A Brief Update from Trusted CI

Jim Basney
Director and PI, Trusted CI
jbasney@ncsa.illinois.edu

CI4MF
January 17, 2024

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Trusted CI:
The NSF Cybersecurity Center of Excellence

Our mission: to lead in the development of an NSF Cybersecurity Ecosystem with the workforce, knowledge, processes, and cyberinfrastructure that enables trustworthy science and NSF's vision of a nation that is a global leader in research and innovation.

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

NCSA

PSC
PITTSBURGH SUPERCOMPUTING CENTER

BERKELEY LAB

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

https://trustedci.org/

Trustworthy Cyberinfrastructure

Cyberinfrastructure is essential to scientific discovery.

Scientists trust that cyberinfrastructure …

is accessible and available.

provides well-defined accuracy and integrity.

implements appropriate data embargoes and protections.

complies with applicable obligations and regulations.

Effective cybersecurity programs address threats and build trust.

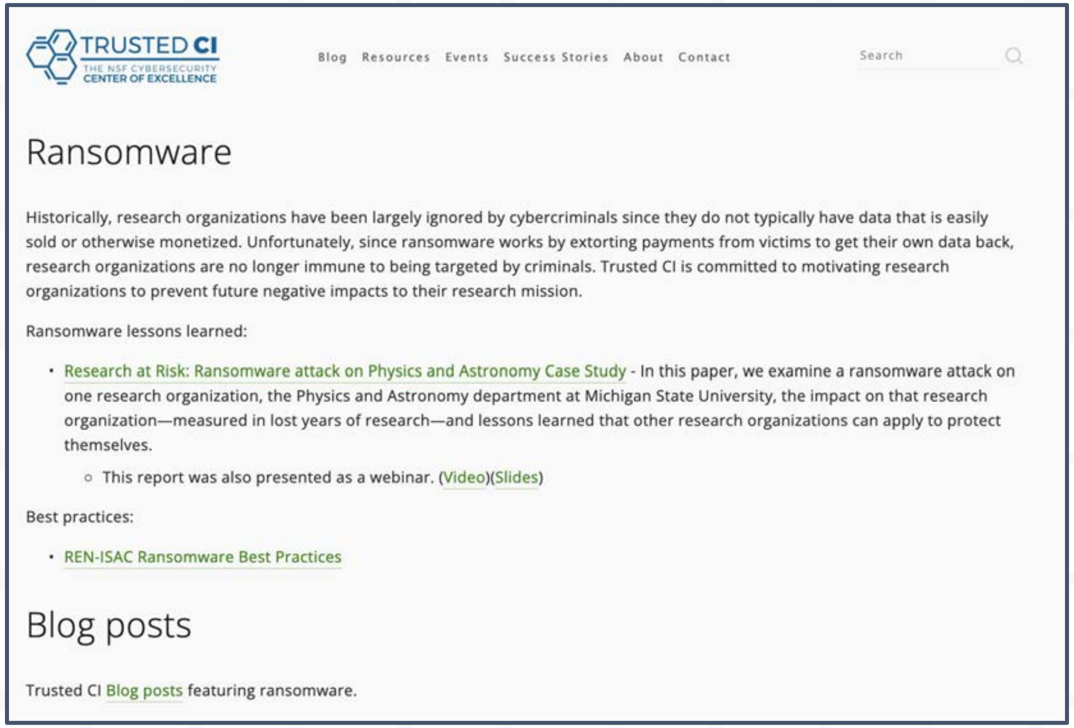
Ongoing Ransomware Risk to Science

Ransomware has changed the cybercrime landscape, broadly expanding potential victims to include hospitals, schools, cities, and researchers.

Trusted CI is warning researchers to take the risk seriously and be prepared for business continuity and extortion attacks.

We are collecting research-focused resources:

https://www.trustedci.org/ransomware


TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE
Blog Resources Events Success Stories About Contact
Search

Ransomware

Historically, research organizations have been largely ignored by cybercriminals since they do not typically have data that is easily sold or otherwise monetized. Unfortunately, since ransomware works by extorting payments from victims to get their own data back, research organizations are no longer immune to being targeted by criminals. Trusted CI is committed to motivating research organizations to prevent future negative impacts to their research mission.

Ransomware lessons learned:

- Research at Risk: Ransomware attack on Physics and Astronomy Case Study - In this paper, we examine a ransomware attack on one research organization, the Physics and Astronomy department at Michigan State University, the impact on that research organization—measured in lost years of research—and lessons learned that other research organizations can apply to protect themselves.
  - This report was also presented as a webinar. (Video)(Slides)

Best practices:

- REN-ISAC Ransomware Best Practices

Blog posts

Trusted CI Blog posts featuring ransomware.

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Operational Technology Security

- The 2022 Annual Challenge investigated Operational Technology (OT) at NSF Major Research facilities
- OT: networked systems connected to computing systems on one side and controls or sensors of physical systems on the other side.
- NSF MF OT: both scientific instruments (e.g., telescopes) and COTS components (e.g., HVAC, power, propulsion)
- Annual Challenge team engaged with IT and OT personnel discussing operations at five NSF Major Facilities.
- 2 reports published with findings and recommendations

U.S. Antarctic Program

ICECUBE NEUTRINO OBSERVATORY

NOIR Lab

U.S. Academic Research Fleet

UNOLS

OOI OCEAN OBSERVATORIES INITIATIVE

TRUSTED CI THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://blog.trustedci.org/2022/11/publication-of-trusted-ci-roadmap-for.html

2023 Annual Challenge: Security by Design of NSF Major Facilities

- NSF MFs deploy operational technology that can have an operational lifetime of 15-30 years.
- Typically no cybersecurity requirements during acquisition and design.
- Trusted CI is engaging with NSF MFs undergoing construction to build security into from the outset.
- 2023 is particularly focusing on the academic maritime and polar domains.
  - Support acceptance testing of the NSF-funded Research Class Research Vessels (RCRVs) at Oregon State University,
  - Support Scripps Institution of Oceanography's design of the California Coastal Research Vessel (CCRV).
  - Support the Ocean Observing Initiative (OOI)'s refresh of its fleet of 351 gliders and other underwater autonomous vehicles (AUVs)
  - Engage with the U.S. Antarctic Program (USAP)'s design of the Antarctic Research Vessel (ARV) and refresh of McMurdo, Palmer, and Amundsen-Scott South Pole Stations

U.S. Antarctic Program

OCEAN OBSERVATORIES INITIATIVE

U.S. Academic Research Fleet

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

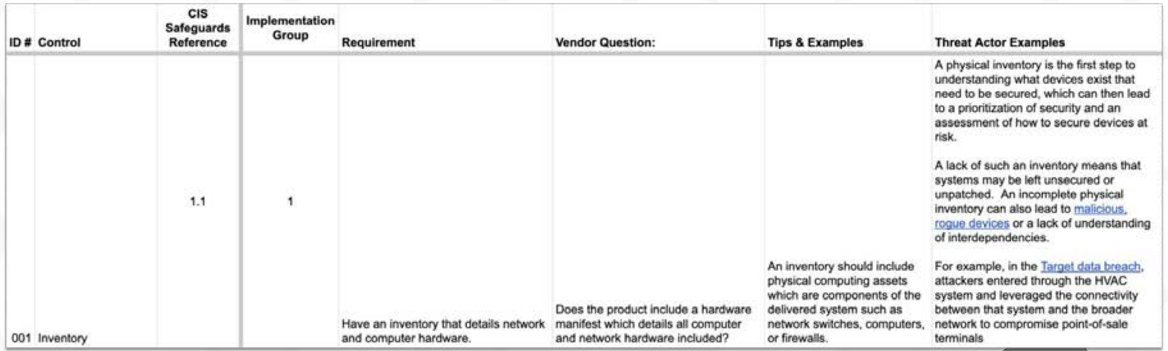
https://blog.trustedci.org/2023/01/announcing-2023-trusted-ci-annual.html

Now Available: OT Procurement Vendor Matrix

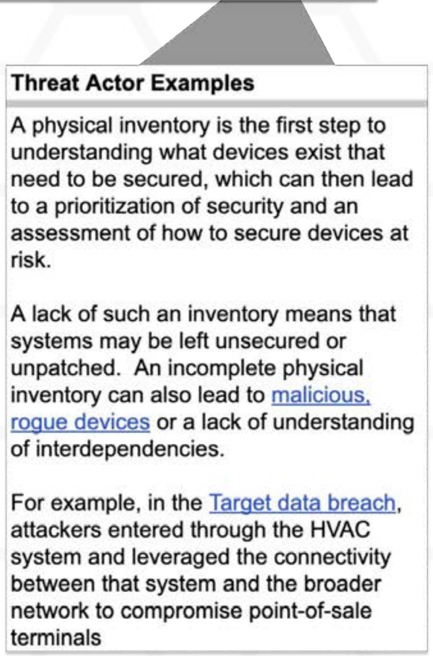
The matrix includes a list of security controls, requirements for the control, potential questions for vendors, and real world examples justifying a given control.

With input from CCRV, RCRV, and OOI representatives.

https://doi.org/k8wf



ID #	Control	CIS Safeguards Reference	Implementation Group	Requirement	Vendor Question:	Tips & Examples	Threat Actor Examples
001	Inventory	1.1	1	Have an inventory that details network and computer hardware.	Does the product include a hardware manifest which details all computer and network hardware included?	An inventory should include physical computing assets which are components of the delivered system such as network switches, computers, or firewalls.	A physical inventory is the first step to understanding what devices exist that need to be secured, which can then lead to a prioritization of security and an assessment of how to secure devices at risk. A lack of such an inventory means that systems may be left unsecured or unpatched. An incomplete physical inventory can also lead to malicious, rogue devices or a lack of understanding of interdependencies. For example, in the Target data breach, attackers entered through the HVAC system and leveraged the connectivity between that system and the broader network to compromise point-of-sale terminals

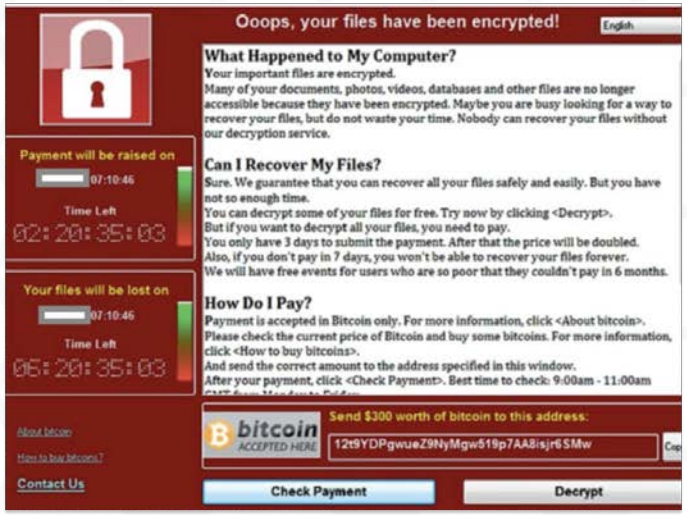


Threat Actor Examples

A physical inventory is the first step to understanding what devices exist that need to be secured, which can then lead to a prioritization of security and an assessment of how to secure devices at risk.

A lack of such an inventory means that systems may be left unsecured or unpatched. An incomplete physical inventory can also lead to malicious, rogue devices or a lack of understanding of interdependencies.

For example, in the Target data breach, attackers entered through the HVAC system and leveraged the connectivity between that system and the broader network to compromise point-of-sale terminals



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
07:10:46
Time Left
02:20:35:03

Your files will be lost on
07:10:46
Time Left
06:20:35:03

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Image source: Elradi, Mohammed & Mohamed, Hashim & Ali, Mohammed. (2021). Ransomware Attack: Rescue-checklist Cyber Security Awareness Program. Artificial Intelligence Advances. 3. 10.30564/aia.v3i1.3162.

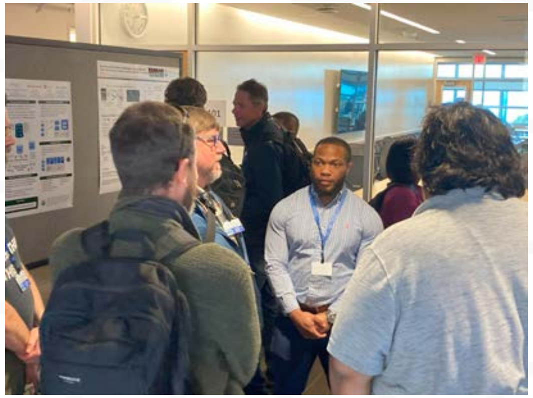
TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Annual NSF Cybersecurity Summit

Training, workshops, and plenary sessions

October 24-26, 2023 at Lawrence Berkeley National Laboratory in Berkeley, CA

October 7-10, 2024 at Carnegie Mellon University in Pittsburgh, PA (tentative)



https://trustedci.org/summit/

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

The Trusted CI Framework

https://trustedci.org/framework

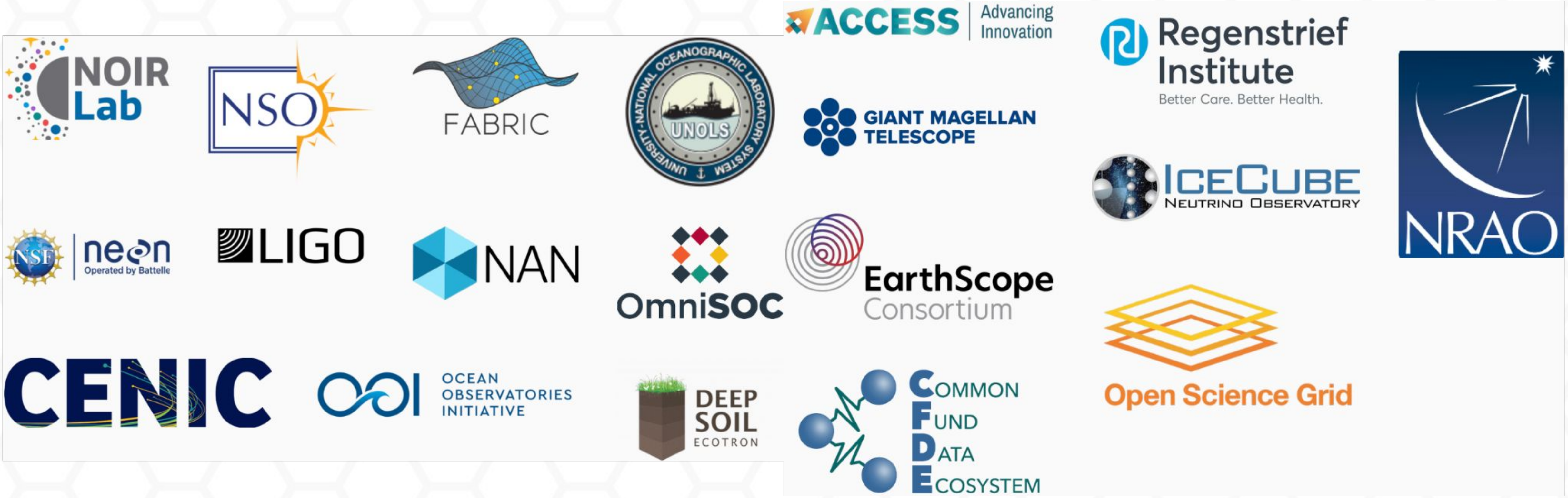
Framework Core:

- Concise, clear minimum requirements for cybersecurity programs organized under the 4 Pillars: Mission Alignment, Governance, Resources, and Controls
- Based in general cybersecurity best practice and evidence of what works.

Framework Implementation Guide:

- Guidance vetted by and tailored to the open science community.
- Curated pointers to the very best resources and tools.

Framework Adopters



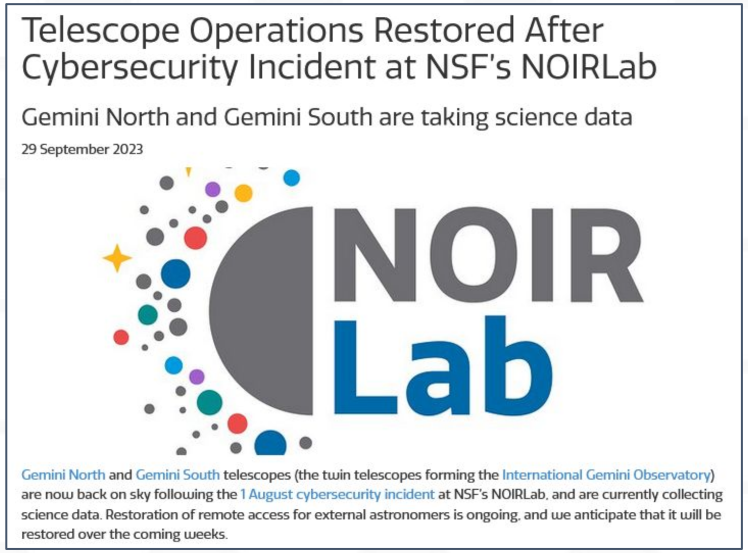
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://www.trustedci.org/framework

Research Infrastructure Security Community

A cybersecurity-focused community of practice built from the practitioners who have successfully completed a Framework Cohort engagement.

Working together to address threats to research facilities.

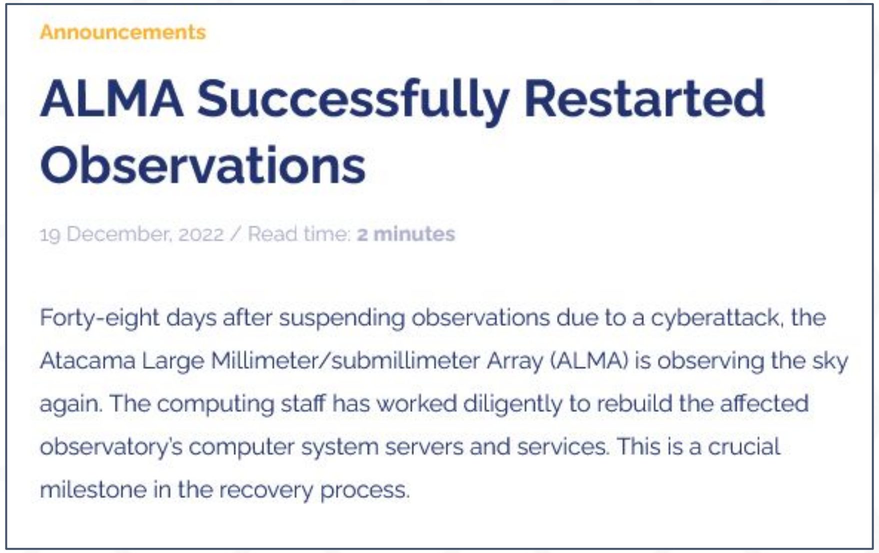


Telescope Operations Restored After Cybersecurity Incident at NSF's NOIRLab

Gemini North and Gemini South are taking science data

29 September 2023

Gemini North and Gemini South telescopes (the twin telescopes forming the International Gemini Observatory) are now back on sky following the 1 August cybersecurity incident at NSF's NOIRLab, and are currently collecting science data. Restoration of remote access for external astronomers is ongoing, and we anticipate that it will be restored over the coming weeks.



Announcements

ALMA Successfully Restarted Observations

19 December, 2022 / Read time: **2 minutes**

Forty-eight days after suspending observations due to a cyberattack, the Atacama Large Millimeter/submillimeter Array (ALMA) is observing the sky again. The computing staff has worked diligently to rebuild the affected observatory's computer system servers and services. This is a crucial milestone in the recovery process.

CI Compass and Trusted CI

- CoEs collaborating to support the NSF science community
- Sharing CoE best practices and lessons learned
- With standing and open communication and collaboration channels

Recent Collaborations:

- Research Infrastructure Workshop planning
- Antarctic Research Vessel requirements gathering
- Student program planning
- Summer CI reading list

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

CICompass

ResearchSOC and Trusted CI

ResearchSOC

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

- 24/7/365 SOC monitoring, alerting, & investigations
- vCISO, advisory, vEngineer, and full security team staffing
- Vulnerability assessment and honeypot programs
- Security exercises and training
- Tackling specific operational, architecture, and controls challenges

- Creating comprehensive cybersecurity programs
- Community building and leadership
- Training and best practices
- Tackling specific challenges of cybersecurity, software assurance, privacy, etc.

https://omnisoc.iu.edu/services/researchsoc/

RRCoP and Trusted CI

Historically, most NSF-funded research (e.g., astronomy, climate, physics, geology) has been unregulated, i.e., not subject to a compliance program.

Trusted CI focuses on cybersecurity programs for unregulated research.

The Trusted CI Framework addresses compliance programs as a class of "obligations".

Compliance requirements (e.g., CMMC) are having a growing impact on CI.

RRCoP is a vibrant NSF-supported community addressing regulated research compliance requirements.

https://www.trustedci.org/compliance-programs

https://www.regulatedresearch.org/

Staying Connected with Trusted CI

Trusted CI Webinars

4th Monday of month at 11am ET.

https://trustedci.org/webinars

Follow Us

https://trustedci.org

https://blog.trustedci.org

https://www.linkedin.com/company/trustedci

Slack

Email ask@trustedci.org for an invitation.

Email Lists

Announce and Discuss

https://trustedci.org/trustedci-email-lists

Ask Us Anything

No question too big or too small.

info@trustedci.org

Cyberinfrastructure Vulnerabilities

Latest news on security vulnerabilities tailored for cyberinfrastructure community.

https://trustedci.org/vulnerabilities/

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Thanks!

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Trusted CI is supported by the National Science Foundation under Grants 1234408, 1547272, 1920430, and 2241313. The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.