HOLD FOR RELEASE
UNTIL PRESENTED
BY WITNESS
January 17, 2018

Statement of
Dr. Patricia Sanders
Chair
National Aeronautics and Space Administration's
Aerospace Safety Advisory Panel

before the

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

Mr. Chairman and Members of the Subcommittee, thank you for the opportunity to appear before you today to discuss the status of NASA's Commercial Crew Program (CCP).

The Aerospace Safety Advisory Panel believes that NASA is at a critical juncture in human space flight development. Both the Commercial Crew Program and the Exploration Systems Development are well beyond paper design with hardware being produced, testing underway, and first flights—uncrewed test flights followed by crewed test flights—on the horizon. This is a time when it is important to retain focus on program details; to maintain a sense of urgency while not giving in to schedule pressure; and to continue with program plans without neglecting, shortchanging, or deleting planned content. Important decisions are facing NASA leadership in certifying these platforms for human space flight that should be based on a strong foundation of test and engineering data.

The Panel has consistently articulated the need for constancy of purpose, as NASA is on the verge of realizing the results of years of work and extensive resource investment in these programs. This includes making sure that the appropriate resources are provided to complete the job. We continue to strongly caution that any wavering in commitment negatively impacts cost, schedule, performance, workforce morale, process discipline, and – most importantly – safety.

With respect to the Commercial Crew Program specifically, we see continual steady progress toward providing the capability for crew transportation to low-Earth orbit and the International Space Station (ISS). Both providers are planning for test flights in 2018, with the first Post Certification Missions to ISS no earlier than November 2018. NASA has procured seats onboard Soyuz 58 and 59 for transportation of U.S. Astronauts to ISS through late 2019.

While the Panel is unaware of any efforts to purchase additional Soyuz seats after Soyuz 59, the current planning dates would allow NASA to utilize the commercial providers to maintain uninterrupted access to ISS. However, based on the quantity, significance, and associated uncertainty of work remaining for both commercial providers, the Panel believes there is a very real possibility of future schedule slips that could easily consume all remaining margin. There

are several major qualification and flight test events that historically are schedule drivers or could reveal the need for additional work. These include pyro shock qualification tests, parachute tests, engine hot fires and qualification runs, abort tests, and both uncrewed and crewed flight tests. Also, SpaceX is still working on the redesign and qualification of the Composite Overwrap Pressure Vessel (COPV) helium tanks for the Falcon 9 (F9), in response to the F9-29 mishap. I will discuss this issue, which has significant work ahead, later.

In addition to the technically complex test and qualification work remaining for the providers, NASA also has a significant volume of work remaining. The final phase of the NASA Safety Review process, where verification evidence of hazard controls is submitted by the provider and dispositioned by NASA, remains ahead. This is in addition to the majority of CCP 1130 and ISS 50808 requirements verifications, where the provider submits the verification evidence via Verification Closure Notices for NASA review and disposition. Even though it is common for verification packages to be completed late in the certification process, the sheer volume of work that remains to adequately review and disposition these Notices is significant. If NASA were to determine that the evidence submitted does not meet the verification standard on some requirements or hazard controls, additional time would likely be required to resolve the issue with the provider.

Despite the volume of remaining work, technical challenges, and end of the Soyuz transportation for U.S. crews, the ASAP sees no evidence that the Program leadership is making decisions that prioritize schedule over crew safety. However, we expect to see several significant certification issues brought to culmination in the next year that will require NASA risk acceptance decisions at a very high level within the Agency. It is possible that in some cases, the most favorable schedule options will require a decision to accept higher risk. The Panel advises NASA to maintain awareness of potential schedule pressure. We note that the strategy of funding two providers was adopted, in part, to avoid a situation where NASA would be forced to accept undesired risk to maintain crews on ISS. Maintaining U.S. presence on ISS, without acquiring additional Soyuz seats, requires one provider be certified and ready to fly crew to ISS by mid to late 2019. Certification of the second provider could happen after that time.

It is worth noting that certification represents the foundation upon which the safety, reliability, and performance of the system rests. It encompasses a validation that all requirements have been properly covered and adjudicated between the provider and NASA. It means that the system configuration is known and fixed. The hardware and software in question must have complied with the adjudicated requirements, and its performance must have been verified in accordance with agreed-to testing, analysis, and/or other certification artifacts as delivered and approved. Each vehicle flown under the certification must have the hardware properly accepted (without violating the qualification limits) and the configuration verified to comply with the certified configuration. Successful achievement and compliance with certification requires that the provider have disciplined engineering and operations processes along with adequate controls to prevent process escapes. Traditionally, this is considered part of systems engineering, but disciplined processes can also be applied by providers employing non-traditional approaches. In February, the Panel made the following formal recommendation to NASA:

The Panel recommends that NASA require the Commercial Crew providers to produce verifiable evidence of the practice of rigorous, disciplined, and sustained system engineering and integration (SE&I) principles in support of the NASA certification and operation of commercial crew transportation services to the ISS.

In response to the recommendation, NASA assessed its insight into and oversight of both providers' engineering practices. NASA reported the following action plan to the Panel:

- Review latest SE&I-related plans and processes
- Increase audits of compliance to SE&I-related plans and processes
- Conduct system-level design reviews to ensure interfaces and inter-relationships of subsystems have been adequately addressed

While the Panel commends NASA for these actions and its acknowledgement of the need for increased surveillance of at least one provider, NASA should expect both providers to exhibit a safety ***culture*** appropriate for human space flight. This requires each provider to internalize the ***value*** of highly disciplined processes and controls and engrain them into the company culture. We intend to hold this recommendation open until we see evidence of achieving this outcome. The investigation into the recent mishap during Merlin engine qualification and execution of critical qualification and validation tests will provide an opportunity to gauge the progress of this effort at SpaceX.

I will now address the Commercial Crew Program's Probabilistic Risk Assessment (PRA) requirement for loss of crew (LOC) which, covering a 210-day mission to ISS, is 1 in 270. In clarifying the requirement, the Program allocated 1 in 200 to the providers' systems, with the remainder allocated to operational mitigations such as on-orbit inspection. There is also a specific PRA requirement for the ascent and entry phases–1 in 500 (combined). The Panel has been monitoring the providers' progress in working toward the LOC requirements, and it appears that neither provider will achieve 1 in 500 for ascent/entry and will be challenged to meet the overall mission requirement of 1 in 200 (without operational mitigations).

PRA is a well-recognized tool that allows the assessment of hazards and their relative contribution to risk to assist in the design and development process. History has shown that the PRA values should not be viewed as an absolute measure of the actual risk during operations. When developing new human space flight vehicles, the unique nature of these systems and limited test data results in large uncertainties in the PRA numbers. In our opinion, the most valuable element of the PRA analysis is the identification of the major risk drivers, which can then be mitigated by design changes, additional testing, or other controls. While there are large uncertainties around the specific numbers resulting from the analysis, the primary risk drivers identified are the same for both commercial systems:

- Micrometeoroid and Orbital Debris (MMOD) damage during docked phase (affects overall mission requirement)
- Parachute performance (affects overall mission and ascent/entry requirements).

Based on the PRA identification of these risk drivers, NASA and the providers have applied resources to improve the capability to withstand MMOD impacts, better understand the ability to tolerate MMOD damage, and perform additional parachute tests. Operational mitigations such as on-orbit inspection and abort weather Launch Commit Criteria were also directly informed by the PRA results. Ultimately, the NASA PRA requirements were established to set an analytical risk standard for the Commercial Crew systems that was significantly better than the Space Shuttle and challenge the providers to make their systems safer by focusing resources on critical areas of the design and operations. The Panel commends the NASA team and providers for using the PRA tool to effectively improve the risk posture. However, the likelihood remains that the providers will not meet all the PRA requirements, and NASA will need to determine if the risk portrayed by the analysis, with its large uncertainties, is acceptable. We encourage NASA to fully consider all factors, including the rationale and environments used to derive the original requirements, when evaluating the final PRA LOC numbers for both providers and making any risk acceptance decision.

I will return now to the Falcon 9 helium tank redesign and qualification. At this time last year, the investigation for the F9-29 mishap was ongoing. SpaceX conducted the investigation with NASA, the U.S. Air Force, and FAA participation. NASA also conducted its own independent analysis of the evidence. Early in 2017, a Panel member attended SpaceX's briefing to NASA, covering the investigation results and conclusions. The Panel also received a copy of the mishap report and was briefed separately by SpaceX. The SpaceX investigation did not find a single most probable cause of the initiating event, instead identifying several credible causes involving the COPV helium tanks. All credible causes were similar in that they involved liquid oxygen (LOX) trapped between the overwrap and the liner with subsequent ignition through friction or other mechanisms. The evidence recovered from the mishap showed indications of buckles in the COPV liner where LOX was likely trapped. Acting from the report findings, SpaceX was able to recreate a buckle event during a COPV test. Additional testing allowed SpaceX to identify specific conditions which would cause a buckle and trap oxygen in the gap between the liner and overwrap. Using this data, SpaceX modified its helium loading configuration, process, and controls to ensure that the COPVs would not be exposed to these identified conditions and, accepting any residual risk, successfully resumed commercial launches with the existing COPV design. However, to further improve safety, SpaceX and NASA agreed that a redesign of the COPV was necessary to reduce the risk for missions with crew onboard.

Using what they learned from the mishap investigation, SpaceX redesigned the COPV and NASA started a rigorous test program to characterize the behavior of the new COPV in the cryogenic oxygen environment. The Panel considers this to be the most critical step in clearing the COPV for human space flight, as it allows NASA and SpaceX to identify the credible failure mechanisms, hazard scenarios and controls, as well as understand the safety margins on the system. With this information, SpaceX can develop a proper qualification program and NASA can decide on the acceptability of the hazard controls and residual risk. The Panel strongly supports this effort and notes that this is another example of the commercial providers and NASA working together to solve a very difficult technical issue. In our opinion, adequate understanding of the COPV behavior in cryogenic oxygen is an absolutely essential precursor to potential certification for human space flight. It also should be noted that NASA and SpaceX are working on an alternative helium tank design should the COPV certification efforts fail.

However, the heavier weight of the alternative design could require significant modifications to the supporting structure to handle the additional loads. Additionally, if the alternative tanks are only flown for NASA missions, the potential hazards and impacts arising from operating a unique F9 vehicle at a relatively low flight rate (as compared to SpaceX launches for other customers) would need to be carefully assessed.

The discussion of COPVs would not be complete without a mention of SpaceX's plan to load densified propellants after the crew is onboard the Dragon2 (often referred to as "load and go"). In last year's annual report, the Panel urged NASA and SpaceX to focus on "…understanding how the system functions in the dynamic thermal environment associated with 'load and go' so that … previously unidentified hazards can be discovered." While the COPV efforts are consistent with that advice, we advise NASA not to discount the other potential hazards associated with loading cryogenic propellants – particularly LOX. Fully assessing all the hazards is critical in determining the best time to load the crew onboard the Dragon2 for launch after considering the risks and benefits associated with such a decision.

In closing, let me say that the Panel believes that NASA is addressing safety properly, but space can be a decidedly hostile environment and human space flight is inherently risky. There is no excuse for negligence in the safety arena, but it is impossible to eliminate or control every potential hazard.

We particularly note that potential for damage from micrometeoroids and orbital debris has become recognized as a major issue in every program. The United States government should seriously consider expanding its efforts to lead in developing international strategies to reduce debris generation and the hazards posed by existing debris.

Recognizing that space flight holds inherent hazards, there is always a probability of mishaps needing rigorous and disciplined investigation to avoid future incidents and to return to flight as safely and as soon as possible. We believe it is important to have mechanisms and procedures in place before a mishap event occurs to enable expeditious and effective investigation.

With the Commercial Crew Program, NASA has introduced an approach to developing space flight assets in cooperation with commercial providers. The future brings the potential for more partnerships bringing both opportunities and challenges with respect to safety processes and mechanisms. In the coming year, the Panel plans to spend focused effort on Commercial Crew and also look to the future of responsible and exciting human space exploration.