

# Developing Cybersecurity Programs for Large Facilities – DKIST & Trusted CI

**Jim Marsteller**  
Trusted CI Co-PI

Envisioning the Future of Facility Science & Cyberinfrastructure

April 5<sup>th</sup>, 2019

Austin

# Developing Cybersecurity Programs for Large Facilities

Bret Goodrich, Senior Software Engineer of the Daniel K Inouye Solar Telescope (DKIST) was tasked with developing a cybersecurity program for his facility. At the time there was no framework tailored to NSF cyberinfrastructure (CI). Bret approached Trusted CI for assistance. After some initial discussions, DKIST and Trusted CI began a six month process to create a guide for developing cybersecurity programs crafted to NSF CI community. At the completion of this effort the collaboration produced the most comprehensive set of security resources specially for the CI community.

## Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects

- Risk based framework influenced by NIST 800 Series
- Tailored to NSF Large Facilities
- Step-by-step processes: identify assets, baseline security controls, risk management, program evaluation
- 18 supporting documents: policy templates, data classification, risk assessment tools and more

Details: [trustedci.org/guide](https://trustedci.org/guide)



# Trusted CI can help

Contact us to request help, from small questions to month-long engagements:

<https://trustedci.org/help/>

See also:

<https://trustedci.org/situational-awareness/>

<https://trustedci.org/webinars/>

<https://trustedci.org/ctsc-email-lists/>

<http://blog.trustedci.org/>

@TrustedCI 



Trusted CI, the NSF Cybersecurity Center of Excellence is supported by the National Science Foundation under Grant ACI-1547272. The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.