IT Security Plan for the Polar EFI Instrument

Summary of Critical Functions

Overall responsibility for all EFI operational and data issues lies with the EFI Principal Investigator, Professor Forrest Mozer, at Space Sciences Laboratory, University of California, Berkeley, CA. 94720, (510)642-0549.

Monitoring the health of the instrument: Timely receipt and evaluation of EFI data is achieved through regular examination of the Level Zero files that are downloaded via ftp on a daily basis. Commanding of the instrument is required infrequently, generally following reorientation of the spacecraft spin axis, because at such times the instrument burst modes have to be adjusted for the new orbit period.

Generating command sequences: EFI commands are generated by the Project Engineer, Peter Harvey, and are validated in ground support hardware before being uploaded to the spacecraft. Routine daily or weekly commanding is not required for EFI operation.

Transfer of commanding sequences to mission operations personnel: Commands are general relayed from the EFI Project Engineer to flight operations personnel via email, or telephone.

Maintenance of support equipment: Support and maintenance of EFI ground hardware is the responsibility of the EFI Project Engineer. Flight software maintenance and upgrades are also the responsibility of the Project Engineer. Data analysis software is continuously being improved and upgraded by Jack Vernetti and Winston Teitler.

Summary of Other, Non-Critical But Important Functions:

EFI also provides gound analysis software, graphic files and associated data dumps to other users of EFI data. It is estimated that about 100 scientists are currently using the SDT data analysis program provided by EFI. The data analysis, display, and data download software resides on several Sun workstations at the Space Sciences Laboratory. Primary responsibility for the maintenance of these servers resides with the EFI software administrator, Jack Vernetti.

EFI Backup and Recovery Policies:

The EFI team has general policies in place that apply to all the servers and software under its responsibility.

All servers and workstations are maintained by a team of three system administrators, Walter Herrick, Jon Loran, and Bruce Satow.

All new information content on the server supporting EFI is backed up nightly under the direction of Walter Herrick. Periodically (approximately every other week) the entire system is backed up. At least quarterly, a restore is performed from the backup tapes to verify backup integrity. In addition, the Level Zero data is stored on CD roms, as an additional safety precaution.

Passwords for key machines and accounts are held by at least two people. Root passwords for the server and important workstations are known to the system administrators and to the software developers.

For critical instrument monitoring and commanding functions: Software for analyzing the Level Zero data from EFI resides on approximately 200 Sun workstations around the world

For data service functions: Recovery of data services will be provided by the use of backup tapes to restore data download/production processes to existing or newly procured servers. Restoration of the files from tape could be accomplished in a day or two and any minor adjustments due to recent modifications would require approximately 1 man-week of an experienced senior programmer's time.

Documentation: EFI software is documented in electronic manuals that are distributed to all users with each new release. New releases occur approximately every 3 months. These manuals include an installation guide and a users guide describing the menu hierarchy and the data quantities that may be computed with the SDT program.

EFI Backup and Recovery Plan:

GSFC security personnel have identified seven levels of security threat to be addressed by NASA mission security plans. Definitions of these threat levels are listed at the end of this document and at http://eiger.gsfc.nasa.gov/burst/. Backup and recovery plans to be applied for EFI, with regard to these levels of threat, are as follows:

7. Credible threat

In normal operation, instrument commanding is not required. Commands can be remotely generated and submitted to the GSFC FOT. The P.I. and the software developers maintain off-site network access for this function and for remotely monitoring instrument health.

Most science data processing and data access procedures are automatically performed by the GSFC server. Service to these should continue uninterrupted even in the event of an absence of IT system personnel. Some maintenance can be performed by remote access by the GSFC system administrators and the EFI Project Engineer.

6. Data loss/corruption

Recovery of software, data, and data processing functions can be provided by the use of backup tapes and existing or newly procured servers.

System and software backup procedures should be adequate such that EFI ground system machines could be restored or duplicated within 1 day to 1 week time depending on the extent the machines are affected and the availability of experienced personnel, hardware, and space resources. New servers and a DLT tape drive for a temporary facility could be acquired in approximately one week or tapes could be shipped to the EFI programmer for use on borrowed servers.

Replacement of the primary GSFC server, data archive and commanding PCs would cost approximately $100k.

Instrument commanding sequences can be remotely generated until the GSFC machines are restored. It is also possible, though not optimal, to command the instrument from within the GSFC mission operation center if experienced EFI commanding personnel have access to that facility.

5. Loss of one or more critical systems
same as above

4. Extended power outage/cyber attack
same as above

3. Localized destruction or contamination

same as above

2. Widespread destruction

same as above

1. Complete devastation

a. Including substantial loss of life

The EFI P.I., the EFI Project Engineer, and the EFI software developers have unique and primary knowledge of instrument behavior and safe commanding procedures that co-investigators do not. Data serving and programming responsibility can be resumed at a temporary site by GSFC personnel, with the assistance of the EFI P.I., the EFI Project Engineer, or the EFI software developers. Commanding of the instrument occurs infrequently so that loss of this capability during a transition period is not critical.

b. Little or no loss of life

same as above

Contact Information:

Forrest Mozer	(510)642-0549
Peter Harvey	(510)642-0643
Jack Vernetti	(510)642-4869
Winston Teitler	(510)642-2405
Walter Herrick	(510)643-8611
Bruce Satow	(510)643-8611
Jon Loran	(510)643-8611

Threat Definitions

Last revised: 11/14/01 (from http://eiger.gsfc.nasa.gov/burst/)

1. **Complete devastation** – Involved institution is entirely, or nearly entirely unusable, whether because of destruction of facilities or contamination with long-lasting agents (*e.g.* radioactive materials). This condition is likely only in the event of a terrorist-type attack, hurricane, tornado or an earthquake.

Including substantial loss of life – devastation occurred during a prime, weekday shift; critical oversight as well as operations personnel lost

b. **Little or no loss of life** – devastation occurred during night/weekend shift or after evacuation of personnel; critical operations could be resumed at remote sites if surviving personnel were able to relocate

2. **Widespread destruction** – Several critical facilities (*cf.* list of critical facilities) inoperable/unrecoverable, but some critical facilities still in working order, and at least some critical personnel available to continue operations. This level of destruction could be caused by a smaller-scale terrorist attack or, more likely, by a smaller scale weather related disaster. This would depend on the durability of individual buildings and IT systems to the conditions imposed. Critical operations could be resumed in on-site or (more likely) remote locations.

3. **Localized destruction or contamination** – Some buildings destroyed or rendered unusable, possibly with some loss of key personnel. This condition could be caused by a tornado, by a fire or by application of chemical or biological agents to a limited number of workplaces. In either case, the affected facilities would be unavailable for an indeterminate length of time. Critical operations could be resumed in on-site locations if backup facilities were available.

4. Extended power outage/cyber attack – Due to terrorist action, natural phenomena, extreme space weather, or simple miscalculation, the electric power grid could be disabled for longer than the period covered by the diesel fuel supply for on-site generators. If widespread, such a loss of power could lead to civil disorder, making resumption of power supply or refilling of fuel supplies unpredictable. Similarly, a successful cyber attack against local area networks or the entire Internet could bring down many critical systems, with no short-term recovery options. Either of these cases would require remote, secure facilities for the resumption of critical operations.

5. Loss of one or more critical systems – Loss of critical operations facilities (*e.g.* Buildings, etc.) or power plant(s) due to physical system failure (*e.g.* water pipe bursting), extreme weather, earthquake, or terrorist/disgruntled employee/former employee action. Critical operations could be resumed on-site if backup facilities were available.

6. Data loss/corruption – Significant mission-critical, financial, or scientific data system data loss and/or corruption, due to any of 1-5, or other causes (*e.g.* sabotage or component failure). Data and software could be reproduced if verified backups were in place, on-site or off.

7. **Credible threat –** Institutional management may have to make decisions on the basis of advice from security, law enforcement agencies, and/or other national authority that it is unsafe for the non-essential workforce, or any of the workforce, to report to work. No loss of facilities, infrastructure or life may occur, but physical access to facilities is denied or limited to a small number of essential personnel.