Cybersecurity

S&MA Trilateral Meeting

June 7, 2018

Kenneth Rehm, NASA IV&V
Donald Ohi, NASA IV&V
Gregory Blaney, NASA IV&V
Topics

• Cybersecurity for Missions
• Policy and Requirements: NIST Cybersecurity Framework
• Communications: CCSDS Security Protocols
• Software: Common Weakness Enumerations
Cybersecurity for Missions

- Cybersecurity needs to address the end-to-end mission system
  - Meeting the cybersecurity challenge requires joint efforts across Project Management, Engineering, Development, V&V, S&MA, Operations & Maintenance, and CIO groups
- Mission cybersecurity assurance needs to leverage existing S&MA processes for safety and reliability
- There are multiple layers to be addressed for mission cybersecurity assurance
  - Agency Policy Layer
  - Communications Layer
  - Software Layer

Mission Systems cannot be safe or reliable if they are not secure
The National Institute of Standards and Technology (NIST) has developed a Cybersecurity Framework (CSF)

Provides a comprehensive structure for making informed, risk-based decisions and managing cybersecurity risks

https://www.nist.gov/cyberframework
Policy Resources are Readily Available

- NIST CSF includes a structured decomposition.
- Categories/Subcategories
- Numerous document references

Need an entity responsible for cyber policy implementation at the Agency level.

Every Agency organization has cybersecurity responsibilities.

Need teams dedicated to independent vulnerability assessments.

https://www.nist.gov/cyberframework
Consultative Committee on Space Data Systems (CCSDS)

- Communications and data systems standards since 1982.
- Includes architecture, archive, security, XML exchange formats.
- End to end data/communications architecture for any mission.

- CCSDC has published numerous guidebooks including standards, protocols, reference architecture

- Security Resources
  - CCSDS 350.1-G-2  Security Threats Against Space Missions
  - CCSDS 350.7-G-1  Security Guide for Mission Planners
  - CCSDS 352.0-B-1  CCSDS Cryptographic Algorithms
  - CCSDS 355.0-R-3  Space Data Link Security Protocol

https://public.ccsds.org
Secure Coding
Common Weakness Enumerations

• The majority of cyber vulnerabilities are found in software.
• Common Weakness Enumeration (CWE) documents code patterns that can result in cyber vulnerabilities.
• The CWE list was compiled by a consortium of government and commercial entities, maintained by MITRE Corporation.

SOFTWARE LAYER

Common Types of Software Weaknesses:
- Buffer Overflows, Format Strings, Etc.
- Structure and Validity Problems
- Common Special Element Manipulations
- Channel and Path Errors
- Handler Errors
- User Interface Errors
- Pathname Traversal and Equivalence Errors
- Authentication Errors
- Resource Management Errors
- Insufficient Verification of Data
- Code Evaluation and Injection
- Randomness and Predictability

Software Quality Assurance should adopt practices that target CWE prevention and removal
- Coding standards, software inspections, and testing
- Commercial and Open Source Static Code Analysis tools are available to help with CWE identification

https://cwe.mitre.org
Summary

- Cybersecurity is a growing risk to space missions.
- S&MA has an important role to play in cybersecurity assurance.
  - S&MA needs to develop cybersecurity expertise to hold mission projects accountable.
  - There are many resources available online to help.
- Cybersecurity assurance requires a multi-disciplinary approach.