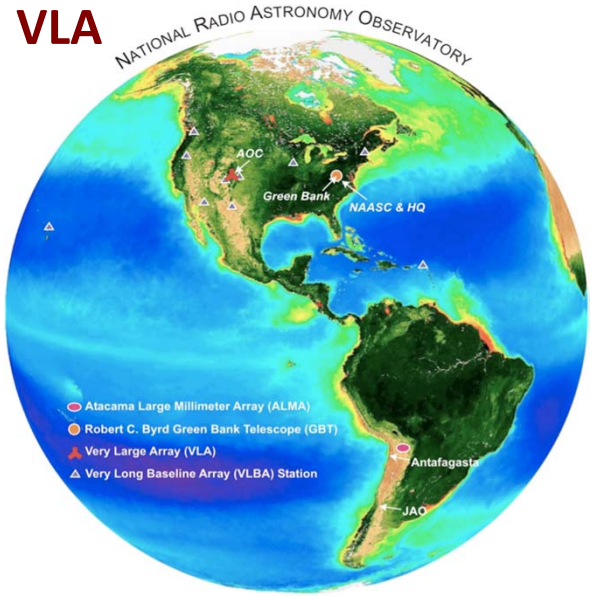
David Halstead, CIO
Pat Murphy, CSO
NRAO

Jansky VLA



GBT

X10 VLBA

ALMA

The National Radio Astronomy Observatory operates a complementary suite of powerful telescopes for exploring the Universe at radio wavelengths

What are the top three information security threats to Large Facilities and CI, in terms of likelihood/frequency?

1. That Information Services will be responsible for setting institutional policy rather than implementing it!
    - "Safe & appropriate workplace conduct" items should be covered by institutions employee/supervisor manual (visitors are a challenge!)
2. Lack of awareness resulting in inappropriate access to systems & information
    A. Phishing for username/password.
    B. Compromised/malicious web sites
    C. Lack of accountability (by owner) on information sensitivity categorization
3. Targeted Advanced Persistent Threat (highly sophisticated/state-sponsored actor.)
4. Misalignment between physical and cyber security.

Who are the likely threat actors?

1. Management, HR, funding agencies
2. Nation States looking for Intellectual Property e.g. Export Controlled Designs
3. Organized crime
4. Recreational Black Hats (historical)/ leap-frog through our CI

What types of attacks / vectors?

1. Reaction to unacceptable staff/user behavior.
2. Phishing: bulk, spear, whale.
3. Exposed services with Zero day and known vulnerabilities.
4. Partner (non-NRAO) compromised system with shared passwords/trusted keys.

What are the top three threats in terms of potential damage to the science mission?

1. Distraction from supporting science:

   e.g. when an astronomy conference was held in China, IS ended up driving travel safety training!

2. Page 1 news: loss of funding/reputation.
3. “Deemed export” of sensitive/valuable design information: Loss of revenue.
4. Corruption of data products/loss of provenance.