National Aeronautics and Space Administration
Office of the Administrator
Washington, DC 20546-0001

October 9, 2012

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

Dear ~~Admiral~~ Joe Dyer:

Enclosed is NASA's response to four recommendations from the 2012 Third Quarterly Meeting of the Aerospace Safety Advisory Panel (ASAP). Please do not hesitate to contact me if the ASAP would like further background on the information provided in the enclosures.

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

Sincerely,

Charles F. Bolden, Jr.
Administrator

4 Enclosures:
2012-03-01 - Software Assurance and Capability Maturity Model Integration (CMMI) Requirements
2012-03-02 - Software Assurance Metrics
2012-03-03 - Software Independent Verification and Validation (IV&V) Requirements
2012-03-04 - Revised Estimate of Loss of Crew (LOC) and Loss of Mission (LOM) for the International Space Station (ISS)

Tracking Number 2012-03-01
Software Assurance and Capability Maturity Model Integration (CMMI) Requirements

Finding:
The ASAP learned that NASA is working toward a Capability Maturity Model Integration (CMMI) Level 3 development standard across the Agency. The documentation seems to indicate that is in place now, but the ASAP would like that to be confirmed.

Recommendation:
All NASA internal safety-critical software development groups should achieve CMMI Level 3 (or an equivalent as established by external validation agent) by the end of FY 14.

Rationale:
Compliance and accreditation at CMMI Level 3 is a requirement for bidding on most U.S. government contracts; NASA should require the same level of performance regarding its internal software related activities. It should also be noted that reduced life cycle cost is one of the expected results of adoption of the CMMI process, which may provide added benefit to NASA if this course of action is adopted.

NASA Response:
NASA agrees with the intent of the recommendation and is already doing this; however, not all safety-critical projects can meet this. Some of our projects are very small, done in programmable logic devices, or are done by the universities.

NASA has required CMMI-Development (DEV) Maturity Level (ML) 3 for Class A software and CMMI ML 2 for Class B software since November 2009 (NASA Procedural Requirements (NPR) 7150.2A, NASA Software Engineering Requirements). Class C software is required to address a subset of this requirement (with the subset decided by the Center). The current CMMI ratings held by organizations at NASA Centers responsible for development of Class A and B software are:

Kennedy Space Center (KSC)	CMMI ML 2
Marshall Space Flight Center Flight Software	CMMI ML 3
Marshall Space Flight Center Software Integration Laboratory	CMMI ML 2
Ames Research Center (Codes TI (Intel) & QS (System Safety & Mission Assurance))	CMMI ML 2
Glenn Research Center Flight Software	CMMI ML 2
Jet Propulsion Laboratory (All Mission Software)	CMMI ML 3
Langley Research Center Flight Software	CMMI ML 2
Goddard Space Flight Center Engineering Division	CMMI ML 2
Johnson Space Center Flight Software	CMMI ML 3

KSC is the only Center responsible for Class A software which does not yet have CMMI ML 3. They are at ML 2 and working towards ML 3 (which they should achieve in FY 13). Dryden Flight Research Center and Stennis Space Center are not responsible for the development of

Class A or B software. As such, they do not fall within the scope of NASA's full CMMI requirement in NPR 7150.2A. These two Centers have local development processes for software which align with NPR 7150.2A and contain requirements that closely align with CMMI process requirements.

Not all safety-critical software needs to be developed and managed at the same level. NASA has Class A safety-critical software that involves human flight and requires the highest level of process assurance and management. NASA also has Class D or E safety-critical software which can be at the test bench level and may involve software turning lasers on and off, or monitoring a critical fluid pressure and temperature for a test chamber, or even a Class C database which maintains flight configuration data. Not all of this safety-critical software requires the rigor, cost, and overhead of obtaining and maintaining a CMMI Level 3. In these instances, NASA does not require CMMI credentials to develop this software and instead has levied NASA requirements that adequately mitigate safety concerns.

NASA has assessed the relative risk and is ensuring that our most critical software, human flight software, is covered by CMMI ML 3 and by NASA software engineering, software assurance, and software safety processes. NASA is on track to have CMMI ML 3 for all Centers responsible for Class A software by FY 13.

Tracking Number 2012-03-02
Software Assurance Metrics

Finding:
ASAP believes that NASA has a comprehensive software assurance process, but would like to see some evidence that the process is working.

Recommendation:
NASA should provide metrics and trends that demonstrate whether the software assurance provisions are working and provide return on investment.

Rationale:
While the processes seem to place emphasis on providing software assurance, progress toward that goal should be measurable. NASA should be measuring the effectiveness of their software assurance processes in order to have confidence that they are providing the expected value.

NASA Response:
NASA agrees with the ASAP recommendation and has software assurance process metrics/measurements to assess the ability of software assurance to meet the needs of the projects and determine where improvements need to be made (see NASA Standard (STD) 8739.8, Software Assurance Standard). NASA also has software quality metrics/measurements to assess the state of the software products and process; these are defined in NASA Procedural Requirement (NPR) 7150.2A, NASA Software Engineering Requirements.

NASA tracks the number and type of projects supported and the number of software assurance personnel assigned to each project. Also, during winter 2011-2012, a survey was sent to software assurance customers (the project managers, software leads, and Chief Safety and Mission Assurance Officers); the results of this survey showed an overall satisfaction rate over 70 percent with software assurance support and an 11 percent disapproval rate (NASA is reviewing this feedback to better understand the reasons behind the disapproval rate).

Acting upon this ASAP recommendation, the Software Assurance Technical Discipline Fellow has sent a data call to all the NASA Centers to collect information on Center reporting and performance metrics for software assurance. This data collection is in work, and NASA will provide the results to ASAP in November 2012.

Tracking Number 2012-03-03
Software Independent Verification and Validation (IV&V) Requirements

Finding:
NASA has clarified the processes and criteria used to prioritize safety-critical software for IV&V and has put IV&V in the overall context of software assurance. The process and criteria seem to be reasonable, but the Panel is concerned that there is not a standard for identifying what level of criticality should require IV&V.

Recommendation:
NASA should establish a standard identifying the level of criticality that requires a software IV&V, i.e., what risk level must IV&V be required and therefore either be resourced, or if that is not possible, a formal waiver process be in place for an accountable individual to accept the associated risk and document it.

Rationale:
Software constitutes a known risk area in any system design and development. After the software is identified as having exceeded a known and defined level of criticality (as measured above) then IV&V is needed to assure that the risk is mitigated. If this is not done then the reason for risk acceptance needs to be formally documented as it would be for any other known accepted risk.

NASA Response:
NASA agrees with the intent of the recommendation to establish a more formal process for selecting projects for IV&V. Currently, the IV&V Board of Advisors (IBA) selects projects for IV&V on an annual basis. The IBA takes into consideration an assessment of the criticality among candidate projects, using input from the NASA Mission Directorates, software development and categorization information contained in the Chief Engineer's software inventory, and criticality assessments from software assurance personnel at NASA Centers and at the IV&V Facility. The process is flexible to allow for the variances in the budget available to perform IV&V work. However, NASA agrees that there needs to be an established process to document the risk considerations in the selection process, that minimum threshold for IV&V should be established, and that a waiver process should be implemented when the threshold cannot be met.

NASA will coordinate and implement the above noted considerations of risk evaluation, minimum threshold for IV&V, and waivers when the threshold cannot be met into a set of project selection guidelines to be used during the IBA review process. NASA will also review related software policy requirements to evaluate consistency and implement necessary updates to reflect the guidelines for the IV&V selection process. NASA will provide status updates to ASAP and anticipates that the IBA guidelines will be in place by the next annual review process (CY 2013) and associated policy revisions will be incorporated into follow-on update of the associated NPR documents.

Tracking Number 2012-03-04
Revised Estimate of Loss of Crew (LOC) and Loss of Mission (LOM)
for the International Space Station (ISS)

Finding:
On the upcoming increment, some additional Micro-Meteoroid and Orbital Debris (MMOD) shielding will be installed on ISS. Also, additional MMOD shielding for Soyuz is now underway and is expected to be complete by 2014. This MMOD protection will change the LOC and LOM numbers regarding ISS.

Recommendation:
Revised estimates for both LOM and LOC for ISS due to both MMOD and other causes through 2020 (based on the current configuration) should be determined and compared to the data previously supplied in this regard which predated any of the recent MMOD hardening that has been implemented on ISS.

Rationale:
Previous data supplied to the ASAP indicated that over a 10-year period, there is a greater-than-30-percent chance of LOM, which in some cases could result in an off-nominal de-orbit of the ISS. The actions being taken now are intended to mitigate that risk somewhat, but it needs to be quantified.

NASA Response:
NASA agrees with the intent of this recommendation and is working to complete the analyses. Given the proximity to the Fourth Quarterly Meeting in mid October and complexity of this topic, NASA requests that we provide our response to the ASAP on 2012-03-04 via our scheduled ISS formal briefing. This will afford us a forum with greater detail and interactive conversation to address this ASAP recommendation.