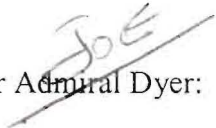


April 6, 2010



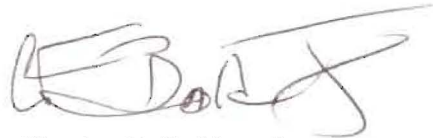
Vice Admiral Joseph W. Dyer, USN (Ret.)  
Chairman  
Aerospace Safety Advisory Panel  
National Aeronautics and Space Administration  
Washington, DC 20546

  
Dear Admiral Dyer:

Enclosed are NASA's responses to Recommendations from the 2009 First, Second, and Fourth Quarterly Meetings of the Aerospace Safety Advisory Panel (ASAP). Please do not hesitate to contact me if the Panel would like further background on the information provided in the enclosures.

I look forward to receiving continued advice from the ASAP that results from your important fact-finding and quarterly meetings.

Sincerely,



Charles F. Bolden, Jr.  
Administrator

6 Enclosures:

1. NASA Response to 2009-01-01b Human Rating Requirements and Engineering Standards
2. NASA Response to 2009-01-03a Risk Management Models and Risk Acceptance
3. NASA Response to 2009-01-03b Risk Management Models and Risk Definitions
4. NASA Response to 2009-01-04 Safety, Reliability, and Mission Assurance Technical Fellows
5. NASA Response to 2009-02-02 Communicating Change
6. NASA Response to 2009-04-02 Center Wide-OSHA Compliance Surveys

**Tracking Number 2009-01-01b**  
**Human Rating Requirements and Engineering Standards**

**Recommendation**

The recently revised HRR standard focuses principally on the process used to reach a human-rating certification. Although it does specify some design requirements (such as fault tolerance and some human factors design standards), it does not include a requirement to implement, tailor, or obtain approval to waive NASA's other engineering design requirements for critical systems. These requirements embody the experience of NASA's best designers and the lessons learned throughout the Agency's vast experience in human spaceflight. These lessons might not be properly applied without such a requirement. To clearly articulate the consistent and comprehensive integration of human safety considerations and mission assurance needs into the integrated design analysis (as required by the HRR), the ASAP recommends that NASA formally establish and stipulate the direct link between the HRR and the applicable NASA standards, such as the NASA-STD-5000 series of engineering directives, as well as relevant technical standards.

**NASA Response**

NASA has implemented a change to paragraph 1.1.2 of NASA Procedural Requirements (NPR) 8705.2B that makes it clear that the human rating process requires tailoring all NASA requirements contained in Agency directives that are categorized as mandatory for all high-priority space systems. The change also makes it clear that human rating includes tailoring of all "mandatory standards" managed by the Office of the Chief Engineer (OCE), the Office of Safety and Mission Assurance (OSMA), and the Office of the Chief Health and Medical Officer (OCHMO). Finally, the revised language clarifies that the Technical Authority may require other NASA, military, voluntary consensus, or industry standards or requirements (beyond the mandatory list) as appropriate to the design concept and mission on a case-by-case basis.

The revised paragraph reads as follows: "1.1.2. The significant monetary investment for complex space hardware requires all missions to meet high standards of public safety, reliability, and mission success. The purpose of this NPR is to define and implement processes, procedures, and requirements necessary to produce human-rated space systems that protect the safety of crew members and passengers on NASA space missions." Human rating further requires implementation of requirements contained in NASA directives that are mandatory for any high-value/high-priority space flight program or project conducted by or for NASA, as well as those standards designated as mandatory by the OCE (<http://nen.nasa.gov/portal/site/llis/standards/>), OSMA (<http://www.hq.nasa.gov/office/codeq/doctree/doctreec.htm>) and the OCHMO ([http://www.nasa.gov/offices/ochmo/policy\\_stds/index.html](http://www.nasa.gov/offices/ochmo/policy_stds/index.html)). In addition, and as part of the human rating process defined in this NPR, Technical Authorities may impose other standards as appropriate to the design concept and its mission on a case-by-case basis. The NPR also

provides a diagram that integrates with other NASA directives to provide direction for the program manager. This action addresses fully the recommendation made by the ASAP. NASA briefed this information to the ASAP on December 21, 2009, and requests that this recommendation be formally closed.

**Tracking Number 2009-01-03a**  
**Risk Management Models and Risk Acceptance**

**Recommendation**

Risk Management Models and Risk Acceptance. In the current Office of Safety and Mission Assurance (OSMA) model, as illustrated in the Constellation Program (CxP), the project manager is the responsible authority for accepting all risks except for the most likely and most catastrophic risk (i.e., in the risk likelihood-consequence matrix, the project manager is responsible for accepting 24 of the 25 categories of risk). Given the integrated nature of this program and other comparably large endeavors, the reasonable conclusion is that the program manager should have a stronger voice in the acceptance of risk at the project level. Moreover, the currently decentralized risk assessment approach offers no ready visibility into the overall risk accumulated by these various projects, which must be integrated at the program level.

The ASAP recommends that the OSMA analyze and emulate the risk management model used by the Exploration Systems Mission Directorate (ESMD), with a particular emphasis on matching the level of risk to be accepted with the level of manager (i.e., project versus program) who must decide whether to accept that risk.

The Panel also recommends that NASA review authority levels in Agency-level policy documents to ensure that authority for medium-level and high-level risk decisions is consistent with the levels of risk involved.

**NASA Response**

NASA has evaluated the recommendation provided by the ASAP and has concluded that the specific suggestions for change that are addressed by ASAP are already contained within NASA policy. No further action is required and NASA considers this closed.

The first suggestion identified within the ASAP's recommendation is that OSMA analyze and emulate the risk model used by ESMD with a particular emphasis on matching the level of risk to be accepted with the level of manager (i.e., project versus program) who must decide whether to accept the risk. This is precisely the model that is contained within NASA Procedural Requirements (NPR) 8000.4A, Agency Risk Management Procedural Requirements. Paragraph 1.2.1 of this NPR contains the key concepts to be applied to risk management within NASA, and subparagraph d. describes the paradigm for matching the level of risk to be accepted with the level of manager who must decide whether to accept the risk or not. The concept, as defined within this paragraph of NPR 8000.4A, is that each organizational level (Agency, mission directorate, program, project, or lower) manages the risks at its own level and oversees the risk management process of the organization(s) at the next lower level. As each level negotiates with the next lower level (the objectives, deliverables, performance measures, baseline performance requirements, resources, and schedules that define the tasks to be performed by the lower level), they also negotiate the predetermined risk thresholds that establish when a risk must be elevated to the next level. The constraints that are established by a program manager to define the

envelope that the project manager(s) must work within, along with the risk thresholds, define the level of risk that can be accepted by that level of manager and what needs to be elevated for acceptance.

The second recommendation is that NASA review the authority levels in Agency-level policy documents to ensure that authority for medium-level and high-level risk decisions are consistent with the levels of risk involved. The model of NPR 8000.4A, described above, incorporates a significant portion of this suggestion. That policy establishes that each level of the organization (Agency, mission directorate, program, project, or lower) defines what level of authority for accepting risk is delegated to a lower level. Each level determines what thresholds to permit the next lower level to accept. There is, however, a check that is applied to that delegation, and that is found within NASA Policy Directive 1000.0, NASA Governance and Strategic Management Handbook. That handbook states, “Decisions related to technical and operational matters involving safety and mission success risk require formal concurrence by the cognizant Technical Authorities (Engineering, Safety and Mission Assurance, and Health and Medical).” These Technical Authorities are established via delegation from the Chief Engineer, the Chief Safety and Mission Assurance, and the Chief Health and Medical Officer to all tiers of the Agency (Agency, mission directorate, program, project), and they have the authority to drive risk decisions to higher levels if they determine that the risk is unacceptable at that level. Additional checks in the form of the Safety Authority and representation by the actual risk taker(s) provides additional checks and balances to ensure that risk is accepted at the proper risk acceptance level.

Finally, NASA must clarify several points made in the text of the recommendation. First, the recommendation indicates that the CxP has assigned the project manager with the responsibility to accept 24 of the 25 categories of risk. The actual CxP implementation of safety risk acceptance is different in that the highest category of risk has been retained at the Agency level, nine have been assigned to the program-level (six directly to the program manager via the Constellation Control Board chaired by the program manager, and three indirectly to the program manager via the Constellation Safety and Engineering Review Panel (CSERP), a program-level-chartered panel, and 15 categories have been assigned to the project-level.

As an additional note, CxP 70038 Revision B, change one, in the Constellation Program Hazard Analyses Methodology, further requires that integrated hazards (those that effect multiple systems or elements) be coordinated with the CSERP with the potential that they are addressed above the project level. This extra step also provides the visibility at the program level to understand the overall risk accumulated by the various projects.



**Tracking Number 2009-01-03b**  
**Risk Management Models and Risk Definitions**

**Recommendation**

The Aerospace Safety Advisory Panel (ASAP) has been pleased to learn in previous reviews that the Constellation Program has established a Top Risk Review risk management matrix that exhibits the characteristics of a modern effective risk management system. This matrix established clearly defined risk levels (carefully specifying both the probability and severity components of risk) and allocated those risks by category, commensurate with overall risk level. Despite these definitions and processes, however, the Panel is concerned that no quality assurance process is in place to assess, and generate data on, whether the matrix actually makes a difference in achieving consistency.

Building on the experience of other agencies, NASA should evaluate whether project and program managers Agency-wide consistently and reliably assign the level of risk for a specified set of examples to the same categories in the risk matrix (e.g., minor, moderate, likely, and so on). This determination then would form the basis for standardizing the definition of these categories so that risk assessments conducted in various NASA Centers can be better incorporated into the risk calculation for the integrated program.

ASAP therefore suggests that NASA measure consistency of performance by devising technical risk examples, supplying them to a cross-section of those personnel who are responsible for deciding where a problem falls on the risk matrix, and evaluating the consistency of their risk matrix category decisions. Without conducting this type of exercise (or some comparable process to demonstrate consistent risk matrix category assignments), NASA will find it difficult to contend that its system for evaluating risk level assignments and decision-making is achieving its performance goal. Furthermore, if the Agency documents inconsistency in risk matrix category decisions, NASA should offer (and develop as necessary) appropriate training materials and tools for the relevant Constellation Program personnel. In addition, if warranted by the evaluation, NASA might need to expand the safety hazard risk matrix to include clear guidance on risk probability and severity definitions, enabling consistent application by all practitioners. ASAP requests that NASA update the Panel at each 2009 quarterly meeting and complete these actions within a year so that the window of opportunity to enhance Constellation Program risk assessments does not close.

**NASA Response**

NASA fully understands the basis for and has evaluated the risk versus reward balance associated with the recommendation provided by the ASAP. NASA has decided not to conduct the risk categorization "test" as recommended.

NASA views the risk matrix as a tool for communication of analysis results, but it does not replace structured risk analysis or risk controls. The results of the analyses themselves and the application of that analytic information to the systems and equipment should be the primary focus of the risk analysis efforts. From the standpoint of risk ranking as a communication tool, an initial ranking might have some variations in application as individuals apply the risk

categorization definitions. However, that initial ranking is subject to numerous reviews at many levels of a program or project via reviews, panels, and boards. The ultimate and beneficial effect of these processes and discussions is that the risks become normalized across the program. These reviews include program personnel, as well as independent reviewers, including the Technical Authorities. We believe that review and Technical Authority vetting is the strength of the process used by NASA for performing human spacecraft development. The ultimate goal of the processes associated with ranking these risks is to ensure a more complete and thorough understanding of the risk. While NASA believes that the definitions applied within the Exploration Systems Mission Directorate, and subsequently through the CxP, are adequate to establish scoring of risks, we also believe that the discussions resulting from differing views related to applying those definitions add to, rather than, diminish the understanding of risk within the program. For these reasons, NASA will not conduct the recommended risk categorization “test.”

**Tracking Number 2009-01-04**  
**Safety, Reliability, and Mission Assurance Technical Fellows**

**ASAP Recommendation**

To raise the level of technical expertise available to the Agency to solve challenging Safety, Reliability, and Mission Assurance (SR&MA) technical and programmatic issues, NASA has worked diligently to establish Technical Fellow positions for the primary SR&MA technical disciplines. The Panel is pleased that NASA allocated appropriate grades to these positions to attract highly qualified candidates, demonstrating the Agency's level of commitment to the SR&MA effort. The Panel was disappointed to learn at this review that NASA currently is not filling these positions because of budgetary constraints.

The ASAP recommends that funding be provided to complete this important step in the process of raising the capability and credibility of the SR&MA discipline at NASA.

**NASA Response**

NASA concurs with this recommendation. The Agency has approved four Safety and Mission Assurance (SMA) Technical Discipline Fellows positions: Systems Safety, Reliability and Maintainability, Quality Engineering, and Software Assurance. The NASA Safety Center (NSC) advertised for, screened applicants (along with the Office of Safety and Mission Assurance Safety and Assurance Requirements Division Director), and recommended candidates for approval to the Chief Safety and Mission Assurance. The initial term of the temporary promotion will be for three years, with two additional one-year options. The successful candidates are to serve as Technical Discipline Fellows and will reside at their host Centers without need to relocate to the NSC. With the concurrence of the Safety and Mission Assurance Directors, NSC has developed a split funding arrangement with the Centers to cover these Scientific and Technical (ST) grade positions and worked with Human Resources to establish and announce the four Safety and Mission Assurance Technical Fellow position vacancies. The four SMA Technical Fellow Positions have now been selected and were approved by the Associate Administrator on November 2, 2009. Effective dates of incumbency for the new Technical Fellows were completed by February 2010. This completes the recommendations made by the ASAP, and NASA requests that this recommendation be formally closed.



**Tracking Number 2009-02-02**  
**Communicating Change**

**Recommendation**

ASAP recommends that NASA be more aggressive and transparent in communicating changes--and the rationale for changes--relating to some areas of the Constellation design and development process. This would prevent NASA's detractors from resorting to using incorrect or incomplete information that puts NASA in a weakened or defensive posture for no technical reason. For example, a significant media miscommunication occurred following NASA's release of information about a change in the number of crew seats on the Orion (a design decision). Media outlets subsequently took this information out of context, resulting in incorrect conclusions being relayed to the public.

**NASA Response**

NASA concurs with the recommendation to clearly communicate areas of change related to the Constellation design and development process and has used various approaches to do so, including media briefings, interviews, and press releases. NASA strives to take a proactive, timely approach to communications to mitigate detractors' use of incorrect or incomplete information. During the design formulation phase of a program, iterative trades and analyses will take place, resulting in internal, pre-decisional data. Although the Agency strives to be proactive and transparent with our communications, it cannot exert complete control over the high-speed tools of the social media. NASA recognizes it is important to communicate key areas of change during the development phase and will make best efforts to communicate in a timely, proactive manner to mitigate misuse of information.

**Tracking Number 2009-04-02**  
**Center Wide-OSHA Compliance Surveys**

**Recommendation**

Finding: The Kennedy Space Center (KSC) is undertaking a center-wide OSHA compliance survey after finding that 50% of the fixed ladders at Launch Complex, 39 were Occupational Safety and Health Administration (OSHA) non-compliant.

Recommendation: The ASAP recommends that NASA Headquarters S&MA assures that other Centers are current in performing OSHA compliance inspections and that there is a sharing of results among the Centers.

Rationale: As part of the Federal Government, NASA is a model workplace and needs to provide a safe work environment for all employees and contractors. Knowing where all Centers are on maintaining compliance with Federal regulations is an important part of the oversight function. The safety findings can also be helpful to NASA leadership in determining priorities for capital expenditures on infrastructure.

**NASA Response**

NASA concurs. No further action is required and NASA considers this closed. The NASA Office of Safety and Mission Assurance (OSMA) policies given in NASA Procedural Requirements (NPR) 8715.1, "NASA Occupational Safety and Health Programs" and NPR 8715.3, "NASA General Safety Program Requirements" require all NASA Centers to implement self evaluation inspections in accordance with 29 Code of Federal Regulations (CFR) 1960, "Basic Program Elements for Federal Employee Occupational Safety and Health Programs and Related Matters to ensure a "safe and healthful workplace" for NASA employees. Annual OSHA audits of each Center are conducted by the Office of the Chief Health and Medical Officer (OCHMO) and coordinated with the Environmental Management Division in the Office of Institutions and Management. As part of these annual OSHA audits, each NASA Center is required to submit an "OSHA Baseline Questionnaire" to the NASA Designated Safety and Health Official (DASHO)." The results of the annual OSHA audit, the baseline questionnaires, and the self evaluations are used to develop the Annual OSHA report. The findings and conclusions of the Annual OSHA report are shared with the NASA community through lessons learned and best practices and during two annual meetings.

The first meeting, coordinated by the OSMA, is the Safety Directors and Occupational Health Managers' meeting. The second meeting, coordinated by OCHMO, is the Annual Occupation Health meeting. Both of these meeting are well attended by representatives from Headquarters, OSMA, OCHMO, and the Center safety, health, and environmental personnel.

In addition, the NASA Safety Center performs Institutional Facility Operational Safety Audits of NASA Centers to ensure that these requirements are being met. The NASA Safety Center provides copies of all reports to all NASA Centers so that the Centers are advised of audit findings, lessons learned and conclusions and, as a heads-up, to look for similar deficiencies.

## **OBJECTIVE QUALITY EVIDENCE from NASA NPR 8715.1 and OSHA 29 CFR 1960**

### **NPR 8715.1 specifically requires the following:**

#### Section 4.1 Frequency of Inspection

4.1.1 NASA Centers or Component Facilities will establish a formal schedule of inspections for all operations/facilities. All active areas and operations of each establishment shall be inspected at least annually ([Requirement 22037 4.1.1\(1\)](#)). More frequent inspections shall be conducted in all establishments where there is an increased risk of accident, injury, or illness due to the nature of the workplace ([Requirement 31562 4.1.1\(2\)](#)).

4.1.2 Any facility, structure, operation, vehicle, or equipment that is in an inactive status must be inspected at least annually ([Requirement 22038 4.1.2\(1\)](#)). Prior to reactivation, the facility, structure, vehicle, operation, or equipment shall undergo a thorough inspection to identify potential hazards ([Requirement 31563 4.1.2\(2\)](#)).

4.1.3 Sufficient unannounced inspections and unannounced followup inspections shall be conducted to ensure the identification and abatement of hazardous conditions ([Requirement 22039](#)).

4.1.4 Special inspections may be conducted at the request of safety and health committees, employees, or their representatives, or upon notice of an unsafe or unhealthful condition.

#### Section 8.2 Center Self-Evaluations

Centers or Component Facilities shall evaluate their safety and health programs and submit the reports in conjunction with the annual OSHA report (see paragraph 7.2.1 of this NPR) ([Requirement 22077 8.2\(1\)](#)). Centers or Component Facilities shall use the OSHA baseline questionnaire, which is based on 29 CFR 1960 requirements, to perform the self evaluations ([Requirement 31615 8.2\(2\)](#)).

#### Section 8.3 Program Evaluation by OSHA/DOL

OSHA is directed by Executive Order 12196, Occupational Safety and Health Programs for Federal Employees, to conduct evaluations of all Federal agency safety and health programs. Any such procedure will be coordinated with the Agency DASHO (or designee) who, in turn, will notify other offices and NASA Centers or Component Facilities, included in the OSHA evaluation.

### **Federal Requirements of 29 CFR 1960**

Executive Order 12196 requires that each agency utilize as inspectors "personnel with equipment and competence to recognize hazards." Inspections shall be conducted by inspectors qualified to recognize and evaluate hazards of the working environment and to suggest general abatement procedures. Safety and health specialists, as defined in section

1960.2(s), with experience and/or up-to-date training in occupational safety and health hazard recognition and evaluation, are considered as meeting the qualifications of safety and health inspectors. For those working environments where there are less complex hazards, such safety and health specializations, as cited above, may not be required, but inspectors in such environments shall have sufficient documented training and/or experience in the safety and health hazards of the workplace involved to recognize and evaluate those particular hazards and to suggest general abatement procedures. All inspection personnel must be provided the equipment necessary to conduct a thorough inspection of the workplace involved. (See 1960.25(a))

All areas and operations of each workplace, including office operations, shall be inspected at least annually. More frequent inspections shall be conducted in all workplaces where there is an increased risk of accident, injury, or illness due to the nature of the work performed. Sufficient unannounced inspections and unannounced follow-up inspections should be conducted by the agency to ensure the identification and abatement of hazardous conditions. (1960.25(c))