DOI Unmanned Aircraft Systems (UAS) Defense-in-Depth, Layered Data Management Assurance / Security Approach

DOI's defense-in-depth, layered approach to data management assurance/security parallels the Department of Homeland Security (DHS) recommended practices and the same construct used in the operational risk management of aviation safety:

1. Identify the hazard.
2. Analyze the hazard.
3. Make risk decisions.
4. Implement independent controls that together as a layered defense, greatly reduce the probability of the hazard occurring.
5. Monitor and adjust based on documented results.

The illustration to the right depicts some of the layered defense-in-depth security measures DOI employs. Others include policy, training, top-to-bottom personnel accountability, regular external audits, etc.

No DOI UAS connect to the DOI enterprise network

DOI enterprise ability to lock out /deny data sharing with UAS platform, payload, and processing manufacturers

Password encrypted payload link

Password encrypted control link

Benign missions collecting publicly releasable data

Only OAS approved updates

Only OAS authorized UAS