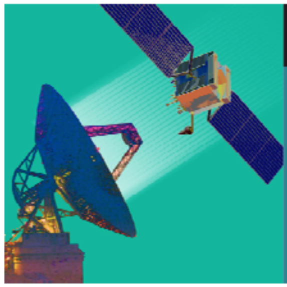
# Working Group Outbrief

## Ground System Architectures Workshop



Session 11B

Cyber Defense in Practice

*DJ Byrne and Bryan Johnson, NASA/Jet Propulsion Laboratory, California Institute of Technology*

# Session Goals

- Benchmarking with peer organizations
- Identification of gaps in existing process
- Keeping relevant over time
- Lessons Learned
- How to engage organization management on cyber defense
- Reasonable/reliable metrics – how do I measure, quantify risk

# Presenters/Panelists

- DJ Byrne – NASA/Jet Propulsion Laboratory, California Institute of Technology
- Bryan Johnson – NASA/Jet Propulsion Laboratory, California Institute of Technology

- Thanks to all workshop attendees that participated in the lively discussion by sharing their experience in this field

# Key Points

- Use standards such NIST SP’s, ISO 27000 series, tailored to meet specific needs.
- Security must be in all phases of a mission or Systems Development Lifecycle (SDLC)
- Review of security events / logs is essential.
  - Break down the review of security events
  - Must review at levels higher than a SysAdmin
- Business cases for cyber remain a challenge
  - Quantitative measures of likelihood continue to be difficult
- Security specific artifacts are required at Milestone Reviews

# Conclusions

- Cyber-threats change rapidly
  - Mitigations have a short half-life
- Full solution to cyber threat problem has not been clearly identified
  - Partial solutions exist
  - Consolidation can, in some cases, increase risk
- Vulnerability assessments must become a standard practice that is also continuous
- Community needs to address information sharing constraints
  - Limits on sharing of lessons learned
  - Limits with shared experiences with commercial solutions (Firewall vendors, Intrusion Detection System vendors, etc.)
  - Our adversaries share more than we do!!!
- Common need for metrics

- We are only as secure as our weakest link.  Is that you?