes.

**3.3 User Authentication**

23. The URS shall provide secure interfaces that can be used by EOSDIS data access services for the authentication of users.

24. The URS shall allow an application to request the return of a selectable set of user profile attributes after a successful authentication. [source: interviews]

25. The URS shall record the origin of an authentication request, authentication frequency, and the last time authentication was requested for that user from that application, separately for successful and unsuccessful authentication.

**3.4 User Profile Administration**

26. The URS shall support the role of User Profile Administrator.

27. The User Profile Administrator shall be able to:

   a) Create or Delete user accounts,

   b) Update user profile information,

   c) Expire user accounts,

   d) Re-activate user accounts,

   e) Create or Delete User Groups,
f) Assign Users to a group,
g) Remove Users from a group,
h) Assign Group Administration privileges to a user.
i) Remove Group Administration privileges from a user.

28. The URS shall authenticate User Profile Administrators before allowing them to exercise user profile administration capabilities.

29. The URS shall allow User Profile Administrators to search and retrieve user profile information.

30. The URS shall allow User Profile Administrators to bulk retrieve user profile information, e.g., into tab- or comma delimited text files.

31. The URS shall allow User Profile Administrators to update a user profile on behalf of a user.

32. The URS shall provide the capability for EMS to pull required user profile information from the URS.

33. The URS shall provide for bulk export reports to be filtered by the following user profile attributes:
   a) Group
   b) Expiration status
   c) Portal or not

34. The URS shall provide an audit log for changes not performed by the user to include: [source KJM comments]
   a) Administrators user name
   b) User name of the account
   c) Reason for the change
   d) Date/time of the change
   e) Fields changed
3.5 URS Administration

35. The URS shall allow the user profile schema and validation rules to be configurable.

36. The URS shall provide user profile reports, such as new user accounts, account expirations, account renewals, number of successful/unsuccessful authentications, and number of active and expired users *(user accounts that were not authenticated within a configurable period of time).*

37. The URS shall provide performance reports, such as number of authentication requests and response time statistics.

38. The URS shall provide availability reports, such as number and durations of URS server and network outages.

39. The URS shall provide reports on security events, such as denied authentication attempts and password resets.

3.5 Group Administration

40. The URS shall allow Group Administrators to search and retrieve user profile information for members of their group.

41. The URS shall allow Group Administrators to bulk retrieve user profile information, e.g., into tab- or comma delimited text files, for members of their group.

42. The URS shall allow Group Administrators to update a user profile on behalf of a user in the group [source: interviews].

43. The URS shall allow Group Administrators to add users to their group.

44. The URS shall allow Group Administrators to remove users from their group.

45. The URS shall automatically add users to a Group for the Application (e.g., ECHO) that they used to access EOSDIS data via URS authentication.

46. The URS shall automatically add users to a Group for each site (e.g., LP DAAC) where they accessed data via URS authentication.
3.6 Performance

47. The URS shall be able to support 1 million registered users.

48. The URS shall be able to perform one million (1,000,000) authentications per day (equivalent to approximately 12 authentications per second peak) [source: interviews and metrics. See Appendix A for the metrics and calculations]. The breakdown of authentications is as follows:

- User lookups: 968K/day
- Email lookups: 1500/day
- New user registrations: 15,000/day
- Profile updates: 15,000/day

49. Any URS action needed as part of the activation of a user’s account (e.g., sending an e-mail, replicating profile information) shall occur within 10 seconds of completion of the event requiring this action (e.g., a user completing the registration form).

   a) The elapsed time should start upon receipt of the request by the URS not upon the users action which initiates the action

50. Any e-mails which the URS sends as confirmation of user account changes shall be sent within 10 seconds after the account change was completed.

51. A URS server shall be able to respond to a user authentication request – including the provision of the needed user profile information - within 0.1 seconds of receipt exclusive of local network latency.

52. The URS shall log events as necessary to determine URS workload and response times.

53. The URS shall be capable of performing 15,000 new user registrations per day. [source KJM comments]

54. The URS shall be capable of performing 15,000 profile updates per day. [source KJM comments]

3.7 Availability

55. The URS shall be available for user registration and authentication 99.99% of the time [source: interviews].
56. The URS shall provide the capability to restore user profile information in case of data loss or corruption at a URS server.

57. The URS shall log events as necessary to determine URS availability, such as the shut-down or restoration of a URS server, loss of network connection, etc.

**3.8 Security and Privacy**

58. The URS shall not reveal password information or include passwords in any log.

59. The URS shall support secure communication mechanisms for the exchange of authentication and user profile information.

60. Applications shall be able to provide non-refutable authentication credentials to the URS as part of the authentication exchange.

61. The URS shall be able to provide non-refutable authentication credentials to the Applications as part of the authentication exchange.

62. The URS shall provide mechanisms to protect user profile data against unauthorized access.

63. The URS shall maintain a security audit trail which records user and administrator logins and result, user registrations, user account de-activations, re-activations, and renewals, password resets, and changes to user profiles to include the nature of the change and the identification of the user who initiated the change.

64. The URS shall be able to recognize excessive user login attempts and alert system administrators when such a situation is discovered.

65. The URS shall lock out an account after excessive login attempts have exceeded a configurable threshold, and lock out subsequent accesses from the source IP address.

66. The URS shall reference, and comply with, the privacy policies as specified in the ESDIS SORN.

**3.9 User Notification of System Status Changes**

67. The URS shall provide user profile information to EMS which will be used in generating reports containing user profile and access information for those users who have accessed EOSDIS data through ECHO or LANCE applications. [Note that the exact content of the reports will be coordinated with EMS, ECHO, & LANCE.]

**3.10 Browser**
68. The URS web pages shall be Section 508 compliant.

3.11 Interfaces

69. The URS shall provide a mechanism for EMS to pull user profile information from URS.

70. The URS shall send log files to EMS.

Appendix A -- Performance Metrics and Estimates

Performance metrics were collected from ECHO and LANCE as representative EOSDIS applications. These metrics are shown in the table below. Note that the 2 systems are very different in that ECHO has a large number of users, but a low authentication rate whereas LANCE has a small number of users, but a high authentication rate.

We used these metrics to calculate the performance requirements based upon the expected load in Phase 2. For those calculations we assumed that 15 applications would be migrated to URS during the Phase 2 timeframe. The final performance requirements (see section 3.6 Performance) exceed the estimates in the table below.

<table>
<thead>
<tr>
<th>Source</th>
<th>Num Users</th>
<th>Daily Authentications</th>
<th>Daily Failed Authentications</th>
<th>Daily Registrations</th>
<th>Daily Profile Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECHO</td>
<td>42000</td>
<td>1357</td>
<td>214</td>
<td>48</td>
<td>4</td>
</tr>
<tr>
<td>LANCE</td>
<td>707</td>
<td>23656</td>
<td>6285</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Avg = (ECHO + LANCE)</td>
<td>21354</td>
<td>12507</td>
<td>3250</td>
<td>25</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>Max = MAX(LANCE,ECHO)</td>
<td>42000</td>
<td>23656</td>
<td>6285</td>
<td>48</td>
<td>4</td>
</tr>
<tr>
<td>Phase 2 Avg = Avg * 15</td>
<td>320303</td>
<td>187598</td>
<td>48743</td>
<td>375</td>
<td>45</td>
</tr>
<tr>
<td>Phase 2 Max = Max * 15</td>
<td>630000</td>
<td>354840</td>
<td>94275</td>
<td>720</td>
<td>60</td>
</tr>
</tbody>
</table>