

Questions	Answers
What are your current pain points?	Meeting Agency requirements with constrained resources. The accelerated schedule of the HEO projects have put difficult resource and achievement challenges on the IV&V program. Adjusting to changing and dynamic development schedules to ensure that IV&V support is provided in alignment with the SW development.
What are IV&V's current challenges as it relates to cyber security?	Staying ahead of cyber threats to missions is the typical challenge of any cyber related activities.
What works well in your current process?	The IV&V program continues to provide high value, and high quality, products and services to our customers. Building good customer relationships has worked very well. From our IV&V support, security services, outreach and software assurance support, our customer base has provided excellent positive feedback of our work. The IV&V has maintained very low false positive rates with regard to the issues identified across our analyses and IV&V has consistently maintained a high degree of phase alignment with the software development.
What would you like to change / improve?	Our relationships and communication of detailed information to the Agency's Program Managers and specific Project managers. The IV&V Program is always interested in identifying and implementing innovative approaches that result in increases in effectiveness and efficiency.
What are the top priorities for the IV&V program?	Safety and the success of mission is our number 1 priority. Mission success comes in many forms from IV&V, security (cyber), software assurance and outreach. Continuing to be a well respected employer in WV is another priority. Providing opportunities for all, including students and interns, to have rewarding work experiences at our facility.
What major goals is the NASA IV&V Facility trying to accomplish in the next five years?	Seamless infusion of mission security from an end to end perspective into our IV&V portfolio and a better characterization of mission security risk such that mission projects can integrate management of security risk together with other risks that impact mission success. Agile flexible IV&V approaches meeting customer needs. Cutting edge IV&V analysis techniques reducing cost and schedule for our support.
What are some recent successes in cyber IV&V?	We have had great success in providing mission critical assessments of various critical systems that support projects. Out of these assessment missions we have been able to address vulnerabilities, mitigate risks and even make design changes to ensure mission security. We have found things such as flight vulnerabilities, ground network access vulnerabilities, mission operations vulnerabilities, and mission interface security issues. Our assessments go beyond compliance to generic standard applying threat and risk based assessments in a mission usage perspective.
Are there any specific challenges your team has experienced under the current SAS effort? Staffing, technically, or otherwise?	This is not necessarily SAS specific but rather a challenge faced by the Program as a whole. As expected with any highly technical specialized work, getting the right personnel in place and up to speed immediately has been somewhat of a challenge. Cybersecurity personnel that have mission experience are difficult to come by. There is no NASA specific mission security training on day 1 so most of our cyber training is OJT. Our internal flexibility has been a great mitigation to these challenges.
What percentage of the contract work is dedicated to NASA missions/projects? Are there plans to increase the amount of support external to NASA?	We only have a small amount of non-NASA mission work. With any external or even non-IV&V type work opportunities, we review the pros and cons of each opportunity, including the return on investment for NASA and proceed accordingly.

Per Section 1.6, Contract Management, what are the current data repositories IV&V expects the Contractor to use?	ECM, Confluence, Jira
Has the IV&V Facility been CMMI appraised? If so, to what CMMI level and version?	For the most part we are not a development organization so the traditional CMMI for software does not apply. Our SWAT organization does develop some tools etc. and they are not CMMI appraised.
Is JSTAR primarily in support of Directed Project (DP) Task Orders (as opposed to IV&V on Software Development Projects)?	JSTAR is used to IV&V project activities and is used within the cyber lab for vulnerability research, verification and validation. At times JSTAR products are developed for external customers wanting virtual environments. Typically JSTAR simulations are not used to verify or buyoff requirements, but rather focused on evaluating the robustness and resiliency of the in focus flight software
Per SOW Section 2.7, is SSO support to other NASA Centers funded through IV&V or by the receiving Center? For example, if a NASA Center (e.g., WFF) requests software assurance support, do they fund the effort?	Mix of both
What percentage of the SAS 2 SOW is dedicated to SSO? How is the SSO work prioritized?	SSO work is prioritized with discussion of our HQ Software Assurance lead within OSMA, the internal SSO office lead and the IV&V OOD/SL. External SSO customers bring funding with the work requests.
What percentage of the SAS 2 SOW is dedicated to Mission Protection Services?	Approximately 10-15%
Which areas of the contract does IV&V want to grow?	Our growth is limited to our funding sources.
We are interested in teaming with one of the other prime bidders and wanted to ask if you could give us a little color around the end users' priorities for the next phase of SAS2.	Our priorities remain consistent with the agency's priorities. Ensuring the correctness, safety and security of the agencies mission systems.
Where would they like to see improvements on the parameters listed on slides 9 and 10 of the Overview (Observed Benefits and Metrics)?	Improvements in all areas is of course a goal. We do not want to single out one goal and have others reprioritized.
Are there goals with respect to reducing cyber events further, or additional productivity gains or cost reduction targets?	The reduction of cyber events is a primary goal in security of missions. A balanced portfolio of IV&V and Mission Protection work is archived through risk analysis.
Are there lessons learned from the last phase of this program that the team is looking to improve upon during this phase?	Communication is key. One lesson learned would be more communication to the advanced analyst sooner.