Trustworthy Cyberinfrastructure

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

NSF Research Infrastructure Workshop

June 29, 2023

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

NCSA

BERKELEY LAB

WISCONSIN
UNIVERSITY OF WISCONSIN-MADISON

PITTSBURGH SUPERCOMPUTING CENTER

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

UNIVERSITY OF SOUTH ALABAMA

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.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

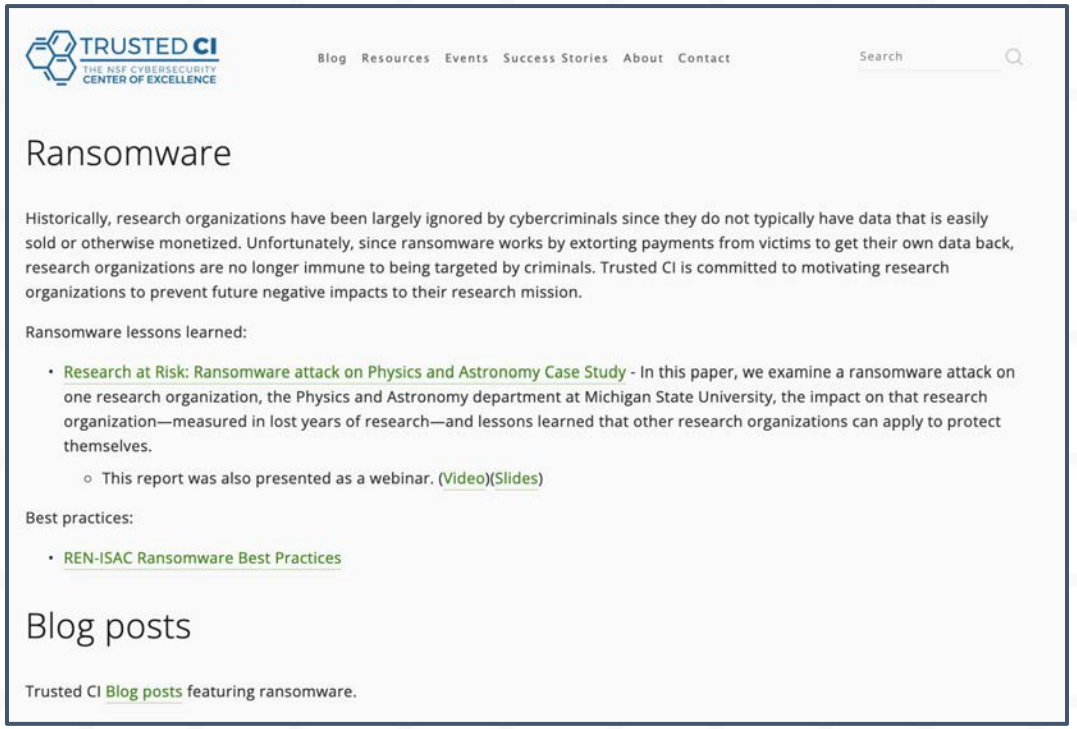
Growing Ransomware Risk to Science

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 at:

https://www.trustedci.org/ransomware



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

JASON Report on Facilities Cybersecurity

7 recommendations on risk assessment, strategy coordination, annual reviews, incident response, resourcing, planning, and national security: https://www.nsf.gov/news/special_reports/jasonreportcybersecurity/

How Trusted CI is addressing the recommendations: https://trustedci.org/2022-jason-report

Trusted CI coordinates with the NSF Cybersecurity Advisor for Research Infrastructure

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

2022 Annual Challenge: Operational Technology

- 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

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: Building Security Into NSF Major Facilities By Design

- 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 will particularly focus on the academic maritime domain.
  - Support acceptance testing of the NSF-funded Research Class Research Vessels (RCRVs) at Oregon State University,
  - Support the U.S. Antarctic Program (USAP)'s design of the Antarctic Research Vessel (ARV)
  - Support Scripps Institution of Oceanography's design of the California Coastal Research Vessel (CCRV).

U.S. Antarctic Program

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

Annual NSF Cybersecurity Summit

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

Training, workshops, and plenary sessions.

https://trustedci.org/summit/

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Summit Student Programs

Each NSF Cybersecurity Summit has a Student Program matching students from across the country with mentors and connecting them with NSF science projects and cybersecurity challenges.

https://blog.trustedci.org/search/label/students

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

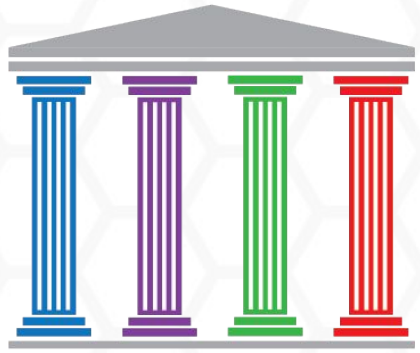
Trusted CI Fellows Program

- Training cybersecurity champions
- Supporting NSF science

https://trustedci.org/fellows

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

The Trusted CI Framework



https://trustedci.org/framework

Framework Core:

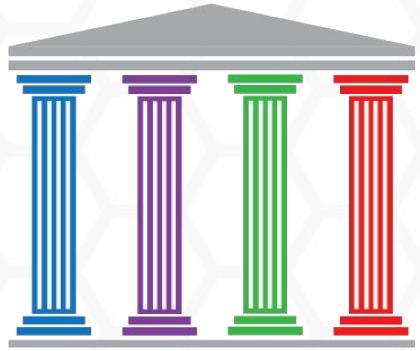
- Concise, clear minimum requirements for cybersecurity programs organized under the 4 Pillars: Mission Alignment, Governance, Resources, and Controls
- Based in general cybersecurity best practice and evidence of what works.

Framework Implementation Guide:

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

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Framework Adopters



NOIR Lab

NSO

FABRIC

UNOLS

ACCESS Advancing Innovation

GIANT MAGELLAN TELESCOPE

Regenstrief Institute
Better Care. Better Health.

NRAO

NSF neon Operated by Battelle

LIGO

NAN

OmniSOC

EarthScope Consortium

IceCube Neutrino Observatory

CENIC

OCEAN OBSERVATORIES INITIATIVE

DEEP SOIL ECOTRON

COMMON FUND DATA ECOSYSTEM

Open Science Grid

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://www.trustedci.org/framework

Trusted CI Partners

https://trustedci.org/partners

ResearchSOC

CI Compass and Trusted CI

- Two of the premier CoEs funded by NSF/OAC to help the NSF science community
- Co-founded the Identity Management Working Group
- Share CoE best practices and lessons learned
- Have standing and open communication and collaboration channels

Not sure which center to approach with a question or challenge?

Approach either and we'll collaboratively figure out how to best help you.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CI Compass

ResearchSOC and Trusted CI

- Operational services and related training for NSF CI
- Community of Practice and Threat Intelligence Network
- Enabling Cybersecurity Research
- Outreach to Higher Ed Infosec regarding research CI

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

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

RRCoP

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

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

@TrustedCI

Slack

Email ask@trustedci.org for an invitation.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

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/

Thanks!

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.