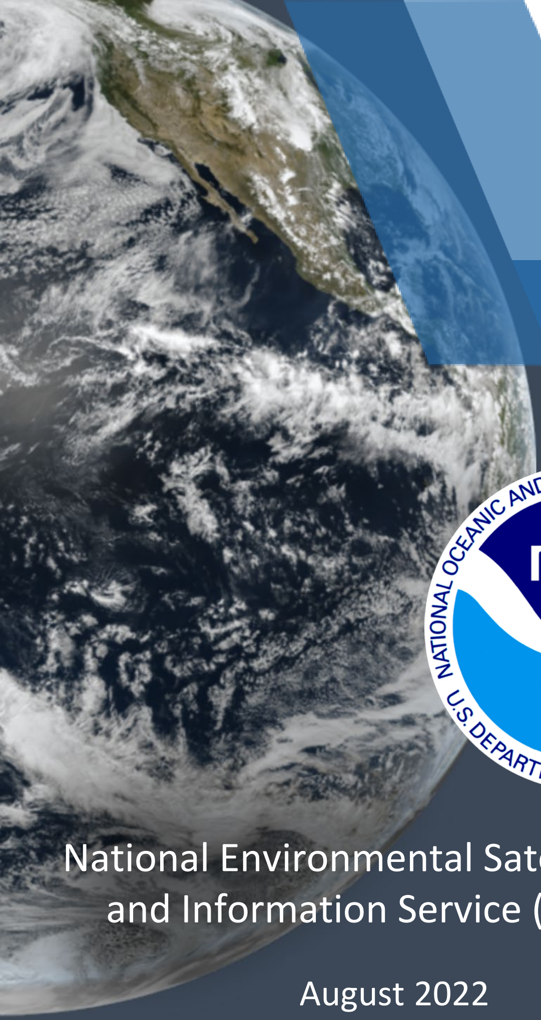

Some observations about cybersecurity and space support systems

Robert Bunge
NESDIS ACIO-S

National Environmental Satellite, Data, and Information Service (NESDIS)

August 2022

Agenda

- The Cyber Threat
- Threat Vectors
- Challenges
- Risk Based Management
- Space/Environmental Challenges
- NIST draft document for cyber security and satellite ground systems
- Questions?

The Threats

- Every day NOAA systems are attacked thousands of times
  - Most are scripted, common tools
  - Exploring, probing
  - Looking for existing, common holes, vulnerabilities
  - Unpatched systems, default passwords
  - Phishing
  - Spear Phishing
  - Ransomware
- State Actors
- Organized groups on behalf of a cause
- Organized crime

(Some of) The Vectors

- Traditional attacks via a network
  - Unpatched servers and network gear
  - Website, public and private, vulnerabilities
  - Email/chat and other communication channel servers/applications
  - Weak/poor encryption
  - Misconfiguration
  - Trust relationships
- Supply Chain Vectors
  - A trusted application is compromised downstream
  - A trusted data flow from a partner is compromised downstream
- Human Vectors
  - Email links, phishing, spearfishing, etc
  - Devices - USB sticks, SD cards, etc
  - Credentials - stolen, guessed, default, etc

Challenges in a Space Environment

- Old apps, old systems, old operating systems
  - Critical applications with dead vendor, can’t be updated to run on new OS
    - Not only is the application a risk
    - The old operating system, perhaps not patched, anymore is a risk
- Unpatched, not updated systems due to operational requirements
  - Systems that are difficult to bring down for patching due to operational requirements
  - Systems that are difficult to patch because of location, no network connectivity, etc.
- Trusted relationships
  - Difficult to interrupt or monitor real time because of latency
  - Difficult to change because of resources/cost

Risk Based Management

- Pick a Framework; there are many; How the US government (mostly) does this:
- FISMA/NIST 800.53
  - "Systems" are identified and tracked
  - Each System has an assigned Information System Security Officer
  - Each has a System Owner (SO) who answers to:
  - Each system has an Authorizing Official (AO) who is a Senior Executive Service (SES)
    - Security performance of the system impacts annual bonus potential
- ISSO and SO document known risks. AO's accept those risks or ID resources to fix
- Each system is independently audited annually and briefed to AO
  - New risks are tracked through an established systems (POA&M)
- The AO accepts and issues an authority to operate (usually for one year)

Space/Environment Industry Challenges

- Environmental Scientists can never have enough data!
  - Pressure to keep that satellite flying for as long as it is working
- Feeding environmental operational models leads to support life/property decisions
  - In risk frameworks, that leads to a higher level of cyber standards
- Challenges in updating old ground systems while maintaining an operational tempo
- Space Based Environmental platforms may encounter some specific threat vectors in the now or in the future
  - Military/disaster operations depend on environmental data
  - Perhaps a threat to a platform for political, military, even terrorism purposes
  - Perhaps a data poison approach to impact downstream products
  - Perhaps a poison pill to impact AI training sets to trigger AI system failures

Applying Cyber Framework to Satellite Ground Systems

- National Institute of Standards and Technology (NIST) has developed a document for applying cyber security framework to assure satellite command and control
  - NISTIR 8401
  - Published April, 22, Comment period is closed
- https://csrc.nist.gov/publications/detail/nistir/8401/draft

Questions?

Bob Bunge

NESDIS ACIO-S

robert.bunge@noaa.gov