



Memorandum

Date:

To: Josh Pepper, Vice President, Program Management Organization, AJM-0
Rolando Caparas, Vice President, Air Traffic Services, AJT-0
Dan Murphy, Vice President (A), Technical Operations, AJW-0
Randa Hayes, Vice President, Flight Program Operations, AJF-0
LaKisha A. Price, Vice President (A), System Operations Services, AJR-0
Christopher Wilbanks, Vice President (A), Mission Support Services, AJV-0

From: Dale McNeal, Vice President (A), Safety, AJI-0

Prepared by: Maggie Geraghty, Director (A), Policy and Performance, AJI-3

Subject: Aligning ATO Safety Policy with NAS Modernization Efforts

To meet the initiative posed by the Federal Aviation Administration Administrator to accelerate programs supporting the Brand-New Air Traffic Control System, as well as future critical engineering solutions, a scalable safety risk management program is necessary. This will complement new efficient acquisition, development, and implementation practices while upholding rigorous safety standards. ATO Safety (AJI) provides the following key principles that must be met for National Airspace System (NAS) acquisitions and system modifications. Responsible parties may meet these principles as they best see fit for their program or system:

Principle 1: Every program must have a program safety plan documenting its safety risk mitigation strategies.

Principle 2: Prior to issuing the Screening Information Request (SIR), programs must:

- Document potential hazards and their severity based on high-level system functions.
- Identify requirements that will control the risk of such hazards to an acceptable level.
- Assign Functional Development Assurance Levels in line with the methodology in SAE ARP4754B, *Guidelines for Development of Civil Aircraft and Systems*, or an equivalent standard, the latter of which requires a gap analysis.
- Incorporate safety requirements and development assurance levels into the SIR for potential vendors.

Principle 3: Once an acquisition solution has been selected, and before the system is deployed in the NAS, programs must:

- Document potential safety hazards, including likelihood, for solution architecture and NAS modifications, along with risk levels, safety requirements, and monitoring plans
- Ensure that risk is accepted by an accountable FAA official.
- Document the validation and verification of safety requirement implementation prior to system deployment.

Note: Prior to conducting safety assessments under Principle 3, the elements of the solution architecture or NAS modification that are not controlled by specific FAA requirements must be identified and accepted by the Authorizing Official and included as assumptions in the safety documentation.

Independent Operational Assessment (IOA): In addition to the principles listed above, the Independent Safety Assessment Team within AJI will conduct an IOA on any program that is designated through the IOA Designation Process. IOAs are completed independent of the Program Office to provide a system-level evaluation of safety hazards and operational readiness of the program to both FAA decision-makers and the Program Office. IOAs are conducted after initial deployment in live operations while the program continues with the waterfall schedule.

Any questions may be directed to Maggie Geraghty, Acting Director, Policy and Performance, at Maggie.E.Geraghty@faa.gov or (202) 267-9163.