

# PDR RID Report

**Date Last Modified** 6/8/95  
**Originator** Donald Collins  
**Organization** JPL PO.DAAC  
**E Mail Address** djc@seanchor.jpl.nasa.gov  
**Document** CSS Services

**Phone No** 818-354-3473

<b>RID ID</b> PDR 227
<b>Review</b> CSMS
<b>Originator Ref</b>
<b>Priority</b> 2

**Section**

**Page**

**Figure Table**

**Category Name** Design-CSS

**Actionee** HAIS

**Sub Category**

**Subject** Security Services - CSS

**Description of Problem or Suggestion:**

Imposition of security - either data or checksum encryption.

**Originator's Recommendation**

Comment:

We need to ensure that these services do not impose an overhead on Internal DAAC Data Flow.

We may need checksum encryption for some external data flows - but most data flows to the scientific community do not require any security on the data set. We do need secure hosts for FTP, etc.

We do not want encryption for DAAC internal data transfer because this will present internal overhead.

**GSFC Response by:**

**GSFC Response Date**

**HAIS Response by:** Forman

**HAIS Schedule** 2/28/95

**HAIS R. E.** N.Hota

**HAIS Response Date** 5/17/95

It is correct to say that data or checksum encryption will cause some amount of overhead in the system.

The security service is set up that the client or server can impose levels of security protection of data or information being sent over ECS. The security level that is used to protect data/information is selectable by the ECS applications developer, based on the defined security need or as may be imposed by ECS guidelines.

Unnecessary use of data or checksum encryption can be avoided in the ECS system, but we do not want to preclude the ability to use encryption where or when needed. Our current baseline is not to encrypt science data to be delivered to users.

**Status** **Closed**

**Date Closed** **6/8/95**

**Sponsor** **Broder**

\*\*\*\*\* **Attachment if any** \*\*\*\*\*