NASA AEROSPACE SAFETY ADVISORY PANEL
National Aeronautics and Space Administration
Washington, DC 20546
VADM Joseph W. Dyer USN, (Ret.), Chair

April 7, 2009

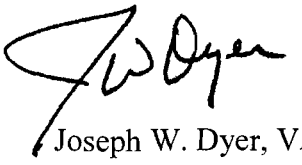
Mr. Christopher Scolese
Acting Administrator
National Aeronautics and Space Administration
Washington, DC 20546

Dear Mr. Scolese:

The Aerospace Safety Advisory Panel held its 2009 First Quarterly Meeting at NASA Headquarters on February 17-18, 2009. We greatly appreciate the support received from NASA subject matter experts.

The Panel submits the enclosed Minutes with Recommendations resulting from this meeting for your consideration.

Sincerely,



Joseph W. Dyer, VADM, USN (Ret.)
Chair

Enclosure

Aerospace Safety Advisory Panel
2009 First Quarterly Report
Minutes and Recommendations

Aerospace Safety Advisory Panel (ASAP)
Public Meeting
February 18, 2009
NASA Headquarters
Washington, DC

ASAP Members Present

- Vice Admiral Joseph W. Dyer, USN (Retired), Chair
- Dr. James P. Bagian
- Major General Charles F. Bolden, Jr., USMC (Retired)
- Mr. John C. Marshall
- Ms. Joyce A. McDevitt, P.E.
- Mr. John C. Frost
- Ms. Deborah Grubbe
- Dr. Don P. McErlean
- Mr. Brock "Randy" Stone

ASAP Staff and Support Personnel Present

- Ms. Katherine Dakon, ASAP Executive Director
- Ms. Susan Burch, ASAP Administrative Officer
- Ms. Sallie Birket Chafer, Reports Editor

Attendees, Public Session

- Mr. Dan Devlin, NASA Office of the Inspector General, Office of Audits
- Mr. Bill Bihner, NASA Space Operations Mission Directorate, Space Shuttle
- Mr. John Marinaro, NASA Safety Center
- Mr. G. Warren Hall, NASA Safety Center
- Mr. Rick Irving, NASA Office of Legislative Affairs
- Ms. Diane Rausch, NASA Office of External Relations, Advisory Committee Management Division
- Ms. Kim Terrell, Katz International Management Solutions (KIMS)

OPENING REMARKS

The Aerospace Safety Advisory Panel (ASAP) held the public session of its 2009 first quarterly meeting at NASA Headquarters in Washington, DC. Admiral Joseph Dyer opened the session by thanking the Headquarters staff for its assistance during the Panel's fact-finding sessions. He noted the Panel's agenda topics, including the Human-Rating Requirements (HRR); Constellation Program implementation of the HRR; update on the Exploration Systems Mission Directorate (ESMD); report on human capital progress; overview of technical excellence; a conversation with Acting Administrator Chris Scolese; the Shuttle, Soyuz, and their interface; and an opportunity to discuss a range of

issues with Mr. Wayne Hale. The Admiral also reported that the Panel successfully completed the required annual ethics briefing.

DEVELOPMENT OF HUMAN-RATING REQUIREMENTS

Admiral Dyer indicated that the ASAP has focused for at least the last three meetings—and to a lesser extent at least one meeting before that—on the HRR. Although this topic has been a difficult one for the Panel to understand in terms of intent, purpose, and direction, he concluded that this meeting significantly clarified the HRR for the ASAP.

As Admiral Dyer described, the HRR represents a significant and substantive shift from a prescriptive approach to one of applying good judgment. Not unlike alpha specifications in the aerospace world, prescriptive standards describe how to do things and are applied fairly rigidly. Although the previous prescriptive technique did limit creativity and did not always produce optimum safety, it did at least provide a checklist, or scorecard, which simplified judging compliance. At the other end of the continuum lies a directive to employ "good judgment," offering less specific direction and guidance. The ASAP sees advantages in both, but while the prior approach provided a clear written record of changes and their justifications, the current approach poses challenges in bookkeeping, accountability, and tracking and communication of those changes as well as establishment of safety performance requirements, in other words, determining how safe is safe enough. As NASA shifts from a how-to specification to a what-is-wanted requirement, the Agency must specify its needs (in this case, level of safety, in a form useful to designers).

The Panel made two relevant recommendations (ASAP 2009-01-01a and 2009-01-01b). First, as Ms. Deb Grubbe noted, for Apollo, Shuttle, International Space Station (ISS), and other programs, NASA has used different approaches to human rating, compiling a significant history and body of knowledge that, if mined, would enhance comparisons of the human-rating approaches of major NASA programs and perhaps inform the future.

Dr. Don McErlean illustrated the value of data mining in a simple example. The Shuttle was designed as a one fault tolerant system with redundancy, while the ISS design uses a full-up two fault tolerant system. The question is whether and how often a two fault tolerant system prevented events that a one fault tolerant system would not avert. It is also important to gather information on the historical record of prior system designs that are included in the failure mode and effects analysis (FMEA) so that the reliability values entered in the FMEA can be traced to whatever degree possible to actual data from similar systems. In that fashion, NASA can assess the validity of the numbers that compose the fundamental FMEA calculations.

Ms. Grubbe agreed, emphasizing that NASA needs to capture near misses, close calls, and other anomalies by reviewing written reports, quantitative assessments, logic trees, and FMEAs to confirm their accuracy—and as needed incorporate organizational learning into the new design. The same issue applies to the Constellation Program.

Second, the Panel recommended a more direct link between the HRR documents and the NASA 5000 directive series. Mr. John Marshall focused on the critical need for a direct link or correlation to the NASA engineering documents to give program managers standard, consistent cross-Agency guidance on performing the integrated safety and

design analysis so that it becomes consistent and comprehensive rather than fundamental and cursory.

Mr. John Frost explained that the NASA 5000 series standards establish the engineering basis for design targets as well as specific safety factors. While the original human-rated policy relied heavily on levels of redundancy as its main safety approach, he concluded that this new HRR wisely focuses less on simple redundancy and more on truly understanding the design and performing risk analyses early, using them to drive the design rather than assessing results afterward, a big improvement. At the same time, with no direct link to the technical standards, the current intention (not explicitly stated in the HRR) can only be assumed to be assessing compliance with the technical standards for each project at some time far down the design process timeline, an approach filled with shortcomings. He suggested that a simple sentence in the HRR standard that ties the two together and makes specific technical standards mandatory unless waived will prevent organizations, internal or external, from assuming that mere compliance with the HRR process is sufficient, when in reality only half the job is done.

Admiral Dyer asked whether the Panel believed that improving the current HRR by linking it to the 5000 documents would make the HRR workable and sufficient. Dr. Jim Bagian responded by turning to the equivalency issue and efforts to use common sense and judgment, but expressed concern about the lack of an explicitly stated benchmark and level of confidence (e.g., about the reliability of the vehicle, mission success, or loss of life). NASA does not now set numbers as a bogey target measure for that equivalence. According to Dr. Bagian, NASA clearly has made a genuine effort and had general success in judging that equivalency without specifying it. However, this approach leaves room for ambiguity, so well-meaning people can make decisions and proceed with actions that are not in concert with activities at other Centers. Mr. Frost added that NASA has relied on program managers to establish those numbers, an approach that could lead to different levels of safety in similar programs. He reported that the Constellation Program numbers look reasonable, but he was concerned that the next program, especially if developed outside of NASA, might vary significantly in its safety goals. Dr. Bagian remarked that the numbers always entail a level of uncertainty, but are not meaningful unless confidence intervals are specified (see recommendation ASAP-2009-01-02a).

Citing a phrase used by Mr. Frost, Admiral Dyer asked, "How much safety is enough?" Unfortunately, the current human-rating documents offer no answer. Mr. Frost observed that the approach is certainly mission-dependent (i.e., it is less safe to go to Mars than to the ISS), but design criteria can still be established for classes of missions. As the Panel observed on several occasions, NASA should let the rising-star program, Constellation in this case, establish the ground rules for programs that follow because most of NASA's effort, money, and brainpower are applied to Constellation. Furthermore, Mr. Frost confirmed that Constellation personnel conducted a lot of good work based on the Exploration Systems Architecture Study (ESAS), past experience, and an understanding of optimizing performance; calculated numbers; and then budgeted them down to the subsystems (per the systems engineering practice). Mr. Frost cited this as a great starting point for defining a group of design target numbers based on the probability of loss of crew.

Synthesizing the Panel's views, Admiral Dyer suggested that NASA could improve the HRR document by supplementing respect for good judgment with a little more specificity (informed by data mining and a knowledge of different methods at different times over different programs). At that point, NASA could test the presumed improvement in light of knowledge gained. Ms. Grubbe noted that such an approach serves as organizational learning because NASA can perform a retrospective on assumptions made during the design of those earlier systems.

Mr. Marshall took a slightly more skeptical view because of this identified lack of specificity. He was struck by the solid reasoning that moving away from stovepipe engineering encourages personnel to keep looking for improvements even if they think they are compliant and that two fault tolerance and redundancy do not always constitute the safest design. Nonetheless, he worried that the HRR is a self-serving change, perhaps overly focused on Constellation needs, that must be managed and monitored very carefully, or it can lead to the wrong processes and to dangerous results. Admiral Dyer summarized that right-hearted people produced the HRR, but it is incomplete and carries its own risks.

Ms. Joyce McDevitt reminded the Panel of its previous HRR-related recommendations, including four from the last meeting that amplify ASAP concerns. She focused on the bookkeeping issue, that is, the need to carefully plan decision documentation because the HRR simply points to common safety and reliability deliverables and other relevant documents that include pertinent information. For example, if an early program strategy or specified level of failure tolerance is superseded by a newly discovered alternative as the design matures, the Panel is concerned about how such changes will be tracked and documented.

Admiral Dyer commented that the old, administratively intensive waiver process generated thousands of hide-bound waivers that did not provide the desired design flexibility, but that weakness could also be viewed as a strength because these waivers were booked, signed, tracked, and accountable. In the current HRR, the weaknesses and strengths have reversed. The HRR is now very flexible, depends on good judgment, and provides greater program management freedom, but has lost crisp tracking and accountability at the individual level. He worried that the current process would require a data-mining exercise to locate all of those decisions (and perhaps even the personnel accountable).

CONSTELLATION IMPLEMENTATION OF HUMAN-RATING REQUIREMENTS

Admiral Dyer confirmed that the ASAP is pleased with the Constellation Program implementation of the HRR, notwithstanding Panel concerns about the HRR process itself.

General Charlie Bolden agreed, citing both kudos and concerns. On the positive side, the best element is the up-front involvement of Constellation safety personnel in the design process. He reported that some NASA veterans recall instances when the analysis and supporting documentation for the Space Shuttle were developed after the design was settled, simply to substantiate existing decisions, but Constellation engineers are incorporating safety in the design phase (specifically in hazard analyses, FMEAs, and

similar analyses) and then integrating them at the program level. The Panel also liked the idea of avoiding the prescriptive, check-the-box mentality. In contrast, the Constellation personnel are trying to understand the requirements; seem to be effectively employing the technical authority governance model, including identifying responsible individuals with go/no-go authority; and are applying heritage processes from earlier programs, from Mercury all the way through the ISS.

General Bolden noted that a major remaining ASAP concern is the residual effects of the zero-based design methodology, which NASA did not adequately define in initial briefings to the Panel. In fact, he declared that today he still does not fully understand the zero-based design because, depending on who is talking, the zero-based design either includes safety considerations or—in line with all of the General's other zero-based design experience—scraps the design down to bare metal and then builds on that. The Panel is concerned because of its lingering feeling that safety had to (or has to) buy its way into the design; this approach is not good safety and mission assurance (SMA) practice. As the flagship program for NASA, Constellation represents an excellent opportunity for the Agency to demonstrate to the world that it can have a successful space exploration program when safety is up front and really means something. The Panel's opinion ebbs and flows about whether the NASA culture fully understands the issue. For example, one presenter commented that once the zero-based design is established, the Agency begins incorporating safety enhancements. As Dr. McErlean appropriately remarked, if it is safety, then it is not an enhancement, it is a necessity. Admiral Dyer described the process as a judgment call of relative comfort about the appropriateness of the task at hand, offering design freedom and program management flexibility, but not crisply answering the question posed.

General Bolden digressed to talk briefly about four overriding themes, specifically (1) foremost, a determination of how safe is safe enough; (2) the timing of NASA involvement in the Commercial Orbital Transportation Services (COTS) Program and in specification of human-rating requirements for COTS vendors, which has not yet been answered (good people are agreeing to disagree); (3) the level of ambiguity in the Constellation risk matrix and the granting of approval authority for hazard reports and risk acceptance to the project level rather than the program level (see recommendation ASAP-2009-01-03a) for one of the largest programs that NASA has ever developed and the first one that the Agency is integrating in decades, an approach that makes the Panel uncomfortable because reason demands that a higher level of approval in the design phase of an integrated project is essential for program oversight and accountability; and (4) the central issue of transparency and clarity when sharing information with the public, particularly the capability to comprehensibly describe the significant risk associated with space exploration.

Acknowledging that General Bolden raised an important point, Admiral Dyer commented that the ASAP would recommend almost a new communications genesis. The ASAP suggested that the new Administration and the in-bound Administrator take time to consider a new approach that would explain not only the level and range of risk associated with space exploration, but also the importance of the work, the reward that justifies the risk, and the acceptance of that risk by willing and knowledgeable astronauts. The public discourse thus would be more direct and clearer, with less interpretation

required. General Bolden agreed, contending that American citizens can handle difficult issues, so NASA should quit treating them as if they are children who do not understand, instead bringing them in as partners.

Dr. Bagian emphasized the need for a more complete definition of risk and safety in the dialogue with the public. When NASA or the ASAP says "safe," the analogy is not taking the elevator to the lobby to get lunch; in reality, the appropriate analog is being shot out of a cannon, base jumping, or worse. Dr. Bagian suggested that perhaps NASA should not even use the word "safe," but should talk instead in terms of the risk that NASA has decided to take because of the potential benefits. Dr. McErlean stressed that nothing about this process is safe in the lexicon of the common man doing everyday activities—nothing is even close. He suggested a transition to "controllable risk" that NASA is mitigating in every way possible because the rewards of exploring and using space are more than sufficient payback for the skilled professionals who knowingly take such risks. Ms. Grubbe observed that the challenge is to articulate the risk so that each respective audience (e.g., appropriators, program managers, the public) understands it and can identify actions that affect that risk. Dr. McErlean rephrased the issue as NASA striving to drive risk down to the level that lowering it any further would require not flying—but that is still a long way from the risk associated with taking the elevator.

Ms. Grubbe warned that managers often take numbers as gospel and do not necessarily understand that such numbers are nothing more than sophisticated guesses. General Bolden deemed that a good segue to the risk analysis process described by NASA, which is quite promising, but the Panel concluded that if NASA more effectively, aggressively, and rigorously mined risk data from previous programs, it would detect facts and events that substantiate current risk analyses and subsequent guesses. He described NASA's approach as a paper program, with numerous up-front hazard analyses and FMEAs that are based on substantial speculation. The ASAP concludes that NASA can better substantiate and validate the analyses underlying such risk decisions by more effectively mining data from past programs and providing valid information to support the Agency's risk-informed decision-making process (see recommendation ASAP 2009-01-02b).

General Bolden reiterated that the Office of Safety and Mission Assurance (OSMA) HRR is neither the integrated picture that the program manager and Administrator should consider, nor the integrated requirements that a customer or vendor building a human-rated spacecraft needs. He stressed that engineering requirements (e.g., the NASA 5000 specifications and some MIL-SPECs still in use) constitute an integral and vital part of the process. Consequently, the Panel suggests that NASA should be more explicit in specifying the engineering requirements and standards that drive human-rated vehicles.

General Bolden affirmed that the Constellation Safety and Engineering Review Process (CSERP) is a great idea, but loses effectiveness when NASA establishes two. The CSERP is supposed to be **the** safety and engineering panel that approves all work, gives the green light to fly, and notifies the program manager and the Administrator. General Bolden contended that establishing two CSERPs at the two NASA Centers with the longest history of competition (Johnson Space Center and Marshall Space Flight Center) is untenable. Dr. McErlean agreed, stating that NASA has not adequately considered interfaces (i.e., one panel cannot allow for risks that the other panel already has accepted, despite crossover effects). He emphasized that this is an integrated project, so NASA

needs an integrated assessment, but instead is bifurcating the overriding philosophy of integrated risk-based design. General Bolden noted that each CSERP is at the project level, but NASA is the program integrator, so it requires a program-level CSERP with a chair who, at absolute minimum, works for the program versus two chairs working for two different projects (see recommendation ASAP-2009-01-02c). Mr. Frost cited a historical example to illustrate the problem: Foam dislodged from an external tank is not a hazard to the tank; the orbiter has no foam on it, so foam failure is not an issue for it; however, an integrated analysis of both reveals the obvious problem.

OVERVIEW OF THE EXPLORATION SYSTEMS MISSION DIRECTORATE

Mr. Frost described the briefing from the ESMD Associate Administrator as a good news story in almost all aspects; ESMD is bending metal, making fire and smoke, and planning for the future. He highlighted a few ESMD successes, including completing the Ares I Preliminary Design Review (PDR) last September, the Orion baseline review, and a number of program starts and milestones. ESMD is still committed to the March 2015 initial operating capability milestone and has undertaken major reviews for the Ares I-X, addressing ground operations, mission operations, and extravehicular activity (EVA) systems. ESMD monitors COTS milestones, and SpaceX recently successfully completed several reviews. ESMD also has started or completed construction of numerous facilities.

As Mr. Frost noted, ESMD expects a bigger year in 2009, including the pad abort test and Ares I-X test, which will show real progress to the American taxpayer. ESMD is working the three main issues properly identified at the PDR, specifically (1) liftoff clearance (the issue of whether the wind can blow the vehicle into the tower), which NASA plans to handle by vectoring nozzles or changing wind ground launch rules; (2) thrust oscillation, which NASA is addressing through a major effort, including making firm decisions to control oscillation on the launch vehicle and conducting crew tests to validate the vibration requirements (although the Panel would like to see more work in that area); and (3) inadvertent contact between the first and upper stages, an engineering problem that NASA identified through its analysis techniques and certainly can solve, preventing it from ever occurring during a test flight (at least one commercial COTS flight failed because of such inadvertent contact).

Mr. Frost concluded that ESMD implemented a number of architecture changes to reach a successful PDR, and the Directorate is still correcting and nudging the design to optimize it. He observed that micrometeoroid and orbital debris (MMOD) still constitutes the leading risk to ISS and Shuttle missions and that this issue will receive increasing attention in the years to come as the quantity of debris multiplies.

Dr. Bagian revisited the thrust oscillation issue, noting that NASA, displaying an abundance of caution, has changed the design to add two mass dampers to mitigate the vibrations from a crew standpoint. Although the Orion PDR is not until the end of the year, NASA should acquire (and slowly is capturing) additional test information to better understand the need for mitigation. Dr. Bagian suggested that Ares and Orion jointly collect such data, sooner rather than later because the data might show no effect on crew

health or performance, so NASA would not need a design change and mass dampers at all.

Mr. Frost described the briefing on the NASA program top risk list and procedures for managing cost, schedule, safety, and performance risks. He commented approvingly that this approach has all of the characteristics of modern risk management systems, including clear delineations of designated decision-makers and lucid definitions of risk levels. He noted with concern, as did General Bolden, that the CSERPs use a different matrix, even though they deal with safety issues that feed the program top-level risks. Moreover, as General Bolden pointed out, the matrix apparently assigns risk acceptance responsibilities for relatively high levels of risk to relatively low-level managers, much lower than the norm. Mr. Frost stressed that it is missing one of the main attributes of a useful risk matrix that can be applied consistently, namely how to tell where a risk sits on the matrix in terms of either numbers or a good narrative description of probabilities and severities; he noted that NASA can handle the severities, but the probabilities need work.

To avoid needless arguments (and wasted time) over defining a moderate or low probability—versus focusing on solving the problem—Mr. Frost suggested aligning the CSERP matrix more closely with the top-level risk matrix, which makes sense from a reporting standpoint and is particularly important as the basis of all other projects. He also recommended that NASA review MIL-STD 882, which could offer useful on-point guidance. Ms. McDevitt cautioned that the latest draft of MIL-STD 882 embodies a change in the whole philosophy of risk management to apply not to the life of the system, as it had for decades, but rather to the next 12 months. Although the new draft maintains a numerical threshold between each of the levels of likelihood of occurrence, this version expresses that risk over the next 12 months. Mr. Frost responded that the most common risk assessment error is not establishing the period of exposure time (i.e., parsing a risk down to a per-minute basis makes it sound acceptable).

Focusing on the matrix definitions of risk, Dr. Bagian suggested that after the definitions are refined (or even now), a natural follow-on would be conducting a reality check at different NASA Centers and projects by posing a technical situation, asking managers where it lies on the matrix, and comparing their results to determine whether the definitions are sufficiently clear to produce consistency. With various entities making same-time decisions, such a reality check is necessary and simple (see recommendation ASAP-2009-01-03b).

Ms. Grubbe contended that the risk lists are very good, but deal entirely with hardware, ignoring people and softer aspects. For example, such matrices could include measures of whether NASA is effectively communicating the right information. As another example, losing the NASA brain trust in one fell swoop (e.g., on the same ill-fated airplane) is not even on the matrix. From a people standpoint, the matrix needs review.

Mr. Frost observed that the COTS program is quite active; work and labor requirements are proceeding for transporting cargo to the ISS, and NASA is managing the safety implications of COTS vehicles contacting the ISS. Orbital Sciences Corporation and SpaceX are both heavily involved, bringing different approaches and skills to the table. In addition, as Mr. Frost and the Space Operations Mission Directorate (SOMD) briefing

indicated, NASA can learn new ways of doing business from COTS firms (although the downside of unsafe commercial procedures still must be monitored).

Mr. Frost also complimented NASA on its systems integration work. Although NASA has not served as the systems integrator for a major program for a long time, the Panel reported that NASA personnel not only are doing the job well, but also are learning and regaining systems integration skills. Ares I is coming together, so the pieces are fitting.

HUMAN CAPITAL UPDATE

Ms. Grubbe summarized the briefing from the Office of Human Capital Management, which has made good progress since its last presentation to the ASAP a year ago. For example, NASA has created one information technology system from the previous myriad of systems, thereby supporting future NASA needs by providing more accurate and readily available data. The team and management architecture that have been in place for a year to 18 months appear to be suited to the current task, although Ms. Grubbe indicated that the sophistication, currency, and necessity of the work should be monitored over time. She observed that NASA is managing immediate personnel needs by making good use of available tools such as term employment, career development, retraining, transition programs, and incentives.

The Agency also is emphasizing multigenerational workforce efforts so that Gen Y employees who join NASA feel as if they are more a part of the organization and the process. Ms. Grubbe noted that many employers now face this issue because young job candidates possess a totally different set of skills and therefore process information in different ways. However, she was heartened to hear that every NASA Center has initiated projects (e.g., cyber cafes) to open up the culture and increase communication.

Ms. Grubbe suggested that the Panel should continue monitoring these efforts and asked the Human Capital Management team to deliver a more detailed analysis, including information on identified skill sets and number of personnel who possess such skills. Some of this information is available, so NASA could apply a team approach (including leaders from major programs) to identify changing elements and how they are managed. She cited this strategy as a possible future recommendation because Headquarters-level personnel probably should not be asked to drill down to that level of detail.

Dr. McErlean added two thoughts. First, he noted that although the human capital briefing explained the Agency's successful changes in the recruiting process and the new-employee process—which are enabling NASA to gain better traction and attract new workers—it did not include an assessment of the process for comparing current and new workforce skills against needs identified by major programs such as Constellation (an evaluation similar to those performed for any acquisition). Expressing his certainty that the information is available, Dr. McErlean asked to see it in the future. Second, he addressed the Panel's small concern that NASA is placing a very heavy emphasis on recruiting from cooperative (co-op) programs. Although that can be an advantage, NASA still must be sufficiently open to acquiring the best available talent that it does not overlook an opportunity to hire a college graduate not in a co-op program. Moreover, the Agency must remain open and available to all college students, avoiding the **appearance** of focusing on co-op students to the exclusion of other recruits. Ms. Grubbe commented

that if the Panel wanted to make a recommendation, it should ask NASA to exert pressure on the Federal system regarding the recruitment of co-op, intern, and college students.

Dr. McErlean raised a question about the Federal Web site process and its relative user friendliness. Although the Web site is designed to offer young people an opportunity to apply for available jobs, the Agency should investigate whether the process is so difficult that students give up, thinking that NASA obviously is not interested.

OVERVIEW OF THE TECHNICAL EXCELLENCE PROGRAM

Dr. McErlean reviewed the briefing from the NASA Safety Center (NSC) and the Technical Excellence Office, which encompassed a couple of prior Panel recommendations. He confirmed that the ASAP views OSMA and SMA as an extraordinarily important skill set in the workforce, serving a vital function in properly addressing SMA in large, complicated programs.

Dr. McErlean summarized two ASAP observations. First, the Panel has suggested raising the "prestige" level of service in this organization so that NASA employees identified as future leaders will tend to process through OSMA. Such assignments will enable future leaders to acquire what the ASAP views as an absolutely essential skill set for their portfolios as they move up the leadership chain.

Dr. McErlean reported that the NSC is making important progress and has established four Technical Fellow (ST) positions, but currently has not filled the jobs (despite its best efforts), apparently because of budget issues. The ASAP is concerned because it has concluded that the Technical Fellows will be role models for other employees who aspire to high-level careers that require these skill sets. The Panel recognizes the importance of these four Technical Fellows and looks forward to seeing the positions filled (see recommendation ASAP 2009-01-04).

Ms. McDevitt suggested the possibility of hiring one full-time Technical Fellow—or one who is assigned part-time to a project or Center-related activity—to demonstrate the benefit of such support. She emphasized that NASA had worked very hard to create these positions and obtain an ST grade level, so the opportunity should not be lost. Dr. McErlean agreed, noting that establishing these four jobs sent the message to management that this is an important capability, but allowing the Technical Fellow positions to remain unfilled sends another, not-so-positive message. Mr. Frost suggested that the Technical Fellows should be treated like a safety-critical Shuttle or ISS subsystem, not just a nicety. As he observed, if NASA keeps doing what it always did, it is going to get what it always got. One of the main changes that NASA can make is to mobilize and exploit the Agency's extensive brainpower. Mr. Frost therefore characterized the Technical Fellows as critical safety positions that ought to be funded and filled immediately and noted that the required funding is small compared to the potential advantages.

Second, the Panel supports NASA in fostering a broader understanding across the total workforce of OSMA functions and their implementation. Dr. McErlean reported that the Technical Excellence Office is instituting a broad-based, multilevel education and training program that drills down into specific competencies (e.g., quality assurance). He suggested that Center directors should encourage personnel to take such training

courses—like the Defense Acquisition Workforce Improvement Act training in the Department of Defense–to raise their competencies in these areas. The Technical Excellence Office is currently assembling courseware packages, launching Internet access, and beginning beta testing. The Panel looks forward to reviewing the results of this promising, apparently robust program. Moreover, as Dr. McErlean observed, the work that NSC is performing should serve as a solid platform for launching such education and training activities.

Ms. Grubbe noted that it is incumbent on the NSC to engage with program personnel to identify their needs and then work backward to essential capabilities and competencies to ensure that the coursework fully matches and delivers the necessary skills. Ms. McDevitt cited this process as an opportunity for the NSC to communicate with human capital workforce personnel to identify the types, meaningfulness, and value of already available data (including defined SMA skill sets), rather than reinventing the wheel by automatically performing its own surveys.

Dr. McErlean indicated that the Panel encourages the NSC to conduct appropriate follow-ups and avoid the throw-it-over-the-transom approach. He confirmed that the NSC is off to a great start and using the right approach, but stressed that the NSC must be engaged with recipients of its services, monitor the match between services and needs, identify potential improvements, and track whether employees are taking the courses, whether the courses serve stated purposes, and whether students acquire targeted knowledge.

UPDATE FROM THE ACTING ADMINISTRATOR

Mr. Marshall declared that, on behalf of all ASAP members, it always is a pleasure to have the opportunity to share thoughts and ideas with NASA Acting Administrator Chris Scolese. Mr. Marshall further noted that the Panel has great confidence in his ability to manage NASA during the interim term and to do an excellent job of ensuring continuity for the next Administrator. Admiral Dyer reaffirmed the high regard that the ASAP has for Mr. Scolese, concluding that the Panel is confident in NASA's technical leadership at the highest levels after discussions with both Mr. Scolese and Mr. Bill Gerstenmaier.

Mr. Marshall reported that Mr. Scolese expressed his appreciation for the support of the new Administration. The ASAP and Mr. Scolese discussed the Shuttle and the future direction of space exploration, which the new Administration still must specify, preferably sooner rather than later because of the significant implications of any change. In the meantime, NASA is pursuing the currently legislatively approved mandate.

The Panel and Mr. Scolese conversed about the COTS program, a central theme of many discussions at this quarterly meeting. The ASAP and Mr. Scolese also revisited the issue of an optimum mix of human and robotic missions. Mr. Marshall noted that Mr. Scolese echoed the need for the Agency to focus more on this issue and expand the concept, perhaps using an alternative or equivalent levels of safety.

Mr. Marshall mentioned two other discussion topics. First, the Panel and Mr. Scolese addressed the recent collision of two satellites. The ASAP generally concludes that NASA does not hold responsibility for monitoring potential collisions and notifying commercial firms. Second, the ASAP and Mr. Scolese discussed the significance of the International Traffic in Arms Regulations (ITAR) and its implications for the Agency,

agreeing that this issue continues to inhibit NASA from fulfilling certain Agency roles and that additional relief from some ITAR provisions is required from the Congress.

SHUTTLE AND SOYUZ RISK ASSESSMENT

Mr. Randy Stone summarized the briefing by the Associate Administrator of the SOMD on the relative risk of flying astronauts on the Shuttle versus the Soyuz. Clearly the Agency has made a long-running decision that the Soyuz is sufficiently safe to fly U.S. crews and to serve as the ISS lifeboat. However, the Soyuz suffered a couple of failures recently when a pyrotechnic system failed to successfully jettison part of the deorbit package, resulting in a fairly rough ride to the ground. Consequently, the ASAP posed a question about NASA's confidence level (from a safety perspective) that the Soyuz will continue to be a safe vehicle for transporting U.S. astronauts to and from the ISS after the Shuttle is retired.

Mr. Stone praised the SOMD analysis. A very different vehicle than the Space Shuttle, the Soyuz is relatively very simple, very structurally robust, and a one-time vehicle (which, by virtue of the single-use airframe, adds a certain degree of robustness). The Soyuz has been a very reliable vehicle, launching on time two to three times annually for a surprisingly long 40 years. Moreover, the Soyuz capsule uses essentially the same launcher as the Progress cargo vehicle, bolstering the 40-year Soyuz record. Any changes are tested first on the cargo module (versus the human module) to gain engineering confidence that the changes are acceptable. If such a pyrotechnic failure occurs again, the Russians have redesigned the system so that its attitude allows the thermal properties of reentry to quickly sever the deorbit package, allowing the vehicle to stabilize.

Mr. Stone stated that NASA does not have nearly as much analytical information on the Soyuz as on the Shuttle, so NASA clearly must review Soyuz performance after every flight, making the same types of judgments about reliability as it does for U.S. spacecraft and adding to the historical record on the vehicle.

Because of the extremely long and successful operational history of the Russian vehicle, the ASAP has concluded that NASA has a good understanding of Soyuz safety and that the processes necessary to maintain its reliability are in place. Admiral Dyer agreed that, from a safety perspective, the Soyuz has the capability to bridge the gap between the end of the Shuttle Program and the availability of Ares and Constellation for transport.

Mr. Stone reported that the Panel asked the SOMD Associate Administrator about the recent unfortunate impact of an operational private U.S. satellite and a decommissioned Russian satellite. The collision produced a fairly large debris field, now orbiting the Earth. Mr. Stone observed that this debris field is not orbiting in the same plane as the ISS, but rather at a cross plane—not necessarily where the ISS is, but in that orbital attitude. Consequently, NASA will increase its vigilance during this time frame, and flight teams will move the ISS if required. Mr. Stone expressed confidence that the Agency can successfully manage this risk.

TRANSITION

Mr. Stone noted that the ASAP always is pleased to talk to Mr. N. Wayne Hale, Jr. Currently the Deputy Associate Administrator of Strategic Partnerships, Mr. Hale has performed many different jobs at NASA and is a trusted voice in the program. Consistent with one of the Panel traditions when conversing with someone who is influential in the program, the Panel asked Mr. Hale what keeps him up at night. Mr. Stone summarized Mr. Hale's thoughtful answer: the momentum-disrupting, potentially significant effects of a major change in Agency direction on the NASA workforce and on cost.

The Panel and Mr. Hale discussed the one outstanding decision that must be made fairly quickly, whether to extend the operational life of the Shuttle. Mr. Stone explained that if the Shuttle program is extended significantly—not just for a few missions—Mr. Hale would worry about lost opportunities over the last 5 years to make a number of Shuttle improvements that would inherently enhance safety and provide greater safety margins, but were rejected because they could not be developed and integrated before the scheduled retirement of the Shuttle fleet at the end of 2010.

Admiral Dyer addressed COTS development of commercial space delivery vehicles, which is focused initially on cargo, and NASA is ensuring freedom of design by taking a hands-off approach. However, the COTS companies, some members of Congress, and other observers contend such vehicles could eventually become human capable. The ASAP is concerned that NASA's hands-off stance has created a potential future capabilities mismatch because COTS firms might make innocent, good-faith design decisions that ultimately preclude future human-rated transport for NASA. Such an outcome would not benefit either the company or NASA, but rather would give the appearance of poor planning and might force NASA to make a time-constrained decision based on duress rather than sound analysis.

Dr. Bagian linked this issue to previous discussions on accepting and quantifying different risks for different operations. To avoid a (potentially) politically untenable position and a technically unfavorable one, in the next few months, NASA should determine the level of risk that the Administrator will accept and communicate that risk to all COTS firms—not instructing them how to get there (a persuasive point about equivalence made by Mr. Bryan O'Conner and others) and not specifying adherence to NASA 5000 series standards—but rather identifying an equivalence level, similar to the approach used in the U.S.-Russia working relationship.

Mr. Marshall cited two resulting dilemmas, specifically (1) NASA does not know what the equivalent level of safety is, does not know that number and how to communicate it, and (2) no one wants to impede current COTS progress and capabilities while adding cost to the current program and associated requirements. As Mr. Marshall noted, the Agency must start that dialogue regardless of the lack of current contractual agreements, and the Panel's consensus is preferably sooner rather than later.

ASAP RECOMMENDATIONS, FIRST QUARTER, 2009

2009-01-01: Human Rating Requirements (HRR)

2009-01-01a. Human-Rating Requirements (HRR) and Data Mining. The ASAP recommends that NASA rigorously research, compare, and contrast the different human-rating approaches used during the Apollo, Shuttle, International Space Station, and other programs. NASA should take advantage of this significant history and body of knowledge not only to assess the validity of the assumptions used in the new hazard analysis (HA) and in failure mode and effects analyses (FMEAs), but also to evaluate the benefits that the various approaches yield in terms of safety and mission assurance, which enhance future HRR modifications.

2009-01-01b. Human-Rating Requirements (HRR) and Engineering Standards. 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.

2009-01-02: Constellation Program Implementation of HRR

2009-01-02a. Constellation Program Implementation of Human-Rating Requirements (HRR) and Design Safety. The recently revised HRR standard represents a fundamental shift from telling developers how to create a safe design (by relying primarily on redundancy) to establishing a process for using a risk-informed design approach to produce a design that is optimally and sufficiently safe. The ASAP applauds switching to such a performance-based approach because it emphasizes early risk identification to guide design, thus enabling creative design approaches that might be more efficient, safer, or both.

However, this approach is viable only if a common understanding of "sufficiently safe" exists, and the current HRR procedures leave that determination to individual programs, which could lead to inconsistent "safe-enough" thresholds among various developers if not carefully managed. This consequence could be especially problematic for development (and possible future use by NASA) of potential future human-rated vehicles produced by organizations external to NASA, such as Commercial Orbital Transportation System (COTS) firms or the programs of other nations.

The ASAP recommends that NASA stipulate directly the HRR acceptable risk levels—including confidence intervals for the various categories of activities (e.g., cargo flights, human flights)—to guide managers and engineers in evaluating "how safe is safe

enough." These risk values should then be shared with other organizations that might be considering the creation of human-rated transport systems so that they are aware of the criteria to be applied when transporting NASA personnel in space. Existing thresholds that the Constellation Program has established for various types of missions might serve as a starting point for such criteria.

2009-01-02b. Constellation Program (CxP) Implementation of Human-Rating Requirements and Data Mining. To strengthen the risk analysis processes that the CxP uses, the ASAP strongly recommends that the program apply a data mining methodology that captures failures, near misses, and other anomalies in hardware and software from other NASA programs (i.e., Mercury through the Space Shuttle and the International Space Station, including expendable launch vehicles). In addition, this methodology should identify personnel issues that positively or negatively affected these previous problems.

2009-01-02c. Constellation Program (CxP) Implementation of Human-Rating Requirements and the Constellation Safety and Engineering Review Panel (CSERP). According to Constellation Program Management (CxPM) Directive No. 013, the CSERP is chartered to provide CxP with an independent review of technical activities and products associated with safety technical risk. Implicit in this directive is a charge to the CSERP to ensure the completion of integrated risk analysis processes, which is a program-level function. The ASAP recommends making one of two modifications to the CSERP organization and review process, specifically (1) elevate the CSERP to a program-level panel or board with the responsibility and authority to review and approve all integrated risks or (2) direct that all hazard reports approved by the CSERP must be forwarded to the Constellation Program Control Board for additional integrated risk analysis and approval.

2009-01-03: Risk Management Models

2009-01-03a. Risk Management Models and Risk Acceptance. In the current Office of Safety and Mission Assurance (OSMA) model, as illustrated in the Constellation Program, 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, 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.

2009-01-03b. Risk Management Models and Risk Definitions. The Panel 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.

The 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. The 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.

2009-01-04: SR&MA Technical Fellows

2009-01-04. Safety, Reliability, and Mission Assurance (SR&MA) Technical Fellows. To raise the level of technical expertise available to the Agency to solve challenging 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.