The Trusted CI Framework

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

3rd High-Performance Computing Security Workshop
March 15-16, 2023
Rockville, Maryland, USA

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

USA UNIVERSITY OF SOUTH ALABAMA

https://trustedci.org/

What is Cyberinfrastructure (CI)?

"The comprehensive infrastructure needed to capitalize on dramatic advances in information technology has been termed cyberinfrastructure (CI). Cyberinfrastructure integrates hardware for computing, data and networks, digitally-enabled sensors, observatories and experimental facilities, and an interoperable suite of software and middleware services and tools. "

-NSF Cyberinfrastructure Vision for 21st Century Discovery

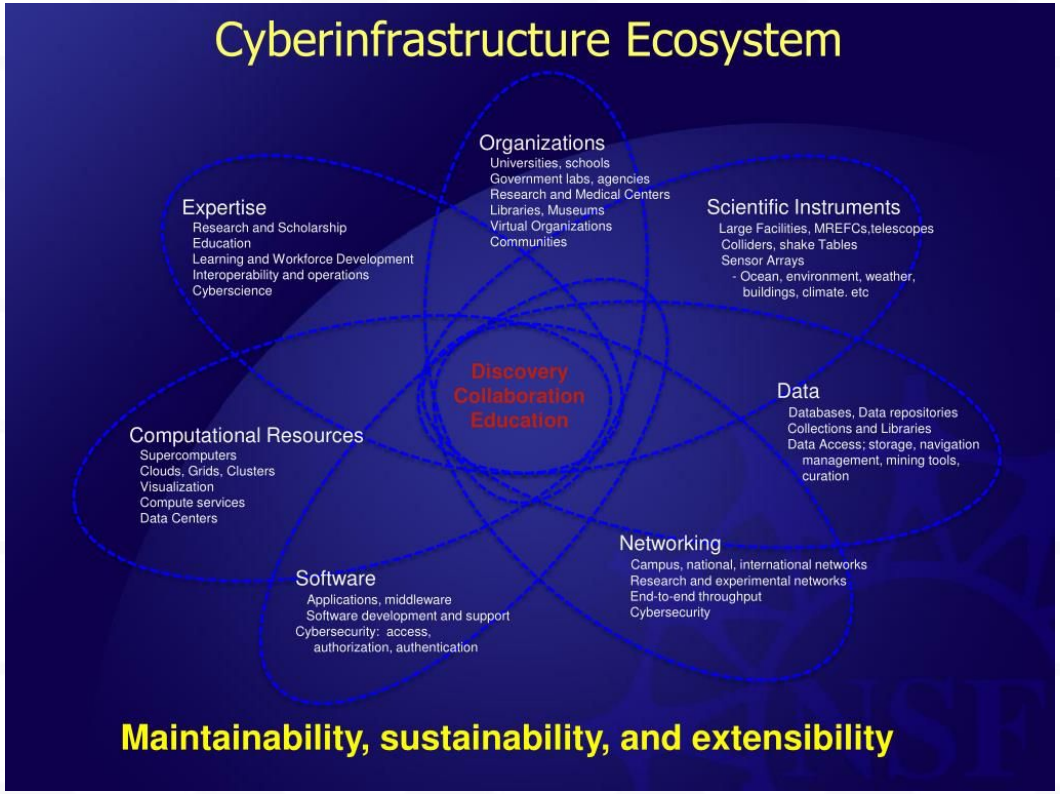


Image credit: NSF

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

NSF Cyberinfrastructure

- Major Facilities / Large Facilities
- Mid-scale Facilities
- ACCESS Resource Providers
- Campus Cyberinfrastructure (CC*)
- Software & Services (CICI, CSSI)
- People & Expertise (CyberTraining)

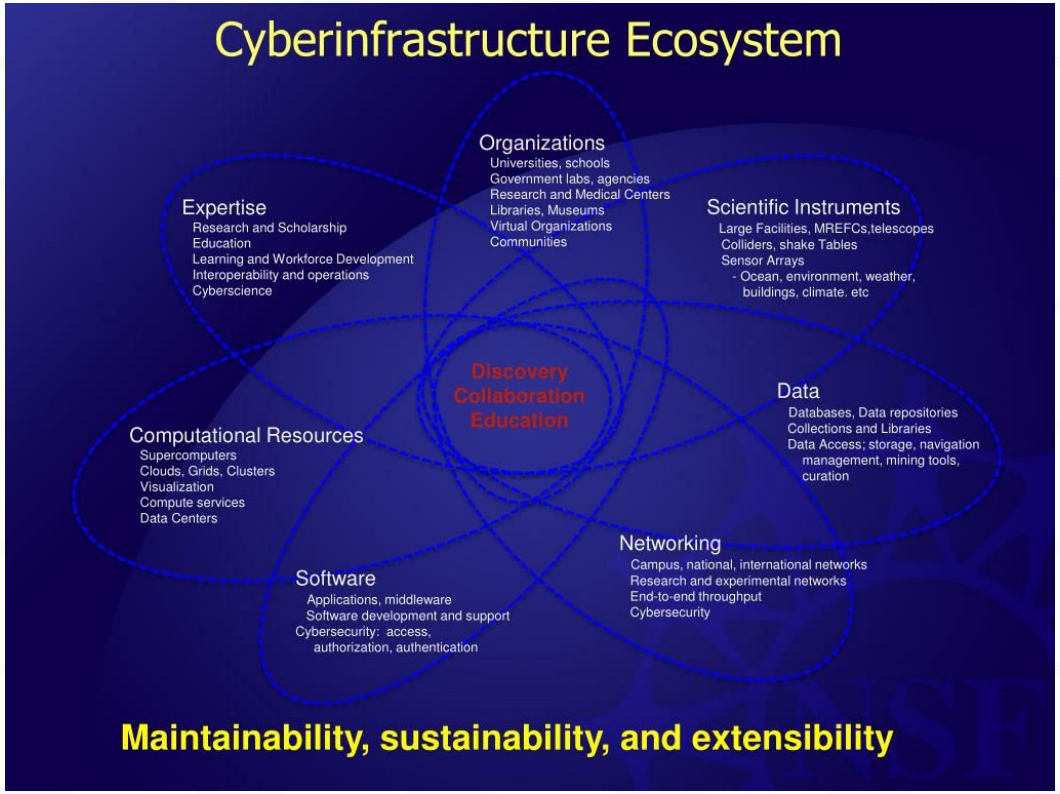
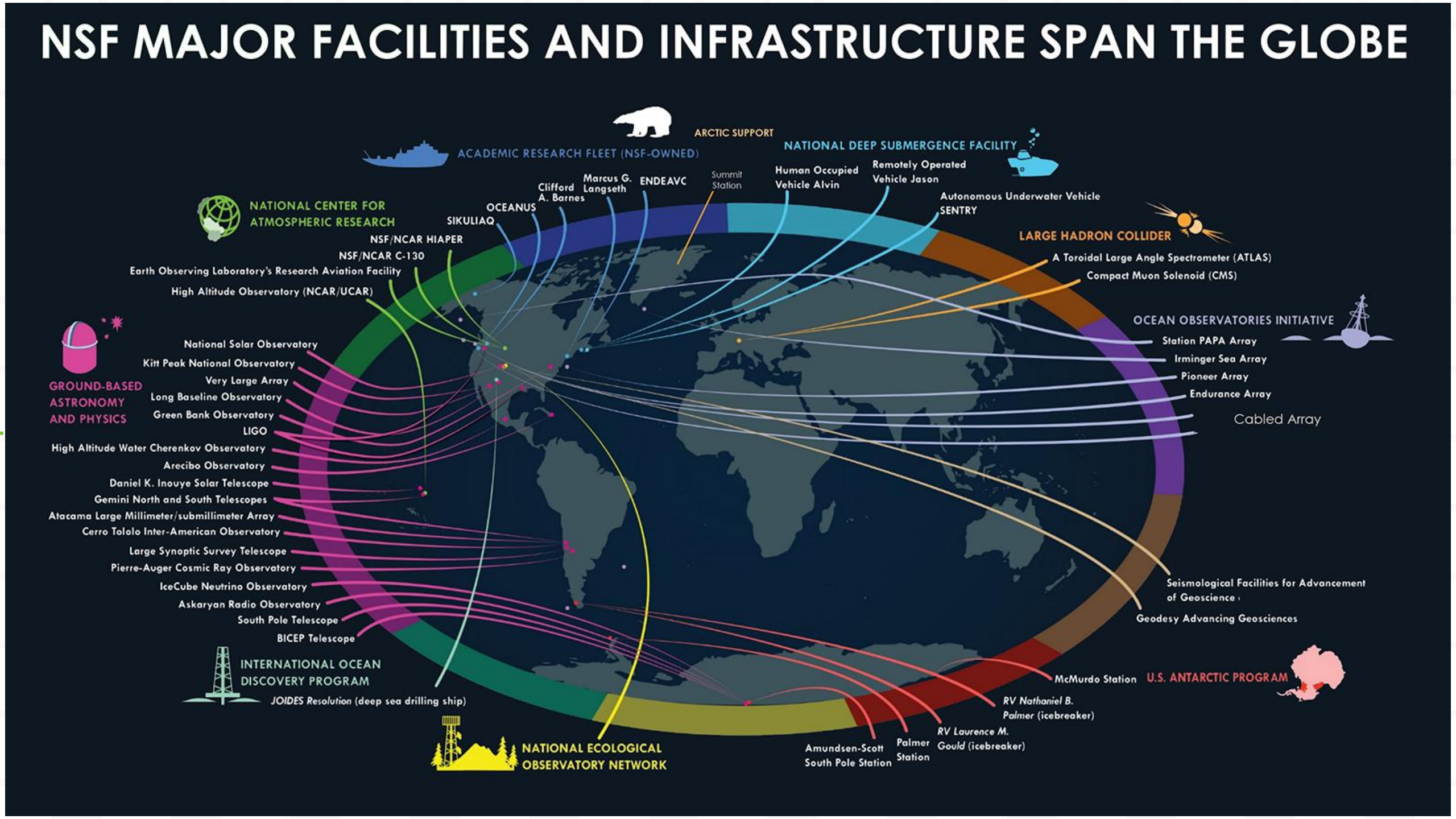


Image credit: NSF

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

NSF MAJOR FACILITIES AND INFRASTRUCTURE SPAN THE GLOBE



NSF CI & HPC

- NSF HPC providers are ACCESS RPs
- NSF Major Facilities rely on NSF HPC
- NSF Leadership-Class Computing Facility (LCCF) is an NSF Major Facility (in design phase)

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

2021 JASON Report on NSF 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/

> "NSF should maintain its current approach of supporting major facilities to enhance cybersecurity through assessments of risk, and development and implementation of mitigation plans. **A prescriptive approach to cybersecurity should be avoided** because it would be a poor fit to the diversity of facilities, would inefficiently use resources, and would not evolve quickly enough to keep up with changing threats."

- Trusted CI support, aligned with the Trusted CI Framework: https://trustedci.org/2022-jason-report
- New NSF Cybersecurity Advisor for Research Infrastructure position https://beta.nsf.gov/careers/openings/od/od/od-2022-87834

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

NSF Science and Compliance

While many cybersecurity compliance programs exist (*e.g.* HIPAA, FISMA, NIST 800-171), most NSF research (*e.g.* astronomy, climate, physics, geology) does not fall under a compliance program.

We coordinate with the Regulated Research Community of Practice (RRCoP) on compliance aspects: https://www.regulatedresearch.org/

Gemini South on the summit of Cerro Pachón in Chile (left) and Gemini North on the summit of Maunakea in Hawai'i (right).

Image credit: Gemini/NSF/AURA

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

NSF Cybersecurity Governance

NSF does not prescribe cybersecurity - it is the responsibility of the awardee.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

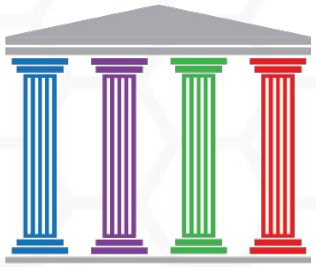
"NSF's responsibility is for overseeing the Recipient's development and management of the facility as well as assuring the successful performance of the funded activities. ***The Recipient is responsible for the day-to-day management of the facility.***"

NSF Research Infrastructure Guide (NSF 21-107), December 2021. Emphasis from source document. https://www.nsf.gov/bfa/lfo/

The Value of the NSF Approach

NSF's approach allows NSF facilities the flexibility to shape their cybersecurity program to best support their science mission.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE



The Trusted CI Framework

https://trustedci.org/framework

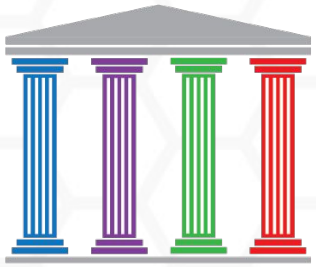
Framework Core:

- 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.
- Infrequent updates.

Framework Implementation Guide:

- Guidance vetted by and tailored to the open science community.
- Curated pointers to the very best resources and tools.
- Frequent (at least yearly) updates.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE



Framework Pillars

Mission Alignment

- Information classification, asset inventory, external requirements

Governance

- Roles and responsibilities, policies, risk acceptance, program evaluation

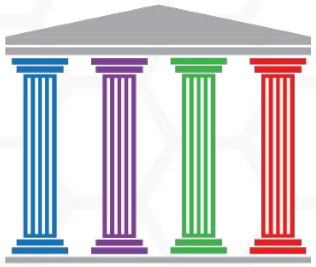
Resources

- People, budgets, services and tools

Controls

- Procedural, technical, administrative safeguards and countermeasures

Goals of the Trusted CI Framework



1. Provide a cybersecurity framework broadly accepted for (particularly NSF) research and science which doesn't have a clear compliance driver or standard for cybersecurity programs.
2. Build on Trusted CI Guide, WISE/SCI, GÉANT Baselines for NRENS, Trusted CI's work on the (former) NSF Major Facilities Guide and (current) NSF Research Infrastructure Guide
3. Capable of being implemented and existing alongside NIST 800-171, HIPAA, etc.

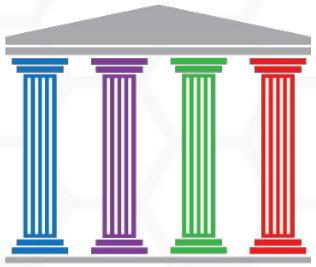
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Aligned with the NSF RIG

"The following sections define and describe a **suggested framework for the facility cybersecurity plan**. This framework is based on the previously mentioned **four pillars of information security programs: Mission Alignment, Governance, Resources, and Controls**. Major facilities may use these pillars as a framework for founding, operating, evaluating, and improving their information security programs, and meeting the award terms and conditions. Since there are interdependencies among the pillars, an integrative approach is required. The exact content and emphasis of the information security program should be **tailored to the mission, phase, size and scope of an individual facility**." NSF Research Infrastructure Guide (NSF 21-107), December 2021. https://www.nsf.gov/bfa/lfo/

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Framework Advisory Board



Steve Barnet (IceCube)
Tom Barton (I2/U. Chicago)
Jerry Brower (Gemini)
Shafaq Chaudhry (UCF)
Eric Cross (National Solar Observatory)
Carolyn Ellis (UCSD)
Paul Howell (Internet2)
Tim Hudson (NEON)
David Kelsey (Rutherford Appleton Lab)
Tolgay Kizilelma (Sutter Health)
Nick Multari (PNNL)
Adam Slagell (ESnet)
Alex Withers (NCSA)
Melissa Woo (MSU)

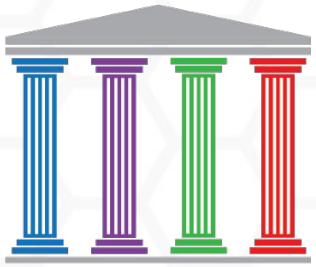
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Framework Adopters

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

https://www.trustedci.org/framework

Framework Implementation Guide for Research Cyberinfrastructure Operators



The guide gives research organizations a community-tailored head start on choosing among good paths and avoiding treacherous ones.

Includes:

- roadmaps for establishing mature cybersecurity programs
- tailored advice on overcoming common challenges
- pointers to resources

Built by Trusted CI's experienced multi-institutional team, and vetted by a Framework Advisory Board representing the diversity of our community.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

NIST RMF Crosswalk

Trusted CI & USAP are developing a crosswalk for NIST RMF and the Trusted CI Framework. Preliminary results show good alignment across the framework components.

Trusted CI is interested in working with the community to provide crosswalks to assist facilities with implementing multiple frameworks.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

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/

Acknowledgments

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

Trusted CI activities are made possible thanks to the contributions of a multi-institutional team:

https://trustedci.org/who-we-are/