CERES SCF STATUS

Description	*September 13, 2000 Status*	*Problems*
Thunder & Lightning	Thunder and Lightning's operating system was re-installed September 4 - 5 after security breach over weekend of September 1 - 3. See "Security" section below.	
Ntrigue/Citrix Metaframe servers	All user passwords was forced-expired due to security breach of password files on Thunder and Lightning. Passwords on terminal servers are now set to auto-expire every 30 days.	
Security	On Friday, September 1st, at 5:23 am, thunder and lightning were compromised by a malicious attacker, who exploited a buffer overflow in telnetd. The CERT advisory had been released the day before, and no vendor patches were available to protect against the exploit. Since thunder and lightning support a large number of outside labs and field missions, their tcp_wrappers setup was less restrictive than the rest of our systems, making them the only systems under our control vulnerable to this particular attack. Most of our systems refuse connections to everyone, and allow a select list of hosts for the convenience of the users, while thunder and lightning refuse hosts and domains that have attacked us in the past. On Tuesday, September 5th (after the holiday weekend) we discovered the security breach. With cooperation of Network Support, we started cleanup of Thunder and Lightning and by September 6th, the systems was restored to a known good Operating System from a clean backup. No trojans are evident in the data files or user files, though monitoring continues since some subtle ones may have been inserted. The users have been informed of the severity of the compromise, have been asked to warn the admins of systems that have contacted anytime within the last month, since their accounts may have been used to compromise those systems, and have been given instructions on how to work as securely as possible with the knowledge that the attacker still has compromised LaRC machines that could be used to sniff any network traffic. User accounts where locked until users where verified. We are working with the DAAC and volunteered assistance as needed. So far Trance has been cleaned with the remaining compromised DAAC machines being brought back during the remainder of the week.	
Remedy Problem Tracking System	Remedy has suggested that we move to use ARWeb version 4 to correct the menu problems. Unfortunately, there isn't a version of the admintool for unix for ARSystem 4, only a Windows NT version with no anticipated support for a Unix version of the admintool. We loaded the NT version of the admintool and used it to port our configuration and data to version 4 of ARSystem. This appears to have fixed the menu problem, we will need to test further. Unfortunately, this also broke the help desk central application (what is used by the System Administrators to manage the help requests). Remedy is working on getting the help desk central application to work with ARSystem 4 no current ETA from Remedy. This is continuing to consume a large portion of System Administration resources.	
Tape Library	Construction in the Tape Library is basically complete.	

Description	*September 13, 2000 Status*	*Problems*
AMLJ	Testing for the AMLJ has been delayed as resources are allocated to recover from Thunder and Lightning's security breach. Testing will restart as soon as possible.	
On site network problems	Network has been normal except for typical sporadic outages. As outages occur we contact and work with Network Support. Network security performed various security scans of machines assigned to Codes REB and REC on September 11 which caused some minor interruptions and nuisance errors.	

CERES SCF/DAAC Server Information

Server Name:	Asdsun	Blizzard	thunder	Lightning	Darrin	Samantha
Operating System:	Solaris 2.6	IRIX64 6.5.7m	IRIX64 6.5.7m	IRIX64 6.5.7m	IRIX64 6.5.7m	IRIX64 6.5.7m (6/22/2000)
Fortran compilers	SUNWspro 4.	7.3.1.1m	7.3.1.1m	7.3.1.1m	7.3.1.1m	7.3.1.1m (6/22/2000)
Toolkit	TK5.2.6v1	TK5.2.6v1	TK5.2.6v1	TK5.2.6v1	TK5.2.6v1	TK5.2.6v1
Ada	N/A	1.3	1.3	1.3	1.3	1.3 (6/22/2000)
IDL	5.1.1	5.1.1	5.1.1	5.1.1	5.1.1	5.2
NAG fortran 95	1.0(428)	1.0(428)	1.0(428)	1.0(428)	1.0(428)	1.0(428)
HDF	4.1.r3	4.1.r3	4.1r3	4.1r3	4.1.r3	4.1r3
Proposed upgrades:	None	None	None	None	None	None
Problems:	None	None	None	None	None	None