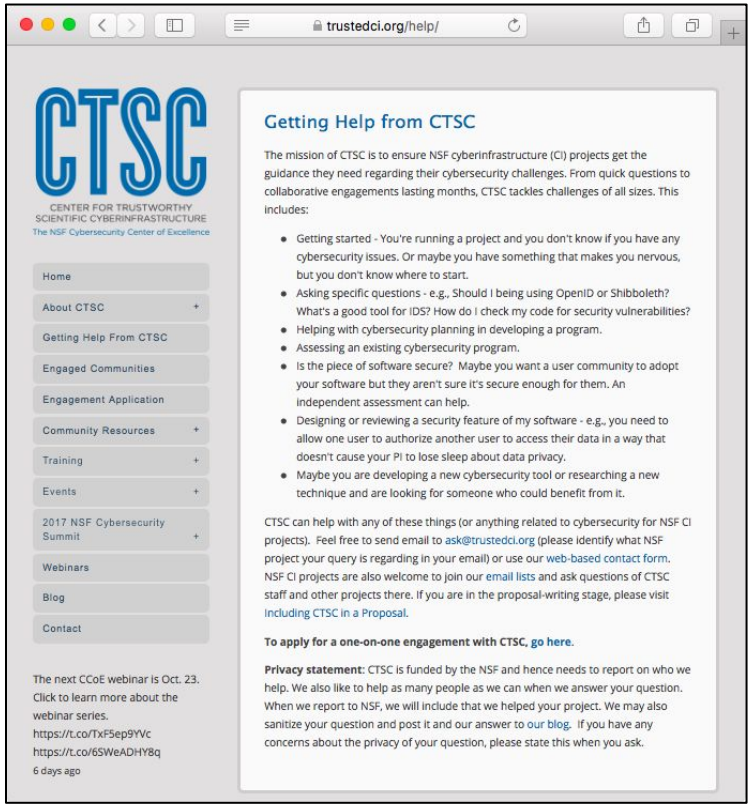
Example CTSC Engagements

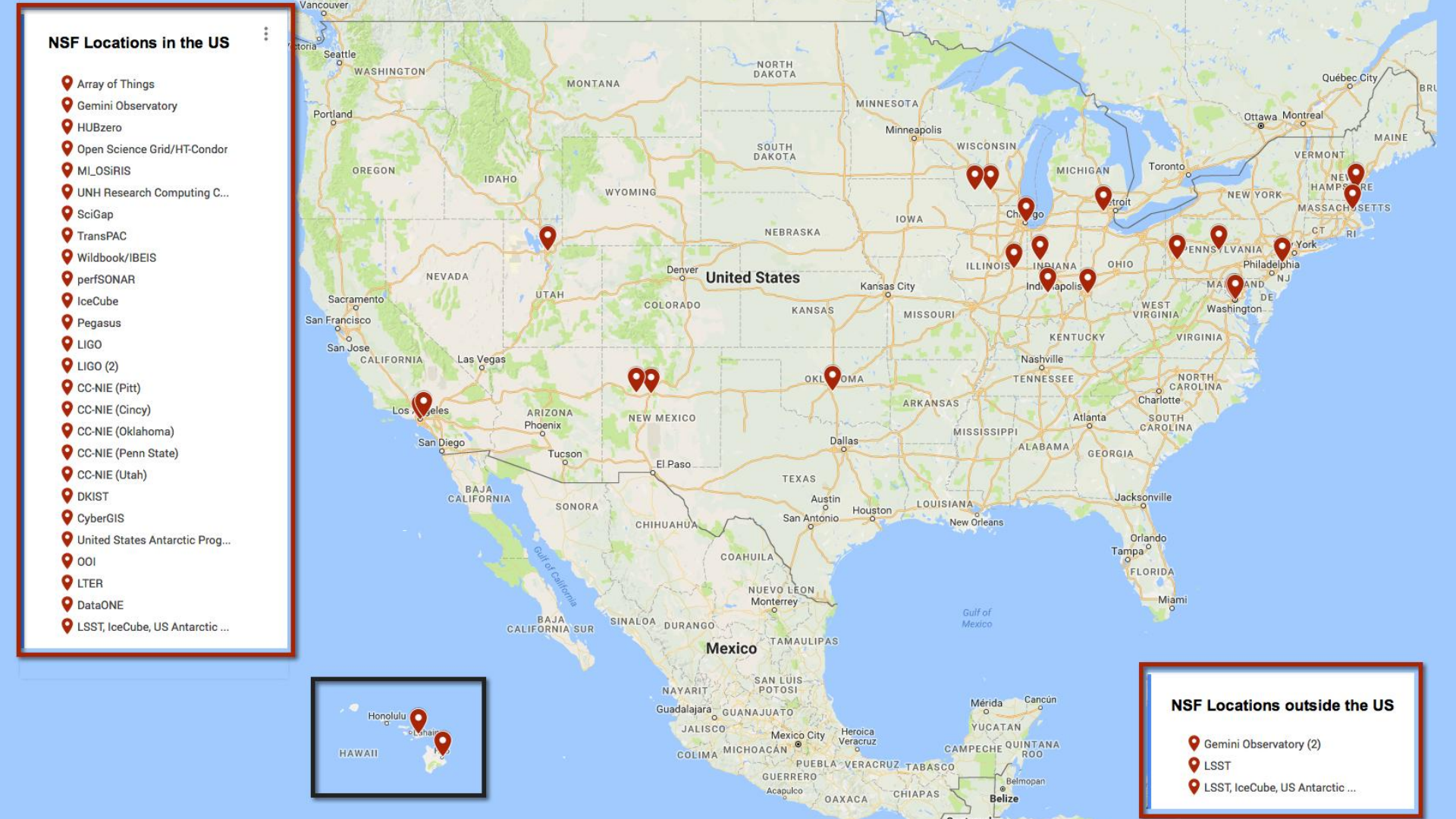
Kay Avila, Jim Basney, and John Zage

This material is based upon work supported by the National Science Foundation under grant number 1547272. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

CTSC Engagements

- Goal: Work collaboratively with NSF projects to address cybersecurity challenges
- Topics:
  - development of new cybersecurity programs
  - assessing existing cybersecurity programs
  - software assurance
  - identity management
  - recommendations on new software features
  - code review
  - staff training
  - implementing a specific process or control



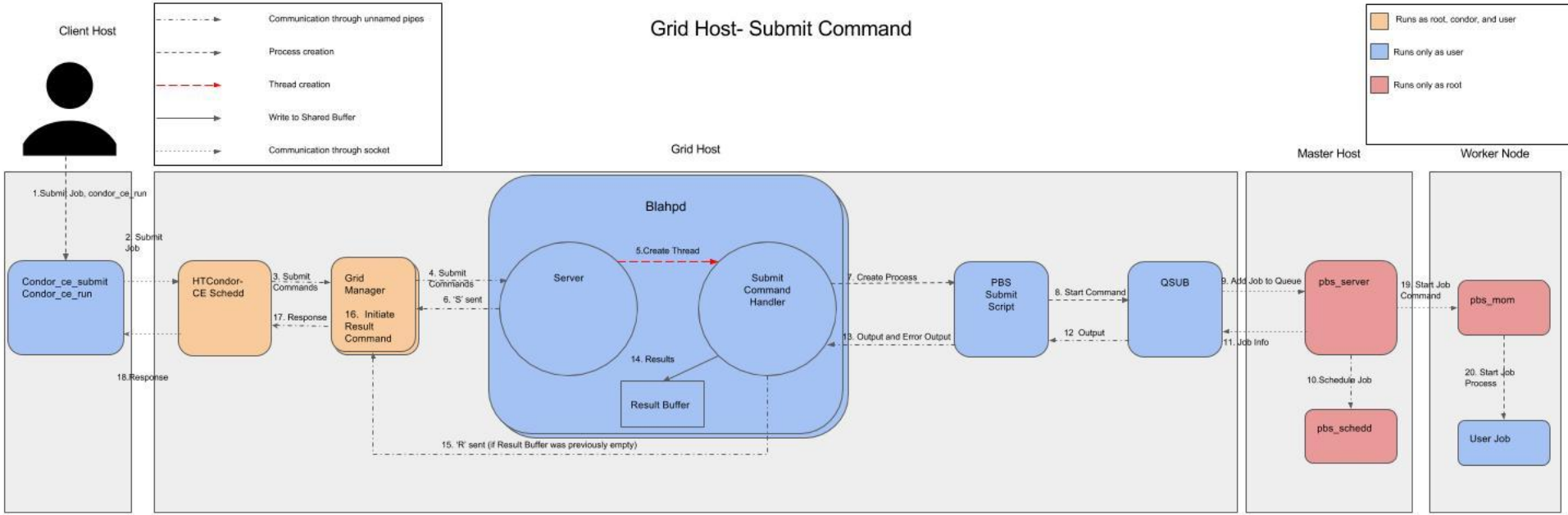

NSF Locations in the US
Array of Things
Gemini Observatory
HUBzero
Open Science Grid/HT-Condor
MI_OSiRIS
UNH Research Computing C...
SciGap
TransPAC
Wildbook/IBEIS
perfSONAR
IceCube
Pegasus
LIGO
LIGO (2)
CC-NIE (Pitt)
CC-NIE (Cincy)
CC-NIE (Oklahoma)
CC-NIE (Penn State)
CC-NIE (Utah)
DKIST
CyberGIS
United States Antarctic Prog...
OOI
LTER
DataONE
LSST, IceCube, US Antarctic ...
United States
Mexico
HAWAII
NSF Locations outside the US
Gemini Observatory (2)
LSST
LSST, IceCube, US Antarctic ...

HTCondor/OSG

- HTCondor-CE is a next-generation gateway software for the OSG
  - Allows local providers to accept jobs submitted from OSG users
- Open Science Grid (OSG) is a national distributed partnership for data-intensive science
- Goal: analyze a lesser-known component of HTCondor-CE, called blahp, for security vulnerabilities using a first principles vulnerability analysis (FPVA) approach

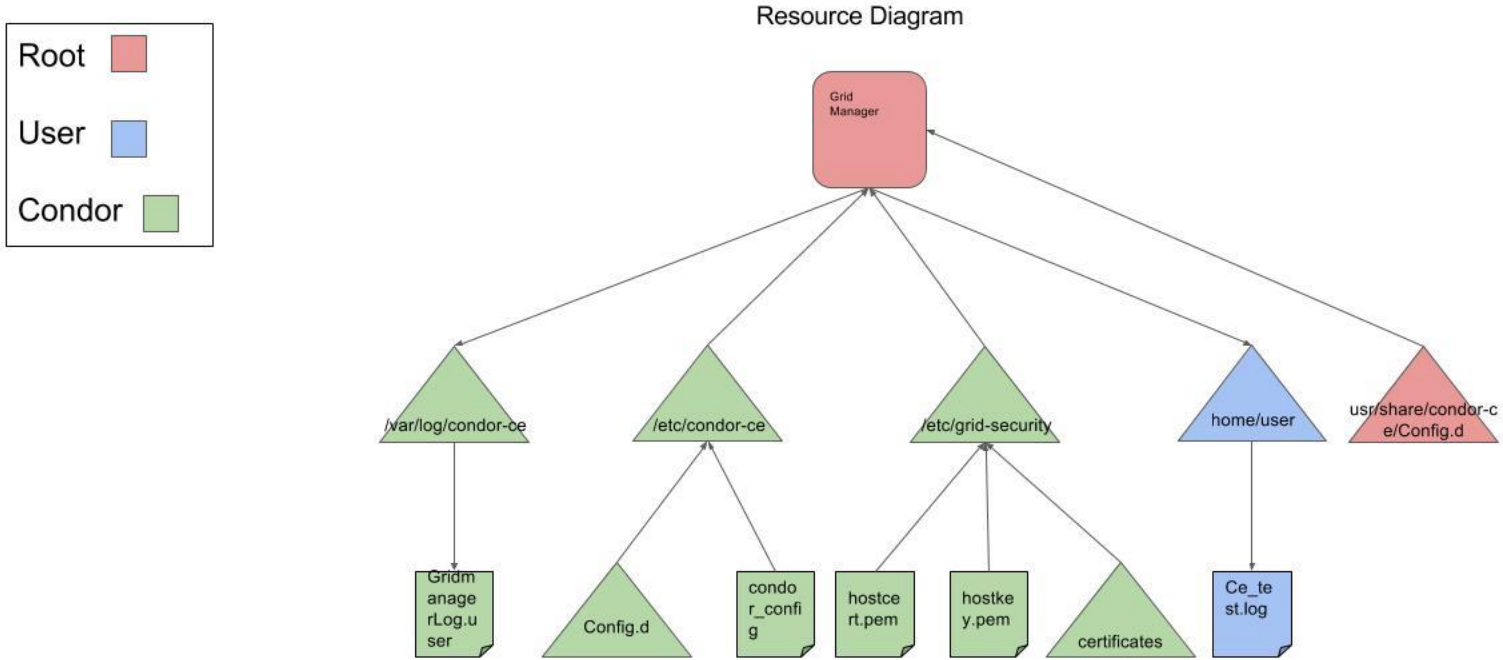
HTCondor/OSG

- FPVA: Starts with Architecture Diagram



HTCondor/OSG

- FPVA: Then moves onto the Resource Diagram

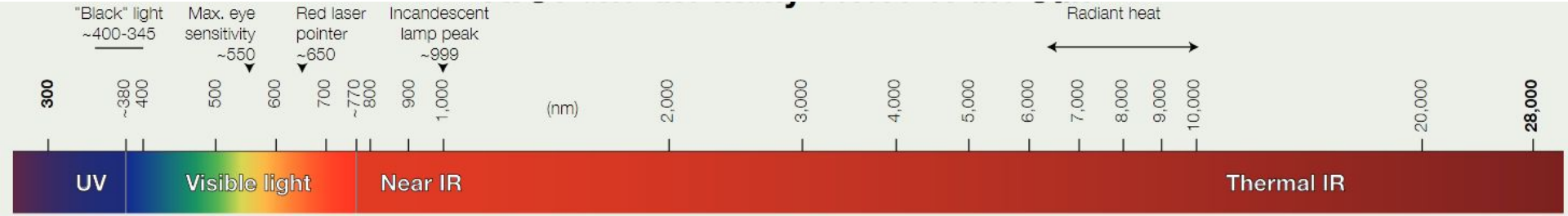


HTCondor/OSG

- FPVA: After these two steps:
  - Analyze possible attack surface
  - Write up possible scenario
  - Test scenario
  - Record our conclusions, then repeat with next scenario

Daniel K. Inouye Solar Telescope (DKIST)

- Project of NSO, under AURA, funded by NSF
- Currently under construction in Maui, Hawaii
- Will become the largest and most precise solar telescope upon completion in 2019
- Expected to produce 9 TB/day of data on average, peaking up to 64 TB/day
- Approximately 50 year lifetime
- Date being stored at a data center in Boulder, Colorado



DKIST Data Center CTSC Engagement

- Objectives
  - Primary - develop a security program for the DKIST Data Center in Colorado
  - Secondary - teach DKIST Data Center staff how to perform a risk assessment using an information asset inventory
- Steps
  - Understand the current state of the data center buildout
  - Review existing policy requirements from the University of Colorado, National Solar Observatory (NSO) and Association of Universities for Research in Astronomy (AURA)
  - Begin with CTSC's **Guide** and **Master Information Security Policy & Procedures**
  - On-site visit to cover risk assessments

OSiRIS - www.osris.org

- 5yr $5m NSF sponsored project
  - Campus Cyberinfrastructure Data, Networking, and Innovation (CC*DNI)
  - Data Infrastructure Building Blocks (DIBBs)
- Providing a distributed, multi-institutional storage infrastructure to allow researchers to read, write, manage and share their data directly from their computing facility locations
- Using ceph.com distributed storage system
- Challenge: access control to data across campuses

OSiRIS - www.osris.org

- CTSC and OSiRIS collaborated on a review of their data authorization design which uses JSON Web Tokens (JWTs)
- Using the OAuth 2.0 Threat Model and Security Considerations (RFC 6819) as a framework for the review
  - user authentication process
  - JWT issuance process
  - exposure of JWTs after issuance
  - malicious client software
  - browser-based attacks
  - malicious resource providers
  - denial of service attacks
- Final report: http://hdl.handle.net/2022/21307

More info at https://trustedci.org/