

HOLD FOR RELEASE  
UNTIL PRESENTED  
BY WITNESS  
December 2, 2009

**Statement of  
Bryan O'Connor  
Chief, Office of Safety and Mission Assurance  
National Aeronautics and Space Administration**

**before the**

**Subcommittee on Space and Aeronautics  
Committee on Science and Technology  
U.S. House of Representatives**

Chairwoman Giffords and other Members of the Subcommittee, thank you for the opportunity to appear today to discuss how NASA works to ensure the safety of human spaceflight. In your letter inviting me to testify at today's hearing, you asked that I address a number of questions related to the Office of Safety and Mission Assurance and the safety of human spaceflight at NASA. My statement will address those questions, and provide additional context.

**The Role of OSMA in Ensuring Human Spaceflight Safety**

The NASA Office of Safety and Mission Assurance provides policy direction, functional oversight, and assessment for all Agency safety, reliability, maintainability, and quality engineering and assurance activities and serves as a principal advisory resource for the Administrator and other senior officials on matters pertaining to human spaceflight safety and mission success. As Chief of the Office of Safety and Mission Assurance, I report directly to the Administrator. OSMA supports the activities of -- but is organizationally separate from -- the human spaceflight Mission Directorates and the Office of the Chief Engineer, thus providing the Administrator an independent view of the safety and effectiveness of human spaceflight designs, flight test and mission operations in addition to all other mission roles of the Agency.

Specifically, the Office of Safety and Mission Assurance:

- Develops strategies, policies, technical requirements, standards, and guidelines for system safety, reliability, maintainability, and quality engineering and assurance;
- Establishes the applicable set of Safety and Mission Assurance (SMA) requirements for all human spaceflight programs, and, through delegated technical authority, formally approves or disapproves waivers, deviations and/or exceptions to same;
- Verifies the effectiveness of safety and mission assurance requirements, activities, and processes, and updates, cancels or changes them as time, technology and/or circumstances dictate;
- Advises NASA leadership on significant safety and mission assurance issues, including investigation of human spaceflight-related mishaps and close calls, and provides guidance for

- corrective actions stemming from those investigations as well as corrective actions related to ground and flight test anomalies;
- Performs broad-reaching independent assessments of human spaceflight-related activities, including formal Independent Validation and Verification (IV&V) of flight and ground software critical to flight crew safety;
  - Oversees and assesses the technical excellence of safety and mission assurance tools, techniques, and practices throughout the human spaceflight program life cycle;
  - Provides knowledge management and training in safety and mission assurance disciplines to the assigned workforce; and,
  - Assures that adequate levels of both programmatic and Center institutional resources are applied to safety and mission assurance functions.

### **NASA Human Spaceflight Safety Initiatives**

In the past several years, OSMA has sponsored several initiatives with the intent of enhancing the safety of human spaceflight. OSMA has increased its emphasis on the qualification and credibility of safety and mission assurance professionals by working with the Center Directors to assign some of their best and brightest employees to safety and mission assurance positions. We have also established a new Technical Excellence Program with a four-tier training and qualification system for all safety and mission assurance professionals across the Agency. Additionally, safety and mission assurance professionals assigned to human spaceflight programs now have formal technical authority for associated safety and mission assurance requirements as well as the authority to determine safety risk acceptability for designs and/or operations, including human spaceflight launch.

Another initiative is an increased emphasis on safety culture throughout the human spaceflight programs. This includes more open communications, including encouragement for dissenting opinions; clear appeal paths to the Administrator for safety dissenting opinions; and the “*Yes if*” initiative, an incentive that promotes the ideal that credible and capable safety and mission assurance professionals not simply know the rules, but understand their rationale to the point that they can help the design or operations team with alternative approaches consistent with safety and mission success.

OSMA has also made improvements in critical software IV&V by increasing the emphasis on validation of critical software requirements early in design. The IV&V team is also increasing the use of modeling and other systems engineering techniques to enhance their effectiveness in assessing the safety and utility of the critical software.

Improved knowledge management and requirements management tools and processes have also been put into place. This includes dedicated knowledge capture, archiving and dissemination activities, as well as better tools for tracking, updating, and rationalizing the more than 3,000 NASA technical and operational SMA requirements (many of which apply to human spaceflight). These activities, as well as improved audit, assessment and mishap investigation procedures and capabilities, are all primarily managed at the NASA Safety Center located near the Glenn Research Center.

Finally, OSMA has increased the amount of mentoring, training and technical assistance provided by our Headquarters SMA experts to the human spaceflight programs and their host Center SMA and engineering organizations.

## **Incorporating Lessons Learned into Agency Standards and Procedures**

The Columbia Accident Investigation Board (CAIB) documented for us once again the inherent risk of human spaceflight, noting that “the laws of physics make it extraordinarily difficult to reach earth orbit and return safely.” To justify the risk, the CAIB called for “a national mandate providing NASA a compelling mission requiring human presence in space.” The Board also recommended that “the design of [the Shuttle replacement] should give overriding priority to crew safety, rather than trade safety against other performance criteria, such as low cost and reusability, or against advanced space operation capabilities other than crew transfer.”

The many CAIB recommendations dealing with root causal factors, as well as NASA’s own Return to Flight assessments, pointed to several important lessons including, but not limited to, those outlined below. These recommendations and lessons indicate that NASA should:

- Maintain clear lines of accountability including strong checks and balances between program/project managers and their assigned independent technical authorities.
- Organize for a strong program-level systems integration function for complex, multi-element human spaceflight programs.
- Infuse the organization with a strong safety culture with open communications in all directions, encouragement of alternate opinions, and formal appeal paths for dissent.
- Treat every crewed space flight like an engineering test flight, and retain adequate program resources to thoroughly prepare for each flight and analyze and resolve ground and flight anomalies.
- Emphasize crew escape, abort and emergency systems and procedures to improve crew survivability during anticipated or unanticipated flight contingencies.

In the early 1990s NASA engaged in a joint U.S.– Russian project called Shuttle-Mir, picking up where the Apollo-Soyuz Test Project had left off in 1975. In preparation for the joint activity, NASA technical experts, including senior safety engineers, spent a significant amount of time over a three-year period talking with Apollo-Soyuz veterans, visiting with current Russian counterparts, and reviewing the long history of Soyuz, Salyut, and Mir operations in an effort to understand the Russian approach to human spaceflight safety. The two governments also established a high-level, joint technical oversight body (the Stafford-Utkin, now Stafford–Anfimov, Commission) in January 1995 to independently review Soyuz readiness for flight and to report its findings directly to the heads of agencies. In March 1995, Norm Thagard became the first U.S. astronaut to launch on the Soyuz. He and the other five astronauts who spent time on Mir used the Shuttle for subsequent transportation, but they all received training in Soyuz as their primary escape system.

Following on the success of the Shuttle-Mir program, NASA and the Russian Federal Space Agency (Roscosmos) agreed to create a joint space station in 1993. The International Space Station (ISS) Intergovernmental Agreement and Memorandum of Understanding (the final version of which was signed in 1998) recognized the Russian government’s responsibility for crewmember safety for their elements, including Soyuz. The next American to launch on Soyuz was Bill Shepherd, the Commander of the first ISS increment in October 2000. Like Thagard, Shepherd returned to Earth on Shuttle, and like the Mir astronauts, he was trained on the Soyuz spacecraft. Since then, 14 different NASA astronauts have flown on Soyuz, bringing the total NASA astronaut trips to 14 up, and 13 down, several of which were made during the post-Columbia Return-to-Flight timeframe. Canadian and European partner astronauts have flown to and from ISS on Soyuz, and the next Soyuz will carry

a Japanese partner astronaut. As we speak, Soyuz is the primary mode of transportation to and from the ISS for all ISS crewmembers.

NASA's Russian partner engineers and managers have been open with their designs, operations, system anomalies, and close calls; however, there have been occasions when, for various reasons, they have restricted technical information transfer to our engineers. On these occasions, perseverance by our technical staff on the ground and dependence on the Russians' proven engineering and operational savvy that spans more than 40 years of human spaceflight, have resulted in sufficient confidence in their systems and operations (approximately 96 percent mission success rate, and 98 percent crew safety record for all versions since 1967), and mutual trust initiated during the Apollo-Soyuz program, and reinforced most recently with over 15 years of joint space station operations. Some of the many human spaceflight safety lessons from NASA's joint work with the Russians on Soyuz, Mir, and ISS include:

- The Russian design philosophy depends heavily upon reliability in addition to adherence to a strong design heritage (robust systems and failure tolerance, often using dissimilar redundancy), but they are big believers in abort, escape, and emergency systems for known or unknown contingencies that are not covered by reliability alone.
- The Russian design philosophy also rests heavily on testing. During the Soyuz update from the TM (modified transport) to TMA (TM anthropometric) version (enlarged in the 1990's to accommodate larger astronauts), they performed multiple tests, including drop tests, to ensure that the design was equivalent, or superior, to previous versions. This testing is often carried to conditions beyond the nominal expected environments. As Roscosmos prepares to upgrade the control computer system on the Soyuz, they are first installing and testing this upgrade in the Progress cargo vehicles. In this way, they can flight test the system with less critical cargo before it is required to transport crew. This provides an additional rigorous test and helps to insure overall crew safety.
- The Russian development philosophy is based on evolutionary upgrades, keeping what works, and modifying or replacing what does not.
- The Russian design and operational organizations include reliability and quality engineering staffs, but they do not have an independent safety engineering staff like NASA does. That said, they include many of the same safety functions as NASA does as part of the other engineering disciplines, and they do provide one of their most experienced engineers as NASA's SMA counterpart.
- The Russian technical staff is very skilled and displays outstanding knowledge of the flight systems. With relatively low turnover, they also have excellent corporate memory, which helps them deal with any repeat problems.
- The Russians, unlike NASA, rely on automation and ground control for certain critical dynamic events like abort initiation, landing, proximity operations and docking.

Although NASA and Roscosmos have occasionally disagreed about relative risk levels for such things as orbital debris, battery hazards, etc., our experience to date shows us that they have no intention of putting crewmembers in known unsafe situations for the sake of expediency.

The Columbia Crew Survival Investigation Report, prepared by the NASA Spacecraft Crew Survival Integrated Investigation Team (SCSIIT) and released in December 2008, is a comprehensive study of crew safety, equipment and procedures used during the Space Shuttle Columbia accident. The report contains 29 specific findings, half of which apply to Space Shuttle and to NASA investigation procedures, and half to future designs. The Constellation Program has assessed the report's findings, incorporating several of them into the Orion design, and the Program plans to incorporate others as

the design matures. The fundamental theme of the findings is that human spaceflight programs should include crew survivability in the system design, and that operational plans should provide for safe egress, abort and/or escape from contingency situations. This is a top level requirement in NASA's most recent human rating requirements policy contained in NASA Procedural Requirement (NPR) 8705.2B (May 6, 2008). The rationale comes from our three fatal human spaceflight accidents. It is not enough to design a human spaceflight system to be reliable. The Earth-to-orbit mission is about managing incredibly high-energy systems and environments, with very little room for error. When measured by number of flights, human spaceflight transportation is still relatively immature, and the designers and operators are continuously learning about the real risks involved with spaceflight activities. Thus, as the report highlights, and the human rating requirements mandate, there is a need to provide the crew with a fighting chance for survival if and when something goes wrong, anticipated or not.

The Constellation Program is using the SCSIIT report as a design guideline; and as the Program tailors its suggestions into Program requirements, we in OSMA are drafting a follow-on technical standard for use by future human spaceflight system developers. The design standard will provide cues for designers and will also make it clear that the addition of any systems to increase the survivability of the crew needs to consider both the system design and concept of operations. In the meantime, NASA has made the SCSIIT report available to the public, sending copies directly to all known commercial space companies. The SCSIIT has also given presentations about the associated lessons-learned to NASA Centers, as well as to the National Transportation Safety Board, Federal Aviation Administration, the Department of Defense, the Defense Contract Management Agency, and others totaling over 4000 people to date.

### **Safety and Commercial Spaceflight**

NASA will require that any Earth-to-orbit and/or orbit-to-Earth system that carries NASA astronauts be human rated, thus ensuring that all of our stringent crew and launch safety requirements would be met before any NASA crew would be allowed to travel on a spaceflight vehicle. As part of that process, the Agency's Technical Authorities (Engineering, SMA and Health and Medical) will determine which of NASA's mandatory standards apply in designing, manufacturing and operating their system. OSMA and the Johnson Space Center SMA organization worked closely with the Constellation program for over six months in 2008 to establish and tailor the applicable SMA requirements for the Constellation Program. This was a very detailed and involved activity that reminded us that the job of validating the right set of requirements for a new crewed flight system is not a simple cookie-cutter or checklist task. Nor is it expected to be a one-time task. The requirements refining and tailoring process will continue as we learn more about the design, the environment and the operational concepts. NASA's Commercial Crew and Cargo Program Office has initiated an effort to determine and establish the requirements (both process and design) as well as any other standards that should apply to commercial partners when engaging in services for transporting astronauts.

Currently, NASA is working with two companies, Space Explorations Technologies Corporation (Space X) and Orbital Sciences Corporation (Orbital), as part of individual Commercial Orbital Transportation Services (COTS) projects designed to develop and demonstrate commercial cargo capabilities to and from low-Earth orbit. In doing so, NASA has agreed to pay both companies pre-negotiated amounts when each company achieves pre-negotiated milestones outlined in Space Act Agreements, and OSMA is part of the review team assessing each company's progress toward meeting required milestones. Last year, NASA also issued contracts to both Space X and Orbital, for cargo delivery to the ISS under the Commercial Resupply Services (CRS) Program.

NASA is utilizing FY 2009 Recovery Act funds to support activities to stimulate efforts to develop and demonstrate technologies that enable commercial human spaceflight capabilities. NASA is also investing Recovery Act funds to begin development of a more concise set of NASA human rating technical requirements. These requirements would be applicable to NASA developed crew transportation systems as well as commercially-developed crew transportation systems for use by NASA. This task is being performed by a team comprised of representatives from NASA's human spaceflight programs, the Astronaut Office, and Agency technical authorities, including OSMA. We are also consulting with other Government partners such as the Federal Aviation Administration and with commercial stakeholders.

### **Conclusion**

In closing, the Office of Safety and Mission Assurance plays a significant role in ensuring the safety of human spaceflight. By continually improving its workforce, communications, and processes, the Office of Safety and Mission Assurance is an organization of technical excellence that is well-equipped to support the Agency's human spaceflight safety efforts. By disseminating and incorporating into its standards and policies the many lessons learned throughout the history of human spaceflight, NASA is able to improve safety in its own future designs, and to facilitate safety in those that may be developed commercially.

Chairwoman Giffords, I would be happy to respond to any questions you or the other Members of the Subcommittee may have.