

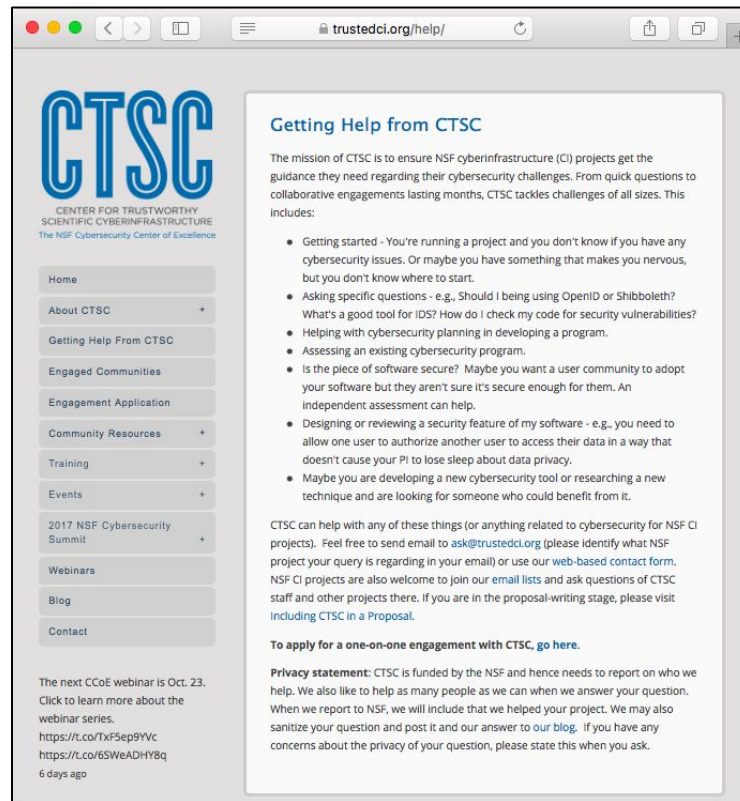
Example CTSC Engagements

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



The screenshot shows a web browser window with the URL trustedci.org/help/. The page features the CTSC logo (Center for Trustworthy Scientific Cyberinfrastructure) and a navigation menu on the left with items like Home, About CTSC, Getting Help From CTSC, Engaged Communities, Engagement Application, Community Resources, Training, Events, 2017 NSF Cybersecurity Summit, Webinars, Blog, and Contact. The main content area is titled "Getting Help from CTSC" and explains the mission of CTSC to ensure NSF cyberinfrastructure (CI) projects get guidance. It lists several types of help available, such as getting started, asking specific questions, and assessing existing programs. A "Privacy statement" section is also present at the bottom.

Getting Help from CTSC

The mission of CTSC is to ensure NSF cyberinfrastructure (CI) projects get the guidance they need regarding their cybersecurity challenges. From quick questions to collaborative engagements lasting months, CTSC tackles challenges of all sizes. This includes:

- Getting started - You're running a project and you don't know if you have any cybersecurity issues. Or maybe you have something that makes you nervous, but you don't know where to start.
- Asking specific questions - e.g., Should I be using OpenID or Shibboleth? What's a good tool for IDS? How do I check my code for security vulnerabilities?
- Helping with cybersecurity planning in developing a program.
- Assessing an existing cybersecurity program.
- Is the piece of software secure? Maybe you want a user community to adopt your software but they aren't sure it's secure enough for them. An independent assessment can help.
- Designing or reviewing a security feature of my software - e.g., you need to allow one user to authorize another user to access their data in a way that doesn't cause your PI to lose sleep about data privacy.
- Maybe you are developing a new cybersecurity tool or researching a new technique and are looking for someone who could benefit from it.

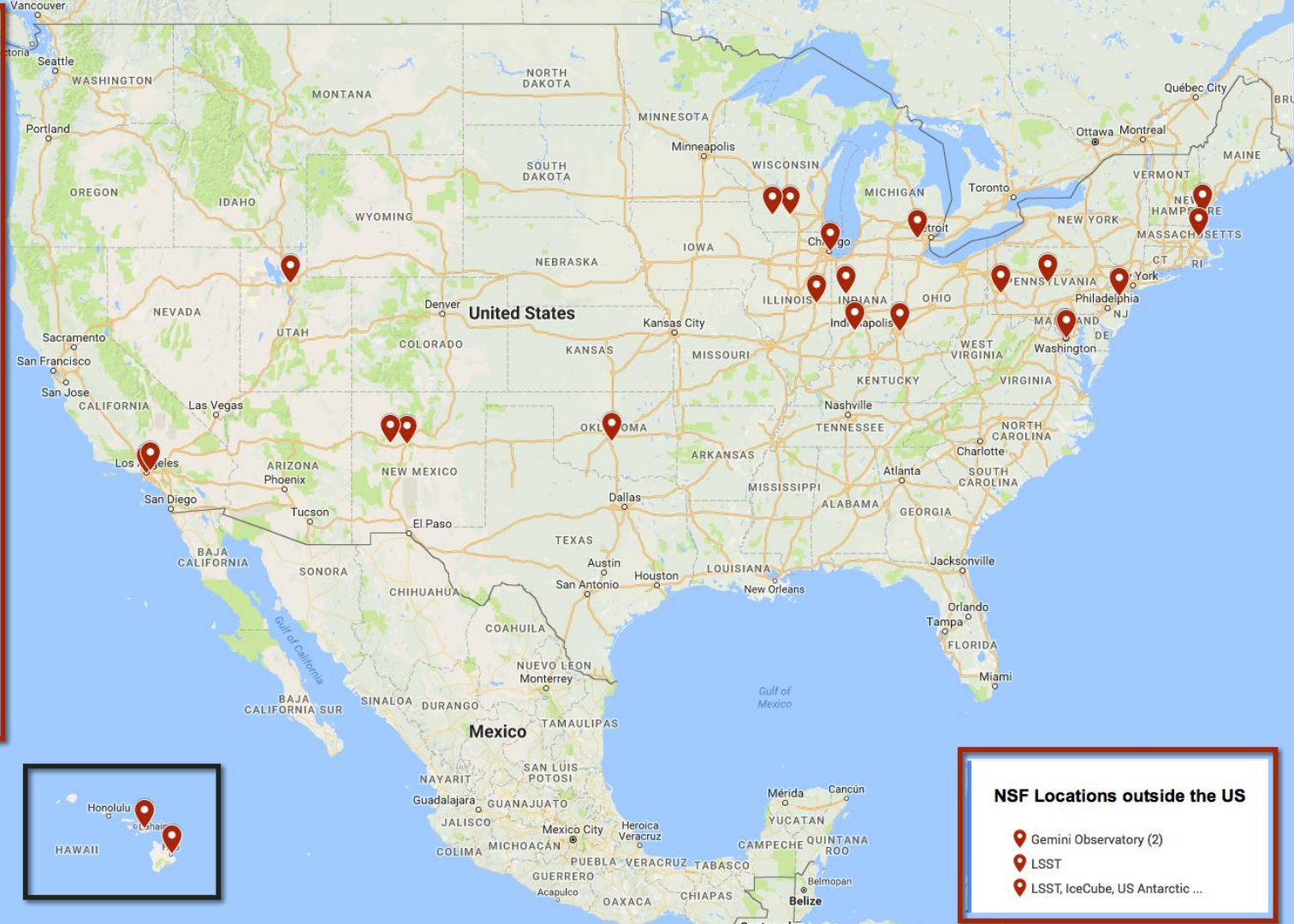
CTSC can help with any of these things (or anything related to cybersecurity for NSF CI projects). Feel free to send email to ask@trustedci.org (please identify what NSF project your query is regarding in your email) or use our [web-based contact form](#). NSF CI projects are also welcome to join our [email lists](#) and ask questions of CTSC staff and other projects there. If you are in the proposal-writing stage, please visit [including CTSC in a Proposal](#).

To apply for a one-on-one engagement with CTSC, [go here](#).

Privacy statement: CTSC is funded by the NSF and hence needs to report on who we help. We also like to help as many people as we can when we answer your question. When we report to NSF, we will include that we helped your project. We may also sanitize your question and post it and our answer to our [blog](#). If you have any concerns about the privacy of your question, please state this when you ask.

NSF Locations in the US

- Array of Things
- Gemini Observatory
- HUBzero
- Open Science Grid/HT-Condor
- ML_OSIRIS
- UNH Research Computing C...
- SciGap
- TransPAC
- Wildbook/IBEIS
- perFONAR
- 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 ...



NSF Locations outside the US

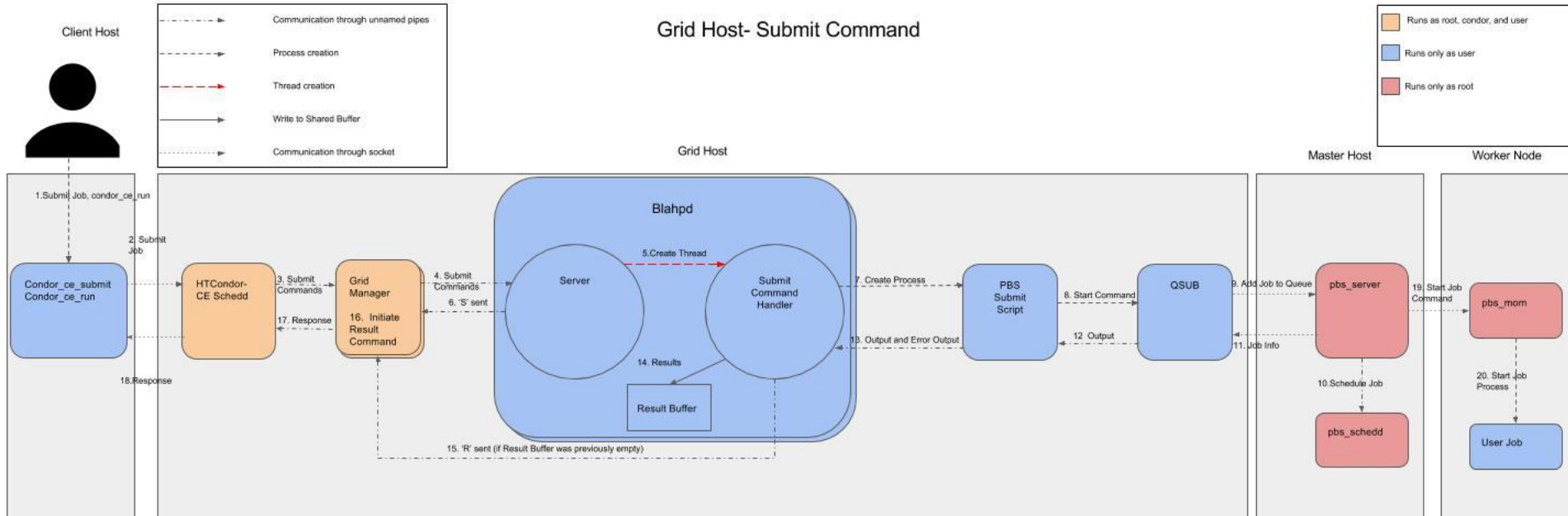
- Gemini Observatory (2)
- LSST
- LSST, IceCube, US Antarctic ...

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

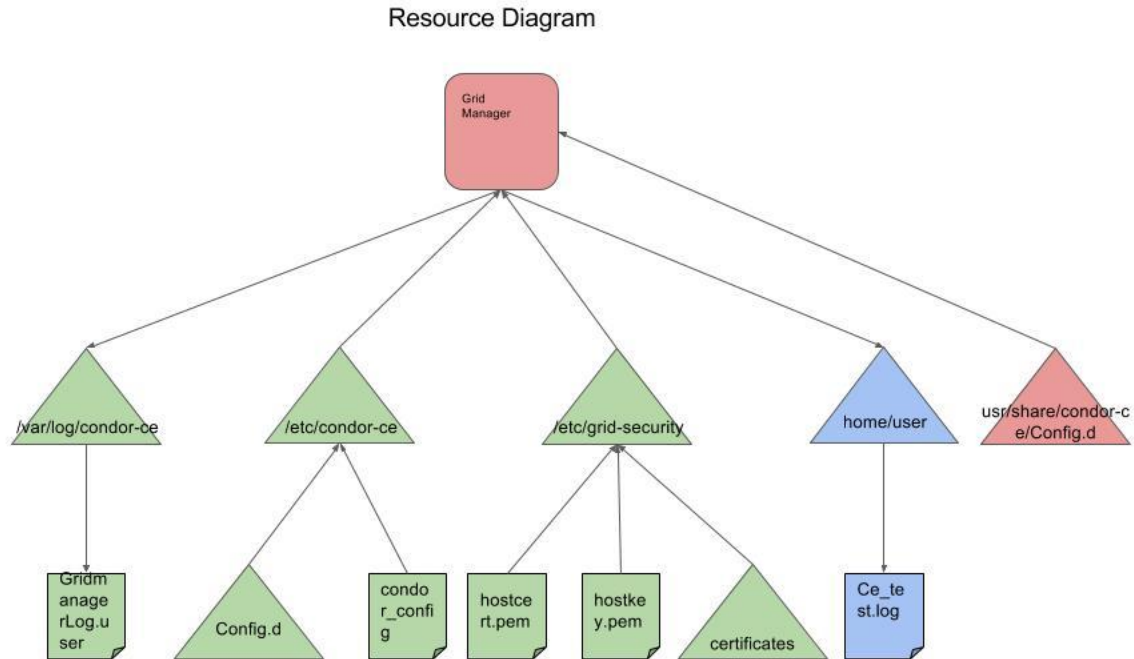
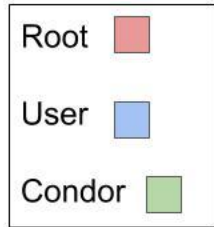
HTCondor/OSG

- FPVA: Starts with Architecture Diagram



HTCondor/OSG

- FPVA: Then moves onto the Resource Diagram

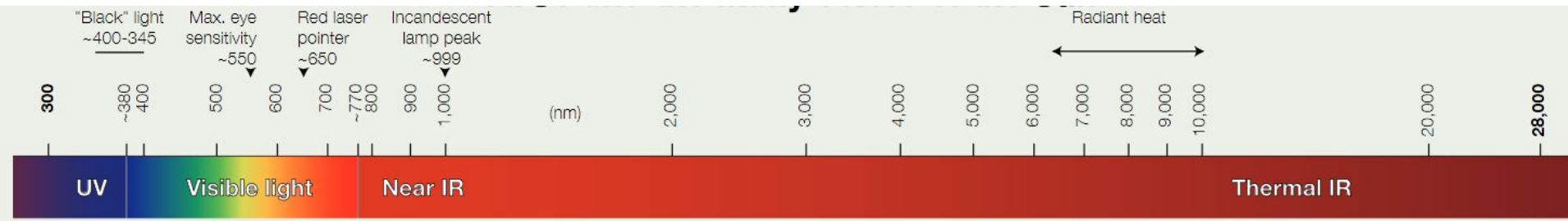


HTCondor/OSG

- 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
- Data 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



Open Storage Research Infrastructure

- ❑ 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/>