Ground System Architectures Workshop

Session 11D
Cyber Impact of Hosted Payloads

Marke Beasley, Frank Belz, The Aerospace Corporation
• Explore the cyber security and cyber resiliency aspects of missions with hosted payload(s)
  – From the perspectives of both hosting and hosted mission
• For hosted payload approaches
  – What are the security challenges associated with Hosted Payloads?
  – What mitigations will address the security considerations / challenges?
  – What are the business / security risk trade-offs?
  – What are the most significant security enhancements?
  – Looking forward, what are remaining technical, policy, process challenges?
• Discuss relevant activities being conducted by the panelists and participants
Panelists

- Brent Armand, Orbital Sciences Corporation
- Lisa Berenberg, The Aerospace Corporation
- John Nilles, The Aerospace Corporation

Presenters

Working Group Participants will give brief summaries of pertinent ongoing work, e.g.,

- Dr. Daniel Fischer, European Space Agency perspectives
Focus is on cyber issues unique to Hosted Payloads
  - Hosted Payloads represent risk sharing
  - Up front business case alignment is essential
    • Must be compatible with architectural solution
    • Must be codified in contractual agreements
    • Cyber resilience must be part of business case alignment
  - Shared risk affects security approach / solutions
    • Maximizing separation of hosted payload information and control simplifies risk management
      - Depends on alignment of business cases
  - Repeatable tailorable process(es) needed despite uniqueness of business case drivers
    • Need trailblazer successes to build momentum

Good fences make good neighbors
Notional Embedded Commanding and Telemetry Links

- Government Payload Hosted on Commercial Satellite
- Host Encrypted Commanding and Telemetry Links
- Government Payload Operations Control Center (POCC)
- Commercial/Government Network
- Host Teleport
- Host Spacecraft Operations Center (SOC)