HOLD FOR RELEASE
UNTIL PRESENTED
BY WITNESS
March 18, 2010

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

before the

Subcommittee on Space and Science
Committee on Science and Commerce
United States Senate

Chairman Nelson and Members of the Subcommittee, thank you for the opportunity to appear before you today to discuss how NASA will ensure the safety of its human spaceflight missions for transport of NASA and NASA-sponsored International Partner crewmembers to the International Space Station.

The President's FY 2011 Budget Request for NASA

The President's budget request cancels the NASA Constellation Program and funds the Agency to contract with industry to provide astronaut transportation to the International Space Station (ISS) as soon as possible, reducing the risk of relying solely on foreign crew transports for years to come.

NASA will take on this new challenge with appropriate respect for hard-learned safety lessons of the past. NASA will use a disciplined acquisition processes to support the development, testing and demonstration of multiple commercial crew systems to the ISS that safely and dependably perform the same functions as the Russian Soyuz system.

The Role of OSMA in Ensuring Human Spaceflight Safety

The NASA Office of Safety and Mission Assurance (OSMA) was established in the wake of the Challenger accident, and provides policy direction, functional oversight, and assessment for all Agency safety, reliability, maintainability, and quality engineering and assurance activities, while serving 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 OSMA, I report directly to the NASA 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, OSMA:

- 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 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.

Crew Safety and Human Spaceflight

The launch and recovery of a spacecraft is a very dynamic event involving tremendous amounts of potential and kinetic energy. Such events expose flight crews to significant inherent risks in the form of a variety of potentially catastrophic hazards and survivability challenges. Further, operations of any system in the proximity of the ISS pose their own safety integration challenges for both vehicle(s) and crew. Therefore, through its program management, systems integration and human rating design, and technical checks and balance, NASA makes every effort to address flight crew safety in a transparent and disciplined way. The process analyzes and manages failure modes and effects, and strives to eliminate hazards that could harm the crew. Where hazard elimination is not practical, the design and operational concept attempts to control or at least mitigate hazards, sometimes with crew procedures, other times with extra controls on the manufacturing, test or inspection of components to minimize human error or chance of hardware/software failure. In addition, the human-rated system provides for crew survival in the presence of catastrophic events through abort or escape. As we have been reminded by all of our major human spaceflight accidents and close calls in the past, system integration, including the interrelated effects of the various flight and ground elements for accident initiation as well as

hazard mitigation should not be underestimated. Spaceflight vehicles traditionally have been certified by NASA to carry crews in an engineering flight-test environment.

It is important to note 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. Compliance with requirements is only part of what makes us comfortable in human spaceflight. Much of what we do in development and operations is proactive and reactive risk management. The risk of human spaceflight is inherently high, and we know from the past that we are never as smart about this business as we think we are. We still see new safety issues on the Space Shuttle after 130 flights. Therefore, we are always looking for ways to improve our risk posture by continuously questioning our assumptions, refining our models, checking our work, and providing appropriate oversight and/or insight to the work of our contractors.

Further, our history teaches us that new risks will come up during the lifecycle of any human spaceflight system. For example, any human system will require extensive iterative work in development and optimization of abort and escape capability. In the future human systems must provide the crew with a reasonable chance at a survivable outcome even when the situation is catastrophic to the flight system. In any number of human spaceflight systems developments in the past, limitations in the abort/escape systems were not known until well into the design, at which time other hazard mitigators such as added robustness or system redundancy, or extra limits to the flight envelope were laid on late in the design cycle. Late safety risks must be treated with the same discipline and respect as any early design challenges; and where safety risks can be reasonably tolerated, their acceptability must be agreed to by all four elements of NASA's governance structure: the relevant technical authority, the cognizant system safety engineer, the flight crew, and finally the program manager. We also know from organizational cultural lapses in the past that we must encourage a reliable, recognized appeal system to hear and deal with any credible voice of dissent concerning crew safety.

In the end, the decision to transition our ISS crewmembers from Soyuz to any new vehicle will be based on NASA leadership attaining the confidence that the new system will meet or exceed its standards and requirements, including the risk level assigned by the agency for the ISS transport mission. This confidence will be based on the combination of NASA technical insight into the design, appropriate levels of management oversight of the development and operation, verification of performance and technical requirements along with demonstrated capability and reliability of components, subsystems (including escape and abort subsystems) and the integrated flight/ground system.

Safety and Future ISS Transportation Systems

The first step on the road to confidence for the next ISS crew transport capability is establishing an acquisition approach and operations model for our government/industry team. To support that approach, we are developing performance requirements, including safety risk metrics, and a generic set of NASA human rating technical requirements that would be applicable to any ISS-bound crew transportation system. NASA's Commercial Crew and Cargo Program Office and its technical authority, in coordination with the ISS program/technical authority, has initiated an

effort to determine and establish the requirements and standards (process, design and operational) that would most likely apply to industry partners when engaging in astronaut transport development and operations.

As part of that effort, NASA is investing funds from the American Recovery and Reinvestment Act of 2009 (P.L. 111-5) to develop a subset of its human rating technical requirements that would most likely apply to the specific ISS transport mission. The technical requirements would be applicable to NASA developed/operated crew transportation systems as well as industry-developed/operated 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 the OSMA. We are also including the Federal Aviation Administration because of its obvious interest in future regulatory activities for human spaceflight. When these documents have completed internal Agency review, NASA plans to issue a Request for Information to alert all interested parties of our intent, as well as to seek industry feedback. NASA currently anticipates completing this process in calendar year 2010. When completed, these requirements documents will provide guiding principles for developing, clearing for flight, and operating any spaceflight system before it is allowed to carry NASA crewmembers. As with any complex, high risk system, the ultimate design and operational requirements are tailored to fit the mission, the design concept, and the industry partner's own standards, experience and processes. This tailoring begins pre-award, but it continues into the early acquisition phases after a contract has been let.

Conclusion

In closing, I would like to reiterate that safety is, and will always be, NASA's first core value, and that everyone at the Agency is dedicated to ensuring that our astronauts are trained and equipped to safely conduct NASA's spaceflight missions.

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