SMEX Safety, Reliability, and Quality Assurance Requirements

Prepared by the NASA/GSFC Explorer Program Office in support of the Small Explorer (SMEX) Announcement of Opportunity Process

December 27, 2002

1.0 GENERAL INFORMATION

1.1 Overview

Missions selected under this Small Explorers Announcement of Opportunity (AO) will be structured so that the Principal Investigators will be responsible for all aspects of their missions, including Safety, Reliability, and Quality Assurance (SR&QA). It is intended that Principal Investigators tailor their SR&QA programs in accordance with ISO 9001 series standards. This approach maximizes the use of existing and proven PI team processes, procedures, and methodologies.

The mission assurance requirements for the program recognize a wide variation in complexity, size, and technology for the mission, which can affect program risks and costs. In addition, the capabilities of investigators and their partners and subcontractors vary widely. For those organizations with established SR&QA processes and a record of success in space flight, this mission assurance requirements document for Small Explorers will be recognized as considerably reduced from that of the past. For those organizations that do not have established SR&QA processes for space flight hardware, NASA is providing in this document a set of requirements and helpful information to supplement the more general standards of ISO 9001. For those organizations that do not have established SR&QA processes for balloon flight hardware, refer to the Balloon SR & QA appendix to this document which addresses tailoring of the SR&QA requirements for balloon missions. As stated in the Appendix "Guidance for Proposers of Balloon Missions, Regarding Tailoring of the SMEX Safety, Reliability & Quality Assurance (SR&QA) Requirements", it should be noted that Design Review requirements are essentially the same for balloons as for free flyer SMEX missions, but with limited tailoring permitted. Integrated Independent Review Team (IIRT) reviews described in section 3.0 should be included in PI planning for balloon missions.

It is recommended that the Principal Investigator consider all aspects of the mission when developing a comprehensive mission assurance program. The mission assurance program will augment the project team's overall risk management process. A Continuous Risk Management (CRM) methodology must be used that identifies existing or emergent technical and programmatic risks, statuses them in the format established by GSFC management, evaluates mitigation efforts, and retires them or carries residual risks forward.

NASA has instituted the Lessons Learned Information System (LLIS) database for use by all missions. The Program Office will assist PI teams to access, scan, and evaluate existing lessons learned entries for useful guidance during mission development. The PI team will be expected to provide NASA sufficient information to describe new lessons learned for entry into the database.

The overall management effort to plan and invest from the beginning in quality design and problem prevention should not be underestimated, as its value in terms of reducing overall cost has been demonstrated.

It is the responsibility of the Principal Investigator to plan and implement a comprehensive SR&QA program for all flight hardware, software, Ground Support Equipment (GSE), and mission operations. This responsibility extends to all of the Principal Investigator's subcontracts and suppliers. Only limited mission assurance insight is planned by the Explorer Program Office and will be focused primarily on those activities that contribute most to product integrity. Deliverable documentation will be significantly reduced, provided the Principal Investigator maintains an adequate internal record keeping system that provides the necessary traceability for a program of this magnitude. The Explorer Program Office will support and participate with the Principal Investigator in assuring that the SR&QA program being implemented is valid, complete, and effective. The Explorer Program Office is prepared to assist the Principal Investigator in any aspect of mission assurance, and to be the PI's focus for ready and regular access to the Goddard Space Flight Center's mission assurance expertise.

Previous Small Explorer missions have been predominately single string systems, with emphasis on simplicity of design and cost control. Rigorous and disciplined systems engineering, combined with the prevention of problems by using high quality parts and materials and using high standards of workmanship, have allowed a limited reliability and quality assurance program, guarded by the test program, to achieve adequate reliability for a low cost. It is recommended that the Principal Investigator consider similar approaches that envelope all aspects of the mission development. A philosophy based on hurried design and development, followed by an extensive test and repair program, has been shown to be a costly and unreliable approach.

An Insight Agreement between the Principal Investigator and the Explorer Program Office addressing the quality assurance activities, reviews, safety, design assurance and verification system to be implemented will be required prior to the confirmation of the mission.

1.2 Applicability for Missions of Opportunity

Under this AO, PI teams are free to propose investigations that involve missions not funded or managed by OSS. GSFC recognizes that in this circumstance, the actual scope of work performed under these requirements by the PI institution may differ significantly from that of complete and independent PI missions. Therefore, the requirements in this document apply, but only within the work scope that is under direct control of the PI institution. Limited applicability is based on the necessity that host missions maintain their own traditional systems for managing Science, Engineering, Safety, Reliability, & Quality Assurance requirements. Furthermore it is reinforced by the fact that the PI institution will be required by the host to abide by those requirements and to physically and functionally match all provided interfaces. No limited applicability is permitted for system safety, range safety, or personnel safety requirements.

2.0 QUALITY ASSURANCE

2.1 Quality System

During Phase B, the Principal Investigator is to define and implement a quality system that is consistent with the requirements of ANSI/ASQC Q9001-1994. The system is to be documented in a quality manual and/or implementation plan to be submitted to the Explorer Program Office before mission confirmation. The Explorer Program Office will review the quality system and provide the Principal Investigator with an assessment and recommendations.

2.2 Workmanship Standards

Workmanship requirements are a critical part of preventing reliability and quality problems. The Principal Investigator is encouraged to use their own workmanship standards, provided they achieve the workmanship levels described in the following NASA documents:

- NASA-STD-8739.3: Requirements for Soldered Electrical Connections
- NASA-STD-8739.4: Crimping, Interconnecting Cables, Harness, and Wiring
- NHB 5300.4 (3H): Requirements for Crimping and Wire Wrap
- NHB 5300.4 (3I): Requirements for Printed Wiring Boards
- NHB 5300.4 (3J): Requirements for Conformal Coating and Staking of Printed Wiring Boards and Electronic Assemblies
- NHB 5300.4 (3K): Design Requirements for Rigid Printed Wiring Boards and Assemblies
- NHB 5300.4 (3L): Requirements for Electrostatic Discharge Control (Excluding electrically initiated explosive devices)

2.3 Mission assurance Audits and Reporting

Assurance Status Reports will be part of the regular, monthly reporting by the Principal Investigator to the Explorer Program Office and will summarize the status of all assurance activities and report on any discrepancies (including corrective actions) that could affect the performance of the investigation.

During all phases of the mission, NASA must be able to assess the reliability of the mission and understand how the Principal Investigator is resolving problems. In order to do this, the Principal Investigator is required to document and report hardware and software failures to the Explorer Program Office beginning with initial power-up of any flight component or assembly (including critical GSE). Reporting is to continue until successful closure by the Principal Investigator's Failure Review Board (FRB).

In order to ensure that the quality system is working the way it is intended, the Principal Investigator is required to plan and conduct audits of his/her internal mission assurance systems and those of his/her subcontractors and suppliers, examining documentation (processes, procedures, analyses, reports, etc.), operations and products. The Principal Investigator is required to generate and maintain a report for each audit. A summary of all audit findings shall be included in the monthly report.

The work activities and operations of the Principal Investigator's team, including subcontractors and suppliers, may be evaluated, surveyed, or otherwise inspected by designated representatives from the Explorer Program Office, the Government Inspection Agency (GIA), or an independent assurance contractor. The Explorer Program Office may delegate appropriate responsibilities and authority in letters of delegation (LOD). All data, documentation, records, etc. necessary to enable these tasks must be made available upon request by designated representatives.

3.0 REVIEWS

The Principal Investigator must focus resources from the beginning and throughout the mission development phase on engineering working-level reviews (peer reviews) to identify and resolve concerns prior to formal, system level reviews. The Principal Investigator's quality system is to track and close-out all actions items identified during these peer reviews to ensure that issues are resolved promptly at the lowest levels and before system level reviews. A list of action items/closures for each peer review shall be maintained by the Principal Investigator's quality system and made available during system level reviews. Any open action items from any peer reviews must be addressed at the system level reviews.

Peer Review is defined as a detailed independent engineering design review focused at the Subsystem and box level, conducted informally with recognized internal or external experts having current detailed knowledge of the design specialties associated with the item under review. Primary design documentation, such as drawings, schematics, wiring diagrams, and analyses are the review vehicles. Its purpose is to substantiate a detailed understanding of the design’s ability to meet all of its performance and interface requirements, to surface correctable problems early, and to ensure best known practices are used that enhance robustness by avoiding known or predictable problems. Timely, accurate insight, through action item documentation and follow-up activities, is vital to the process. For each review a written record must be kept of time, place, and attendees.

Upon request, the Explorer Program Office will supply technical expertise as required for participation in the areas undergoing peer reviews.

Unlike the many informal engineering peer reviews that are required during the project life cycles, there are two semiformal reviews focusing on requirements and the mission concept. In addition, six formal system level reviews are required to concentrate on 1) critical systems; and 2) end-to-end mission level technical, safety, reliability, flight operations, ground operations, and programmatic issues. If warranted, additional formal reviews may be required for unusually complex areas such as safety and/or flight and ground operations. The following represent the semiformal and formal reviews required under this program:

- Requirements Review (Semiformal)
- Concept Review (Semiformal)
- Preliminary Design Review (Formal)
- Critical Design Review (Formal)
- Pre-Environmental Review (Formal)
- Pre-Ship Review (Formal)
- Operations Readiness Review (Formal)
- Flight Readiness Review (Formal)

Semiformal and formal reviews are to be conducted by an Independent Integrated Review Team (IIRT) panel populated by the GSFC Systems Management Office, NASA approved PI nominees, and independent experts agreed upon by the Explorer Program Office and the Systems Management Office. The Explorer Program Office must be invited to attend all reviews. Copies of the presentation materials must be provided to the Explorer Program Office for information. Formal IIRT reviews are to be chaired by GSFC's Systems Management Office. It is the Principal Investigator's responsibility to address all concerns and action items identified during these reviews.

Included in the above list of formal and semiformal reviews is the Operations Readiness Review (ORR). This review shall be held with GSFC to assess readiness, and to document the final details of the approach agreed to be used for flight operations. The result of this review shall be reported at the Mission Readiness Review. The mission operations agreement reached at the ORR cannot be changed without NASA concurrence.

Independent NASA IIRT reviews now include the previously separate Red Team review activity. A Confirmation Review as described in the AO, will also be conducted.

(Independent balloon mission reviews will be conducted as described in the Balloon SR & QA appendix. A more streamlined design review process is envisioned for balloon missions that are confirmed at significantly lower budget levels and/or which allow multiple flight opportunities. The Explorer Program Office, PI, and Systems Management Office will agree upon Details of such reviews.) These reviews will be coordinated with the Principal Investigator so that they can coincide with other reviews when possible. It is the Principal Investigator's responsibility to address all concerns and action items identified during these reviews.

Red Team reviews, now included within the IIRT construct, have been commissioned for all NASA/GSFC missions in response to NASA/HQ direction to assess across all flight programs the health and thoroughness of institutional internal design review processes. The Red Team is a standing body of technical experts who operate under Center Director authority in accordance with NASA/HQ direction. They utilize standardized criteria to independently and objectively rate overall mission risk level and officially report it to the Center Director via Program Management Council. Results of these reviews are considered a necessary basis for proceeding to launch operations.

4.0 SAFETY

4.1 General

The PI is required to plan and implement a system safety program that identifies and controls hazards to personnel, facilities, support equipment, and the flight system during all stages of the mission development, launch, and operations. The program is to address hazards in the flight hardware, associated software, ground support equipment, and support facilities.

The NASA requirements translate into a series of specific scheduled deliverables, whose nomenclature, relative timing and process flows will differ depending on the selected launch method: Expendable Launch Vehicle (ELV); or the National Space Transportation System (NSTS); or Long Duration Balloons (LDB). Paragraph 4.2 below cites the controlling requirements documentation for ELVs. Paragraph 4.3 cites the requirements that must be met for NSTS launched payloads. These documents are extremely detailed and NASA expects them to be implemented by the PI team to correctly fit each selected mission. To assist PI groups with their system safety cost planning efforts, process descriptions and typical processing flow diagrams, “Expendable Launch Vehicle (ELV) System Safety Milestones and Process Flow” and “National Space Transportation System (NSTS) System Safety Milestones and Process Flow” are available in the Explorer Program Library. Paragraph 4.4 cites the requirements that must be met for National Scientific Balloon Facility (NSBF) launched balloon payloads.

4.2 ELV Payload Requirements

The PI team’s system safety program must meet the system safety requirements stated in the applicable launch range safety regulation. The top level governing documents are: 1)

EWR 127-1, “Eastern and Western Range Safety Requirements”; or 2) RSM-93, “Range Safety Manual for Goddard Space Flight Center/Wallops Flight Facility”.

4.3 NSTS Payload Requirements

The PI team’s system safety program must meet all Space Shuttle safety requirements imposed by the Johnson Space Center for NSTS payloads. The controlling safety documents are (NHB) 1700.7, “Safety Policy and Requirements for Payloads Using the Space Transportation System”; and (KHB) 1700.7, “STS Payload Ground Safety Handbook”. The Space Shuttle Program typically requires 3 safety reviews. Proposers are advised that Space Shuttle safety requirements are particularly strict and may lead to unexpected design changes, additional test or analysis requirements, and associated cost increases. Therefore, higher contingency levels are recommended for Shuttle based missions

4.4 NSBF Requirements

The PI team’s system safety program must meet the system safety requirements stated in documents “NASA Balloon Program National Scientific Balloon Facility Payload Safety Process” and “NASA Balloon Program National Scientific Balloon Facility Ground Safety Plan”.

4.5 Ground Operations Procedure Approval

The PI is additionally required to submit, in accordance with an agreed to schedule, all ground operations procedures to be used at GSFC facilities, other NASA integration facilities, or the launch site, for review and approval by NASA. All hazardous operations, as well as the procedures to control them, are to be identified and highlighted. All launch site procedures are to comply with the applicable launch site safety regulations.

4.6 Documentation Availability

All of the ELV and NSTS safety documents cited in this AO are available in hard copy from GSFC Code 302 at 301-286-6490. . The top level documents governing ELV and NSTS system safety efforts are also available on the world wide web at: “http://arioch.gsfc.nasa.gov/302/safety/passpg.html”. This URL takes the user to the Integrated Safety Information and Requirements System (ISIRS) home page. Any NASA business partner with U.S. citizenship can obtain password access to this library of safety information by following the instructions given at the bottom of the ISIRS page. Balloon safety documents that are cited above in paragraph 4.4 are available in the Explorer Program Library.

5.0 DESIGN ASSURANCE

5.1 Electrical, Electromechanical, and Electronic (EEE) Parts

The Principal Investigator is required to implement an appropriate EEE parts program consistent with the scope of a Small Explorer mission. Previous Small Explorer missions have utilized parts programs that provided early and frequent interaction between the design team and GSFC EEE parts assurance personnel, to ensure reliable EEE parts while at the same time maintaining a cost effective parts program. The Explorer Program Office recommends that the Principal Investigator consider a similar approach with the parts program.

As a guideline, EEE parts should be selected and processed in accordance with the current revision of GSFC 311-INST-001, "Instructions for EEE Parts Selection, Screening, and Qualification", or an internal procedure that meets these standards.

The Principal Investigator is responsible for verifying that any part used in the mission is flight worthy and is not affected by any GIDEP Alert throughout the mission development cycle. In addition to GIDEP, GSFC has regular access to multiple missions' developmental and flight experience with EEE parts and materials. Frequently, NASA management reacts to problems on a particular mission, which are of a potentially global nature by elevating the technical issues to a level of high visibility spanning across all NASA projects. Usually NASA advisories are written to provide up to date advice on such situations, and are provided to all active projects. When NASA management requests that missions evaluate these situations and provide risk assessments with necessary plans of action, the PI institution is required to respond promptly and as fully as necessary to resolve the issue well in advance of completed project milestones that would rule out corrective measures.

5.2 Materials

The Principal Investigator is required to implement a materials and processes control program beginning with the start of Phase B. The Principal Investigator is required to maintain lists and usage records for inorganic and metallic, polymeric, lubricants, and processes. The PI institution shall review all materials lists with an Explorer Project materials expert, and should strongly consider providing printed wiring board coupons to GSFC, or to a GSFC approved laboratory for destructive physical examination screening. Test results are normally obtained prior to population of printed wiring boards with flight parts. For balloon missions, the PI should account for the duration of exposure to thermal environments when qualifying all materials.

5.3 Reliability

Early in the program's preliminary design phase, the Principal Investigator is required to identify specific reliability concerns and the steps being taken to mitigate them. As a minimum, the Principal Investigator is to conduct Failure Modes and Effects Analysis (FMEA) to a sufficient level of detail that mission critical failures are identified and dealt with effectively. IIRT reviewers will expect a demonstrated understanding of failure modes and effects down to the subsystem level of detail. Strong emphasis should be placed on critical single string design features. Appropriate use of the analytical tools and techniques collectively known as Probabilistic Risk Assessment (PRA) will significantly influence NASA's final judgement on the mission's overall reliability. These tools can include combinations of FMEA, Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Event Sequence Diagrams (ESD), Master Logic Diagrams (MLD), or Reliability Block Diagrams (RBD). PRA is a systematic, logical, comprehensive discipline that periodically blends use of these tools to quantify system architecture embedded risk and to maintain a current state of knowledge about risks of failure. Each individual tool provides a graphic representation of a complex thought process, which relates causes to outcomes, either from a deductive or inductive logic reference frame. Used together with a thorough test program and Continuous Risk Management techniques, the selected tools promote situational awareness regarding probabilities of unwanted consequences and the magnitudes of their possible impacts.

It is expected that the Principal Investigator team will accumulate several hundred hours of error-free operation of the integrated spacecraft and instrument(s) prior to the start of environmental testing.

5.4 Contamination

The Principal Investigator is required to plan and implement a contamination control program consistent with the requirements of the mission. The plan must address all aspects of contamination control throughout the mission, including transportation and launch site processing. The contamination control plan must be made available to the Explorer Program Office if requested.

5.5 Software Assurance

For guidance on software assurance related activities, reference the following NASA Standards: NASA-STD-2201-93, Software Assurance Standard, NASA-STD-2100-91, Software Documentation Standard, NASA-STD-2202-93, Software Formal Inspections Standard.

Software assurance is the planned and systematic set of activities that ensures that software lifecycle processes and products conform to requirements, standards, and procedures. The developer shall plan and document software development processes and procedures, software tools, resources, and deliverables throughout the development life cycle in a Software Development Plan. Also, the quality manual or implementation plan

required in section 2.1 must address SQA roles and responsibilities, surveillance activities (i.e., process and product audits), supplier control, records collection, maintenance and retention, and risk management.

The developer shall present software design and development material during the series of IIRT formal design reviews. Engineering reviews (peer reviews) conducted throughout the development lifecycle shall be used to identify and resolve concerns prior to formal, system level reviews. The detailed peer reviews are expected to include such activities as code walkthroughs.

The developer shall develop and implement a documented Software Configuration Management (SCM) system that provides baseline management and control of software requirements, design, source code, data, and documentation. Configuration management practices for software may either be included in the project's overall Configuration Management Plan, or in a separate software CMP. Change control procedures must provide for acceptable visibility to the Explorer's Project Manager.

The developer shall implement a process for Software Problem Reporting and Corrective Action that addresses reporting, analyzing, and correcting software nonconformances throughout the development lifecycle.

Monthly SQA status shall be provided to the Program/Project Office via the existing reporting process. The status reports shall include a blend of current applicable data to provide the following kinds of software assurance highlights:

1. Organization and key personnel changes.
2. Assurance accomplishments and resulting metrics for activities such as, but not limited to, inspection and test, reviews, contractor/subcontractor surveys, and audits.
3. Trends in metrics data (e.g., total number of software problem reports, including the number of problem reports that were opened and closed in that reporting period).
4. Significant problems or issues that could affect cost, schedule and/or performance.
5. Plans for upcoming software assurance activities.

The developer shall conduct a software safety effort integrated with the overall software assurance and systems safety program, which ensures that software safety measures are taken, where needed, to protect personnel and valuable infrastructure from harm caused by incorrect or malfunctioning software.

The developer shall assess the inherent safety risk of the software and develop a tailored approach to address software safety. The developer shall document their approach to the software safety program in the System Safety Implementation Plan developed for the systems safety effort. The developer shall ensure that project specific software safety

requirements are clearly identified, documented, traced and controlled throughout the lifecycle.

The developer can determine and identify software that is safety critical based upon several factors including the allocation of safety critical system level requirements to software, specific software safety requirements levied on the system, and any hazards identified via engineering analyses (PHA, FMEA, FTA, etc).

The developer shall conduct a software reliability management program to optimize the reliability of software through a series of planned activities that emphasize software error prevention, fault detection and removal, and the use of measurements to maximize reliability. The software reliability program can be tailored to the appropriate level based upon criticality of the software to the mission, software safety criticality, as well as project constraints such as resources, schedule and performance. The software reliability management program shall be integrated with the software safety program and risk management program such that software safety critical issues/concerns, as well as risks associated with software, are proactively identified, understood and mitigated to avoid and/or minimize software failures, reference IEEE Standard 982.1-1988 for guidance.

The developer shall provide all information required for the NASA Independent Verification and Validation (IV&V) effort to NASA IV&V personnel. This includes, but is not limited to, access to all software reviews and reports, contractor plans and procedures, software code, software design documentation, and software problem reporting data. Wherever possible, the developer shall permit electronic access to the required information or furnish soft copies of requested information to NASA IV&V personnel.

The developer shall review and assess all NASA IV&V findings and recommendations. The developer shall forward their assessment of these findings and recommendations to NASA IV&V personnel accordingly. The developer shall take necessary corrective action based upon their assessment and notify NASA IV&V personnel of this corrective action. The developer shall also notify NASA IV&V personnel of those instances where they decided not to take corrective action on specific IV&V findings and recommendations. A developer Point of Contract shall be assigned and available to NASA IV&V personnel for questions, clarification, and status meetings, as needed.

Note: The level of IV&V effort and associated programmatics shall be in accordance with the Software Independent Verification and Validation (IV&V) Policy, NPD 8730.4. The GSFC Program/Project Manager shall work jointly with the IV&V Facility to assess the level of IV&V support based on the cost, size, complexity, life span, risk, and consequence of failure. This assessment and the overall project approach to IV&V will be documented in an IV&V project plan. The NASA IV&V facility shall provide IV&V support for software developed for NASA.

The developer shall implement a Verification and Validation (V&V) program to ensure that software being developed or maintained satisfies functional and other requirements at each stage of the development process and that the final product meets customer requirements and expectations. To assist in the verification and validation of software requirements, the developer shall develop and maintain under configuration control a Software Requirements Verification Matrix. This matrix shall document the flow-down of each requirement to the test case and test method used to verify compliance and the test results. The matrix shall be made available to NASA upon request.

6.0 VERIFICATION

The Principal Investigator is required to conduct a verification program to ensure that the spacecraft and instrument(s) meet the specific mission requirements. It is recommended that the Principal Investigator use the Goddard Space Flight Center's General Environmental Verification Specification for STS and ELV Payloads, Subsystems, and Components (GEVS-SE), available from the Explorer Program Office, as a tool and a model to prepare the mission verification plan and specification. Refer to the Balloon SR & QA appendix and the "Long Duration Balloon Opportunities" documents available in the Explorer Program Library to assist with verification planning for LDB missions.

The Principal Investigator is required to prepare and submit adequate verification documentation including a verification matrix, environmental test matrix and verification procedures to the Explorer Program Office for review. The ability to assemble complete test histories from detailed verification records has been proven necessary during recent Red Team activities, and has been shown to be supportive of the PRA process.

7.0 MISSION OPERATIONS REQUIREMENTS

Once GSFC Space Science Enterprise (SSE) missions including PI missions transition to full operations, Code 444, the Space Science Mission Operations Project (SSMO), has project management responsibility and provides oversight of their maintenance and operations.

Although SSMO Project oversight formally occurs after orbital verification is complete and routine operations are underway, the SSMO Project is involved in the various phases of the mission life cycle from the formulation and approval phases through the implementation and evaluation phases to eventual deactivation. SSMO Project involvement is to help assure safe and effective missions from an operations perspective. Benefits of this involvement accrue because the complexity and cost of operations may be dramatically affected by decisions that occur early in the development cycle. There may be trades that can create options for cost reduction by reducing the operational complexity of the mission.

To fulfill its management responsibilities the SSMO Project needs PI Missions to meet the following requirements. These requirements generally flow from the processes defined by the GSFC Quality Management System which is consistent with the ANSI/ASQC Q9001-1994 standard.

Reviews

- Include the SSMO Project in all reviews, formal and semiformal from the Requirements Review to the Flight Readiness Review and the transition to operations Receiving Review.

Configuration Management

- Configuration management shall be provided in the operational phase and shall be consistent with the processes outlined in "SSMO Project Configuration Management Procedures", 444-PG-1410.2.1.

Best Practices

Operational procedures and processes should be consistent with industry best practices. The SSMO Project participates in, and endorses the AIAA Space Operations and Support Technical Committee (SOSTC) efforts to establish industry-wide best practices for satellite operations. While the document is a work in progress (it can be accessed at http://www.aiaa.org/tc/sos/Ops_Best_Practices.PDF), it is a useful tool for the preparation and execution phases of mission operations. The practices identified are/will be consistent with those expected by the SSMO Project and should be addressed in proposals and within the mission operations component of Project reviews.

IT Security Plan

Project plans for Information Technology (IT) systems shall be consistent with "NASA Information Technology Security Guidelines," NPG 2810.x.

Risk Management

- Risk management approaches implemented in the mission development phase shall address risk occurring in the post-launch and operational environments

- Continuous Risk Management, CRM, shall be used during the operational phase and shall be consistent with the processes outlined in "Risk Management", GPG 7120.4. Periodically but at least annually mission risk assessments shall be conducted and the results reported to the SSMO Project.

Anomaly Management

- Anomaly and incident reporting shall be provided in the operational phase and shall follow the process outlined in "SSMO Anomaly and Incident Reporting", 444-PG-5340.2.1

- Anomaly, incident and nonconformance resolution including corrective actions shall be implemented in the operational phase and shall be consistent with the processes outlined in "CONTROL OF NONCONFORMING PRODUCT", GPG 5340.2 and "CORRECTIVE AND PREVENTIVE ACTION", GPG 1710.1.

- The PI mission shall ensure the availability of spacecraft developer support of anomaly resolution efforts during the mission's operational phase.

Records Management

- Mission records shall be defined, accessible and managed in accordance with the process outlined in the "SSMO Records Transfer Plan", 2nd draft, February 20, 2002

- Weekly orbital status summary reports shall be provided to SSMO.

- Quality Management System Effectiveness

- The PI mission shall establish and maintain a qualified mission operations work force as demonstrated by previous flight operations launch experience, training and the completion of certification programs.

- Periodically but at least annually first party audits shall be conducted to assess the effectiveness of the mission's Quality Management System. The results shall be reported to the SSMO Project.

- When required by the SSMO Project the PI mission shall support second party audits.

.

Appendix

Guidance for Proposers of Balloon Missions, Regarding Tailoring of the SMEX Safety, Reliability & Quality Assurance (SR&QA) Requirements

1.0 GENERAL INFORMATION

This appendix is a supplement for guidance in tailoring SMEX Safety, Reliability, and Quality Assurance. Henceforth, for sake of distinction, the "SMEX Safety, Reliability, and Quality Assurance Requirements" document will simply be referred to as the SMEX SR & QA. This appendix will be referred to as the Balloon SR & QA.

It is expected that the Principal Investigator will conform to the SMEX SR & QA document when addressing safety, reliability and quality using specific alternatives addressed in this appendix. The Explorer Program office also anticipates that a considerable amount of mission unique tailoring will be implemented when the SMEX SR & QA Requirements are applied to balloon missions. It is not the purpose of this appendix to levy additional requirements on balloon missions but rather, to ensure those proposals for all types of missions have an equal opportunity to be selected.

It is understood that balloon missions differ significantly from low Earth orbit missions based on the environment and duration of a single flight and also the possibility of reflight. It is further recognized that significant differences will exist in needed environmental verification and qualification testing, as compared to longer duration orbital missions. It is the intent of the Explorer Program Office that SMEX balloon missions will meet an adequate set of documented SR&QA requirements, to augment science derived engineering requirements, therefore increasing the likelihood of success. This will later be used as the baseline for measuring adequacy of the selected investigation's Phase-A effort with respect to mission assurance.

2.0 QUALITY ASSURANCE

2.1 Quality System

During Phase B, the PI must implement a quality system. It is desired, but not required, that this be based on ISO-9001. The system is to be documented in a quality manual and/or implementation plan. This quality system should be based on the flight duration (21 days for LDB flights), the flight environment and number of required re-flights.

2.2 Workmanship Standards

Same as the SMEX SR & QA.

2.3 Mission Assurance Audits and Reporting

Same as the SMEX SR&QA Section 2.3. In addition, program management of NASA's Long Duration Balloon missions is performed by the Balloon Program Office (Code 820) located at the Wallops Flight Facility. Together with the National Scientific Balloon Facility (NSBF), who supports balloon launch and flight operations, the Balloon Program Office oversees certain audit and reporting functions which include but are not limited to:

- Completion of the NSBF LDB Flight Application.
- Establishing concise and achievable flight success criteria.
- Insuring gondola structural certification.
- Insuring thermal compatibility with NSBF flight systems.
- Insuring integration with NASA LDB flight support systems.
- Insuring LDB mission planning that is consistent with established operational and safety guidelines.
- Review of responses to actions assigned from reviews, as described in the following section.

3.0 REVIEWS

Same as the SMEX SR&QA Section 3.0. A test plan is required in the Critical Design Review. Balloon missions could have elaborate re-flight or multiple flight plans. These must be reflected in the test plan.

In addition, the Balloon Program Office will conduct the following independent reviews. These reviews will be coordinated with the PI so that they can coincide with other reviews.

- Mission Initiation Conference (Semiformal) – This review will be conducted after submission of the NSBF LDB Flight Application. It will include the Principle Investigator's team and representatives from the Explorer Program Office, Balloon Program Office and the NSBF. Although the feasibility of each candidate mission's requirements will be reviewed prior to Phase-A, this *Mission Initiation Conference* will focus upon specific flight support requirements for the purpose of insuring assignments and tasks are properly assigned and being worked toward the program schedule requirements.

- Mission Readiness Review (Formal) – This review is conducted immediately after completion of integration and testing of the PI's gondola and instrumentation with the NSBF flight support systems. This is a balloon program review required by NASA HQ prior to shipment to the remote launch site. The purpose of this review is to assess the readiness of the integrated payload (this does not include a review of the merits of the science instrument or other SMEX mandated conformance reviews.) This review will focus upon the readiness and completeness of the science instrument, flight support systems, ground support systems, and Mission & Operations plans. The objective at the time of this review is that all systems be integrated, tested, and definitions / configurations / certifications are complete.

- Flight Readiness Review (Semiformal) – The Balloon Mission & Operations Management conducts this review at the launch site. The purpose of this review is to establish that all pre-

flight readiness preparations are complete and to insure that both science and NSBF support personnel clearly understand the script for the launch, flight, and recovery operations.

- Post Flight Review (Semiformal) – This review is conducted by both the NSBF Mission & Operations Management and by the NASA Balloon Program Office. It will review all phases of the NSBF pre-flight support, launch, flight and recovery operations. Solicitation of PI comments and recommendations are the main focus of this review.

4.0 SAFETY

The PI is required to plan and implement a system safety program that identifies and controls hazards to personnel, facilities, support equipment, and the flight system during all stages of the mission development, launch, and operations. The program is to address hazards in the flight hardware, associated software, ground support equipment, and support facilities.

The PI team's system safety program must meet the system safety requirements stated in documents "NASA Balloon Program National Scientific Balloon Facility Payload Safety Process" and "NASA Balloon Program National Scientific Balloon Facility Ground Safety Plan." Balloon Flight Operations & Mission Safety is managed by the NASA Balloon Program Office, who will insure compliance in accordance with science mission objectives. These safety documents are available from Explorer Program Library.

5.0 DESIGN ASSURANCE

5.1 Electrical, Electromechanical, and Electronic (EEE) Parts

Same as the SMEX SR & QA Section 5.1 with the following revision.

The Principal Investigator is required to implement an appropriate EEE parts program consistent with the proposed balloon mission concept for a Small Explorer mission. A LDB mission will typically be less than 21 days duration; however, the payload could be retrieved, refitted, and re-flown several times. Based on this, high quality commercial / industrial grade parts could be used on a balloon flight provided they are tested, inspected, properly stored and properly handled.

High voltage components must be operated through the entire pressure range, ground to float, to insure arcing does not cause latent damage or permanent failures. All parts should be life tested based on mission duration and pressure, and thermally tested through the entire balloon environment range, ground to float. Balloon systems can potentially impose high static electricity buildup on the balloon and parachute. Balloon electronic support and instrumentation systems must incorporate proper grounding and shielding to mitigate risks associated with potential static discharges.

As a minimum, life cycle thermal testing should verify that all systems will continue to operate for the entire flight duration as bounded by nominal thermal hot and cold cases and thermal cycling. And demonstrate that all systems will recover and operate successfully after undergoing predicted thermal extreme hot and cold cases. Any operational mode that is tailored to

accommodate any thermal operational limitation of the scientific instrument(s) must be indicated in the test plans and operations plans.

5.2 Materials

Same as the SMEX SR&QA Section 5.2.

5.3 Reliability

Same as the SMEX SR&QA Section 5.3 with the following amendments.

Balloon missions are unique in that payloads are normally recovered in such a condition that lends itself toward quick refurbishment and reflight. The Principal Investigator is encouraged to design the payload to survive landing and be capable of re-flight. As with any flight, there is always the risk of damage to the payload to such an extent as to make quick refurbishment impossible. To this extent, the Principle Investigator is encouraged to consider the availability of a backup payload or critical spares. By careful planning and by taking advantage of the multiple flight opportunities that may become available, for some instruments, LDB missions can offer an overall success rate that rivals that of expendable launch vehicles carrying space-rated instrumentation.

Balloon payloads do not experience the acoustics/vibration of a rocket launch and do not need to be designed or tested for these. Instead, LDB mission specific attributes that should be factored into every design are risks of high voltage arcing induced by a residual atmosphere environment, longer thermal dwell times (day / night / earth albedo), and survivability of mechanical shock loads during parachute opening and payload impact at the end of each flight. It is the Principal Investigator's responsibility to test for these.

5.3.1 Test Flight

Principle Investigators are encouraged to fly new balloon borne instruments on a short duration test flight for the purpose of verifying all elements of payload and mission operability. However, a short duration test flight is not a suitable substitute for thermal-vacuum qualification tests. Short test flights cannot be guaranteed to subject the payload to the environmental extremes that are likely to be encountered on a LDB mission.

5.3.2 Thermal Qualification

The Principal Investigator is required to provide a plan for implementing environmental testing that is appropriate to his/her mission. Thermal-vacuum testing must be conducted in such a manner as to demonstrate not only the thermal model, but also to provide system qualification. Thermal qualification testing for balloon missions can be more extreme than that required for ELV or NSTS systems because of the dwell times, albedo, etc. Balloons can be subject to several hours of daylight receiving direct solar and reflected (albedo) radiation. The night time environment can last several hours which includes not only cold sky, but also contribution from cold cloud tops, albedo, etc.

As part of Phase B, the Principle Investigator must provide a detailed thermal analysis. In turn, the NSBF's thermal analyst will use this information to insure close-coupled NSBF flight support systems are operating within proper limits and to insure the PI's instrument is not adversely affected by NSBF support systems. Principle Investigators are advised to schedule the services of a thermal analyst from the beginning through the final design configuration phase in order to be responsive to addressing configuration changes that might arise during the development, fabrication, and integration phases.

Thermal "Worst Case" limits for nominal (operational limits) and maximum (survival limits) for articles exposed to both earth and sky are listed below. These are provided only to lend an appreciation for the possible extreme thermal environment that may be encountered. For example, cloud top temperatures for typhoons can expose the payload to –90C temperatures for a relatively short period. But the nominal cold extreme is –65C. Depending upon the terrain over which the balloon is flying, cold limits for any particular night may be warmer than those listed here. Conversely, high albedo during daytime can expose parts of the payload to +55C. But nominal upper limits are +40C or less. Passive and/or active thermal controls may be required in order to operate under these conditions.

- For articles exposed to external ambient

- Cold Case Temperatures: Operational down to –65C (nighttime)
  Survive down to –90C (2-hour duration)

- Hot Case Temperatures: Operational up to +40C (daytime)
  Survive up to +55C (2-hour duration)

- Unique Cases/Specialty Hardware

- Photo Voltaics (PV) should operate up to +75C and survive up to +90C. Higher ratings for photo voltaics are due to the solar orientation and the color/material absorptivity properties. Designs must account for thermal emissions off the backsides of PV cells. Similarly, any other unique material properties have to be evaluated on a per case basis as the above limits are stated only to provide for general planning consideration and not as absolute limits for all cases.

The balloon payload environment is close-coupled with earth albedo. Because of the wide latitude in payload geometry, attitude control, packaging, coatings, modes of operation, and various thermal control options, balloon payload designs must be tailored based upon each mission's requirements and constraints. For approved LDB missions, the NASA balloon program will assist with providing environmental data, for a particular flight scenario, for use in thermal analysis.

5.3.3 Random Vibration/Shock Tests

In flight, balloon payloads will not experience the vibration levels encountered on ELV or NSTS missions. However, Principle Investigators must provide documentation of test methods and results and/or inspections, practices and records, which clearly demonstrate the mechanical integrity of wiring, circuit boards, and mechanical assemblies. Essentially, this is a "proof of workmanship" verification. Low-level three-axis random vibration testing at sub-system levels may be considered as an acceptable means for verification. However, the Balloon Program Office imposes no standards for vibration testing.

Typically, prior to flight, the most severe mechanical shock loads experienced by balloon payloads are those encountered during shipment, particularly over-the-road. Along with overall payload design considerations, the PI must plan for proper shipping containers that will be accommodated by commercial carriers. Shipping includes over-the-road, sea, and turbo-prop air transport. Handling by NSBF at the launch site is normally a smooth transition from the payload preparation facility to the launch site. However, track-wheel vehicles are a mainstay support vehicle used with NSBF Antarctica flight operations.

At the end of the flight, shock loads associated with parachute opening and payload impact on the ground are the most severe mechanical loads associated with any balloon flight. The NSBF has established mechanical certification criteria, which is available as an appendix to the LDB Flight Application Form that can be obtained off the NSBF web site at http://master.nsbf.nasa.gov/pub/ldb-fy2000.pdf. This requirement stipulates a 10g structural loading requirement at the gondola vertical suspension point and 5g off-axis horizontal loading. Albeit these requirements are established for gondola structures, but when planning for the contingency of a quick turnaround of the payload for possible reflight, designers are advised not to reduce these load requirements when applying how they translate back into their design of internal component shock load integrity for such items as circuit boards, gimbal mountings, cable harnesses, connectors, etc.

5.4 Contamination

Same as the SMEX SR&QA Section 5.4.

5.5 Software

Same as the SMEX SR&QA Section 5.5.

6.0 VERIFICATION

The Principal Investigator is required to conduct a verification program to ensure that the gondola and instrument(s) meet the specific mission requirements.

The Principal Investigator is required to prepare and submit adequate verification documentation including a verification matrix, environmental test matrix and verification procedures to the Explorer Program Office for review.