November 2017

Space Cyber Framework

How the Space Community Should Approach Cyber Security

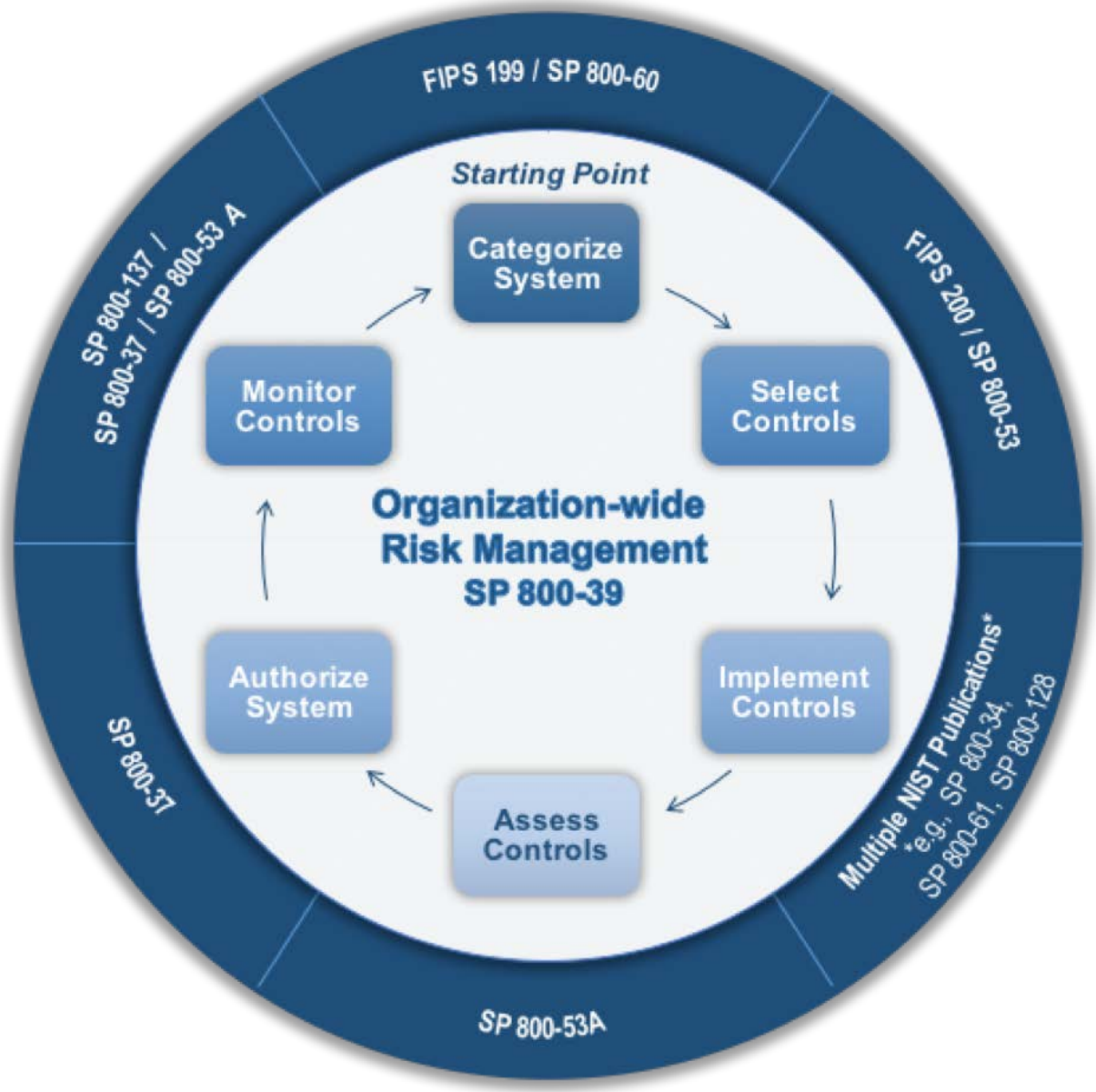
RENAISSANCE STRATEGIC ADVISORS

1300 Wilson Boulevard, Suite 500
Arlington, VA 22209
703-504-9307

Space Cyber Framework Disconnection?

- Space is no different than the rest of the cyber world—the cyber framework for Space exists already
- The NIST Guidance is a great place to start:
  - Risk Management Framework
  - Cyber Security Framework
- Concept of End point security is necessary
- Concept of Mid point security is necessary
- The Space Community must take the threat seriously and implement

The NIST RMF is the start to Securing Space Systems: Assessment all of its Platforms—Space is Critical



The CSF allows the Space Community to methodically evaluate the entirety of the Space Infrastructure

Architectural

- Multi node, Multi mode
- Instrumented for Cyber
- Self-forming & repairing
- Modular & flexible

Satellite

- MultiPath
- Variable Power
- Adaptive Modulation
- Onboard vs Off Board
- Embedded controls and protections

Ground

- Enterprise-wide solutions
- Threat based Isolation
- Common messaging standards
- Encrypted storage

Supply Chain Mgt

Access Mgt

Network Monitoring

Threat Assessment

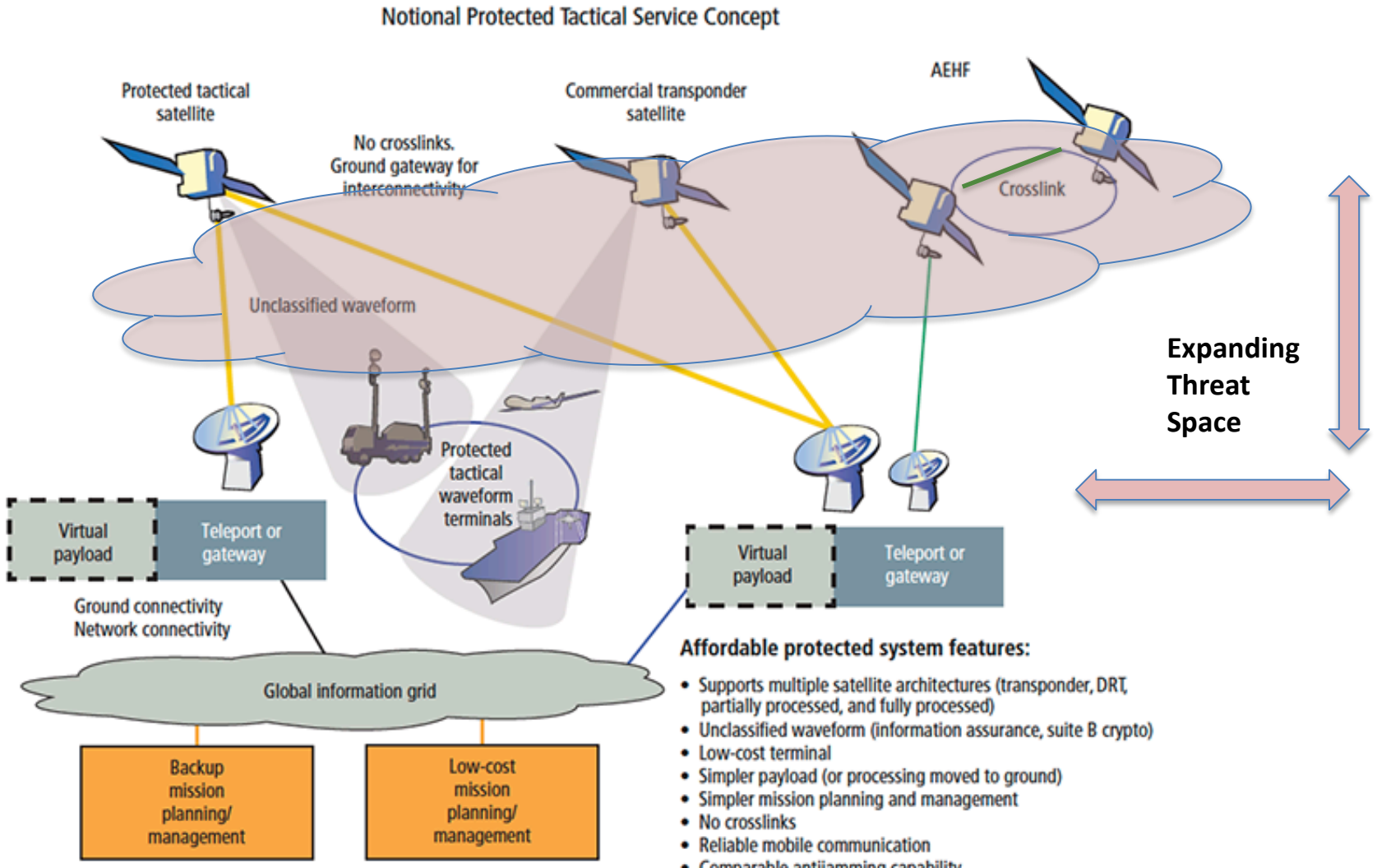
Incident Response

Continuity Of Service Construct

Cyber Resiliency

Almost every major piece end-item hardware should be considered an Endpoint in the Space Community

Midpoint security is a growing threat space that must be considered



Space Cyber Framework Disconnection

- Space Cyber Framework Disconnection = Lack of focus and priority
- The cyber framework for Space exists
- Traditional approaches to Cyber work for Space
- The Space Community must take the threat seriously and implement methodologically
- The USG must make this a priority

Joshua Hartman
JHartman@RSAdvisors.com

1300 Wilson Boulevard, Suite 500
Arlington, VA 22209

222 Broadway, 19th Floor
New York NY 10025

22a St. James's Square
London SW1 4JH