Research Cybersecurity Insights for 2022

Jim Basney
Director, Trusted CI

EDUCAUSE Annual Conference

October 2022

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

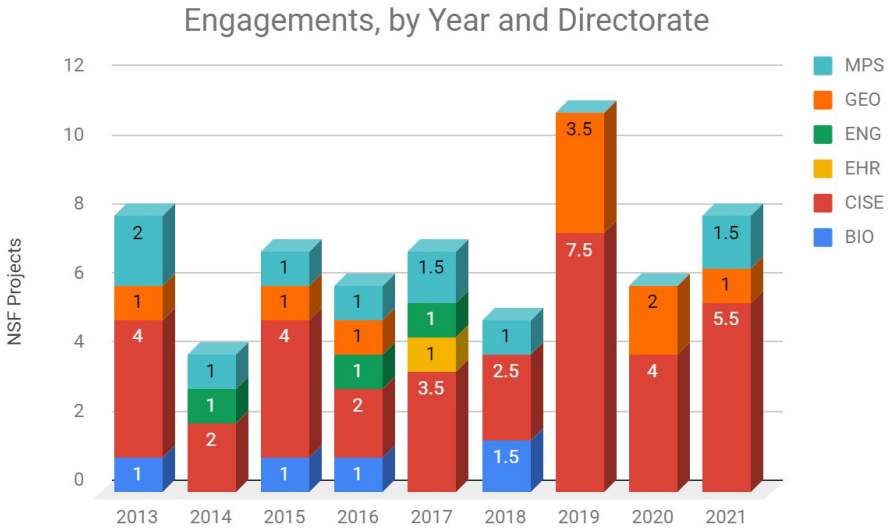
WISCONSIN
UNIVERSITY OF WISCONSIN-MADISON

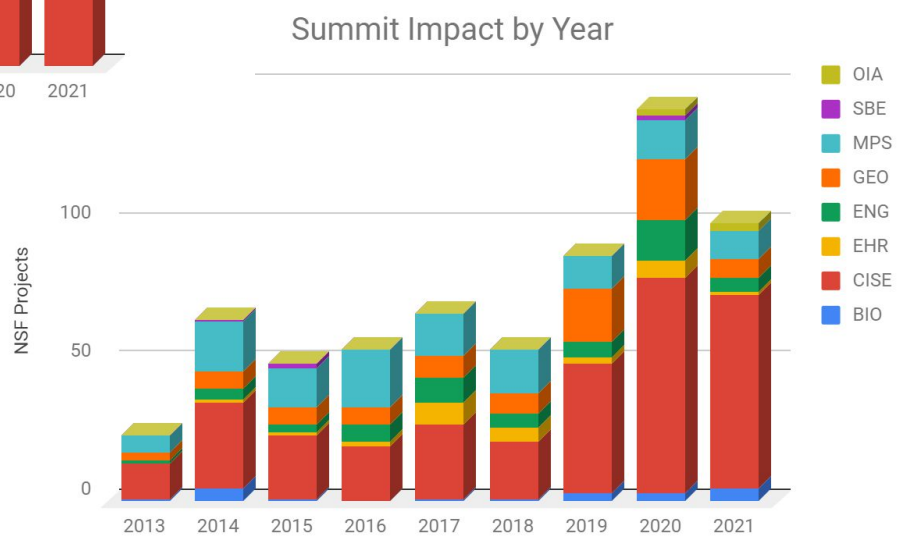
PITTSBURGH SUPERCOMPUTING CENTER

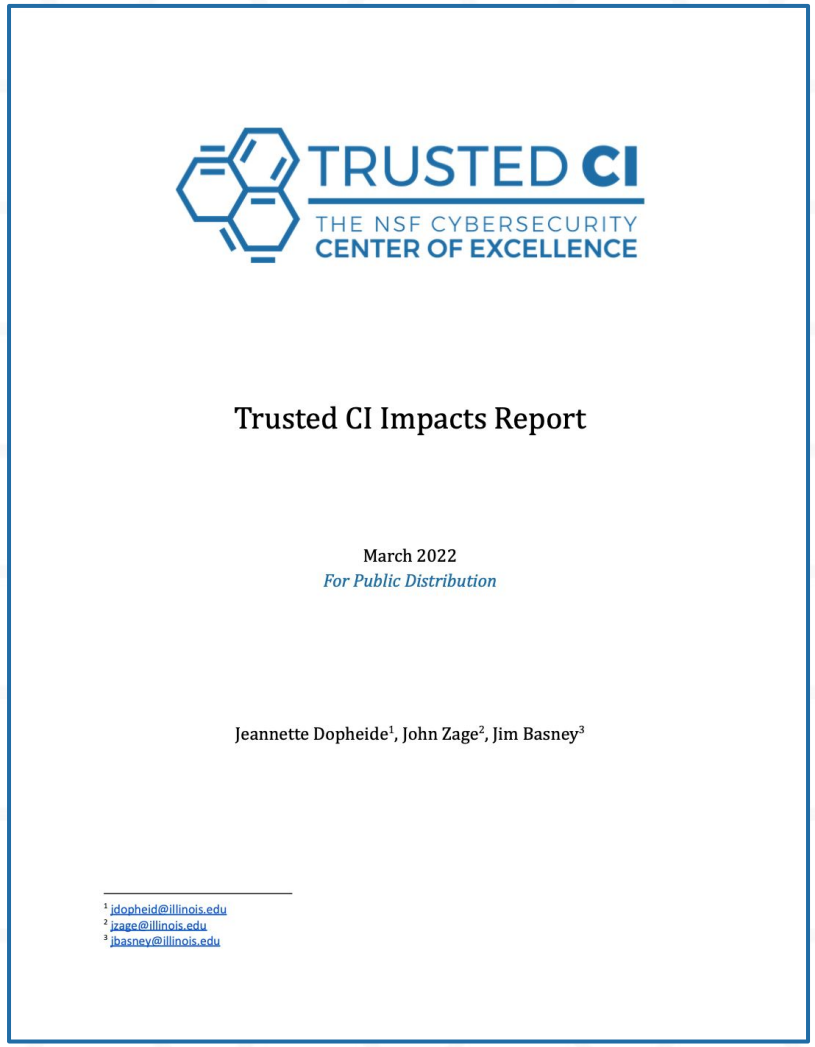
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

UNIVERSITY OF SOUTH ALABAMA

https://trustedci.org/







TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Trusted CI Impacts Report

March 2022
For Public Distribution

Jeannette Dopheide[1], John Zage[2], Jim Basney[3]

[1] jdopheid@illinois.edu
[2] jzage@illinois.edu
[3] jbasney@illinois.edu

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Dopheide, Jeannette, Zage, John, & Basney, Jim. (2022). Trusted CI Impacts Report. Zenodo. doi.org/10.5281/zenodo.6374207

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

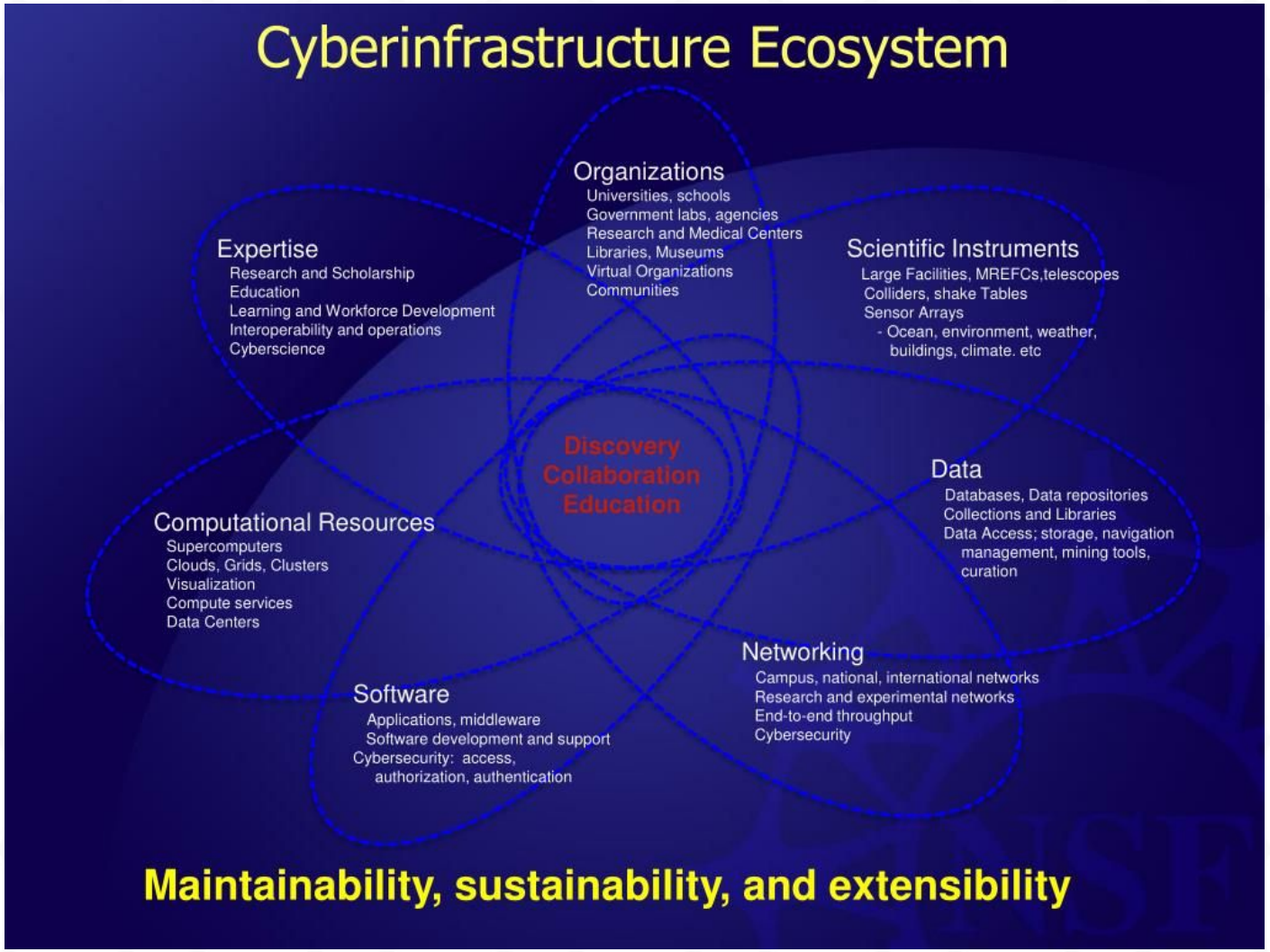
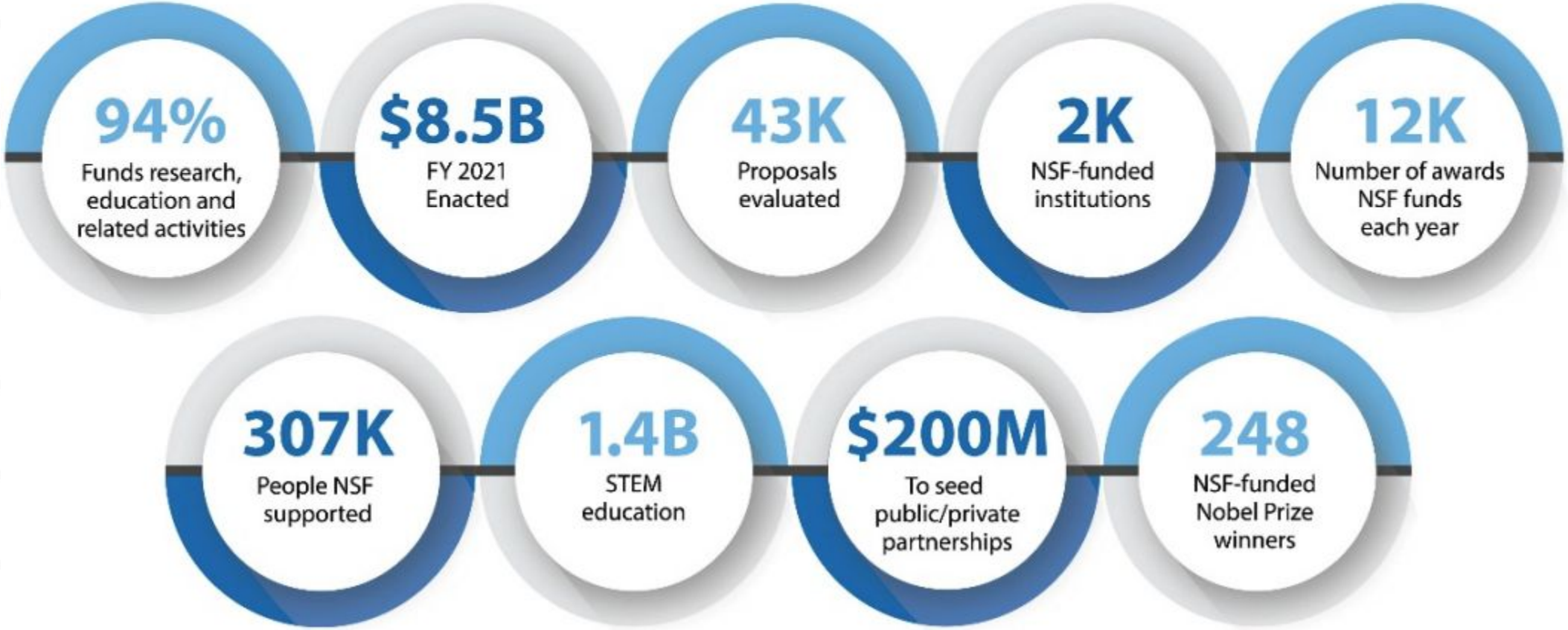


Image credit: NSF

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

NSF BY THE NUMBERS



https://nsf.gov/news/factsheets/Factsheet_By%20the%20Numbers_05_21_V02.pdf

NSF Cyberinfrastructure

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

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

NSF Major Facilities (examples)

Facility	Managing Institution(s)
Arecibo Observatory	University of Central Florida
Academic Research Fleet	University of Washington, Oregon State University
IceCube Neutrino Observatory	University of Wisconsin
International Ocean Discovery Program	Texas A&M, University of California-San Diego (Scripps Institution of Oceanography)
Leadership-Class Computing Facility	University of Texas, Austin
Large Hadron Collider	SUNY Stony Brook, Columbia University, University of Nebraska-Lincoln, Cornell University
Laser Interferometer Gravitational-wave Observatory	California Institute of Technology
National High Magnetic Field Lab	Florida State University

https://www.nsf.gov/bfa/lfo/docs/major-facilities-list.pdf

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/
- Trusted CI support, aligned with the Framework: https://trustedci.org/2022-jason-report
- New NSF Cybersecurity Advisor for Research Infrastructure 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) do not fall under a compliance program.

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.

The Value of the NSF Approach

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

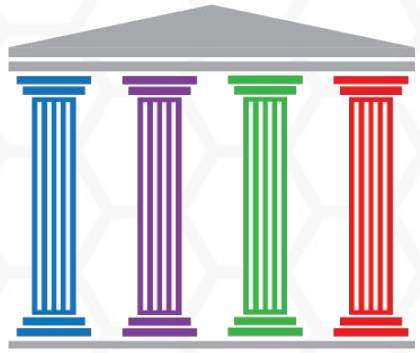
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Cybersecurity supports organizational mission

Organizational mission translates into different priorities for cybersecurity.

Imagine the program for a bank and hospital – confidentiality, availability, Integrity, resilience, etc. are all prioritized differently.

The Trusted CI Framework



The Trusted CI Framework establishes
best cybersecurity practices for cybersecurity programs.

- 16 clear and concise requirements.
- Based on best practices and evidence of what works.
- Designed to be universal and timeless.

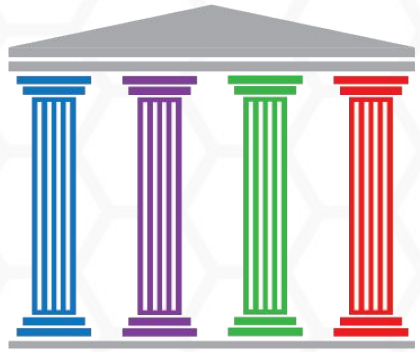
It focuses on cybersecurity programmatics:
Mission Alignment, **Governance**, **Resources**, and **Controls**.

This goes beyond technical controls to address the full spectrum of cybersecurity best practices.

https://www.trustedci.org/framework

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

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:

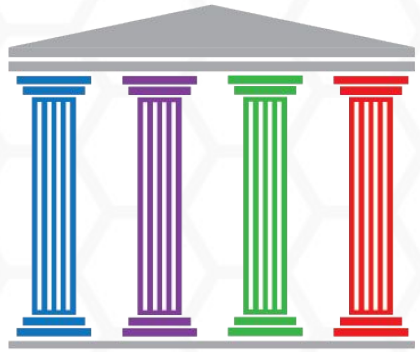
- roadmaps for establishing mature cybersecurity programs
- tailored advice on overcoming common challenges
- pointers to resources, including our publicly available tools and templates

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

https://www.trustedci.org/framework

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Framework Adopters



Example Framework Adopters:

- FABRIC
- GAGE
- LIGO
- NOIRLab
- NRAO
- NSO
- OOI
- ResearchSOC

https://www.trustedci.org/framework

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

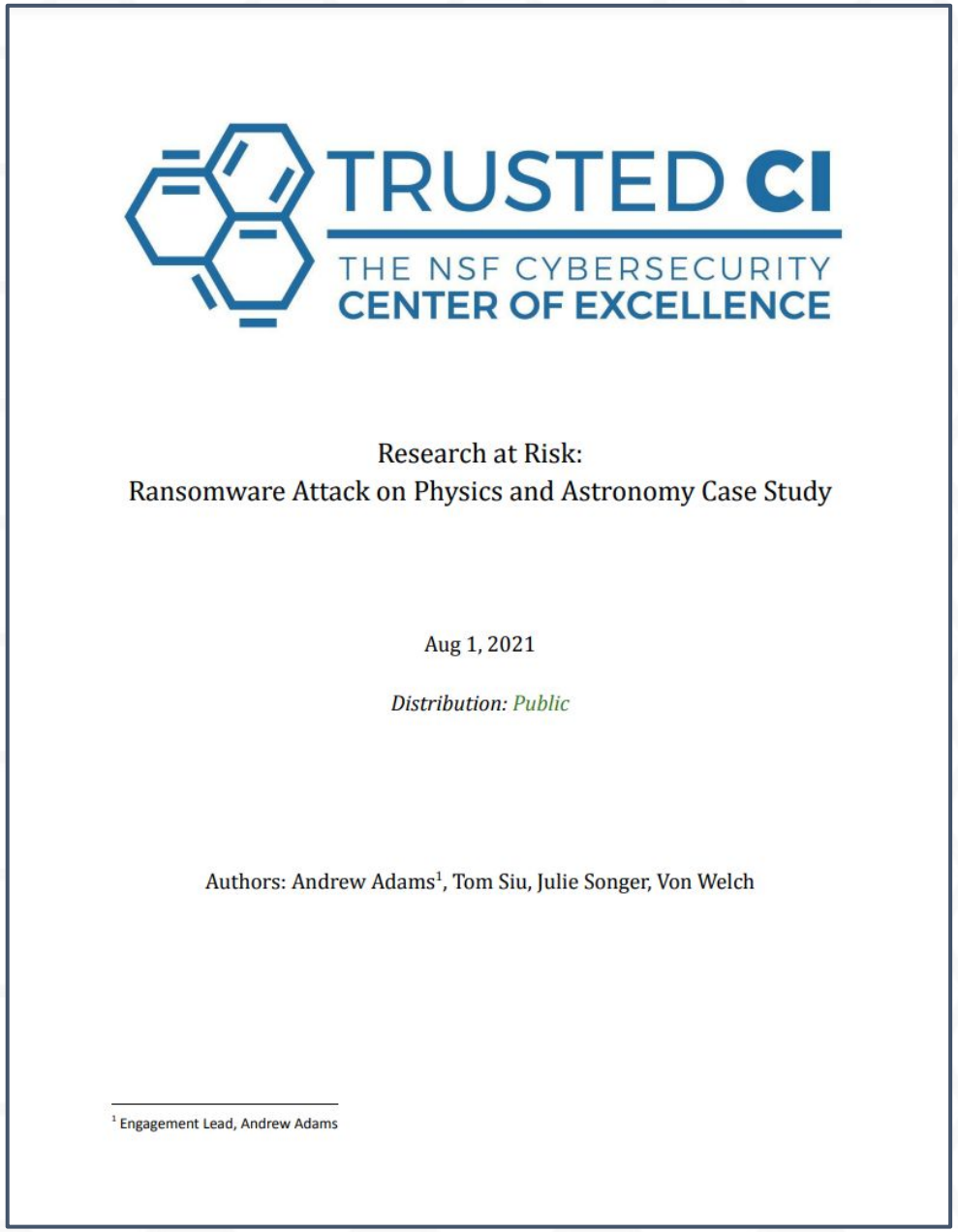
Growing Ransomware Risk to Science

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

Trusted CI Collaboration with Michigan State University office of the CIO to document impact of ransomware attack on research.

Report available at:
hdl.handle.net/2022/26638

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Research at Risk:
Ransomware Attack on Physics and Astronomy Case Study

Aug 1, 2021

Distribution: Public

Authors: Andrew Adams[1], Tom Siu, Julie Songer, Von Welch

[1] Engagement Lead, Andrew Adams

Science Gateways Security

September 2013: "Science Gateway Security Recommendations" at the Science Gateway Institute Workshop in Indianapolis

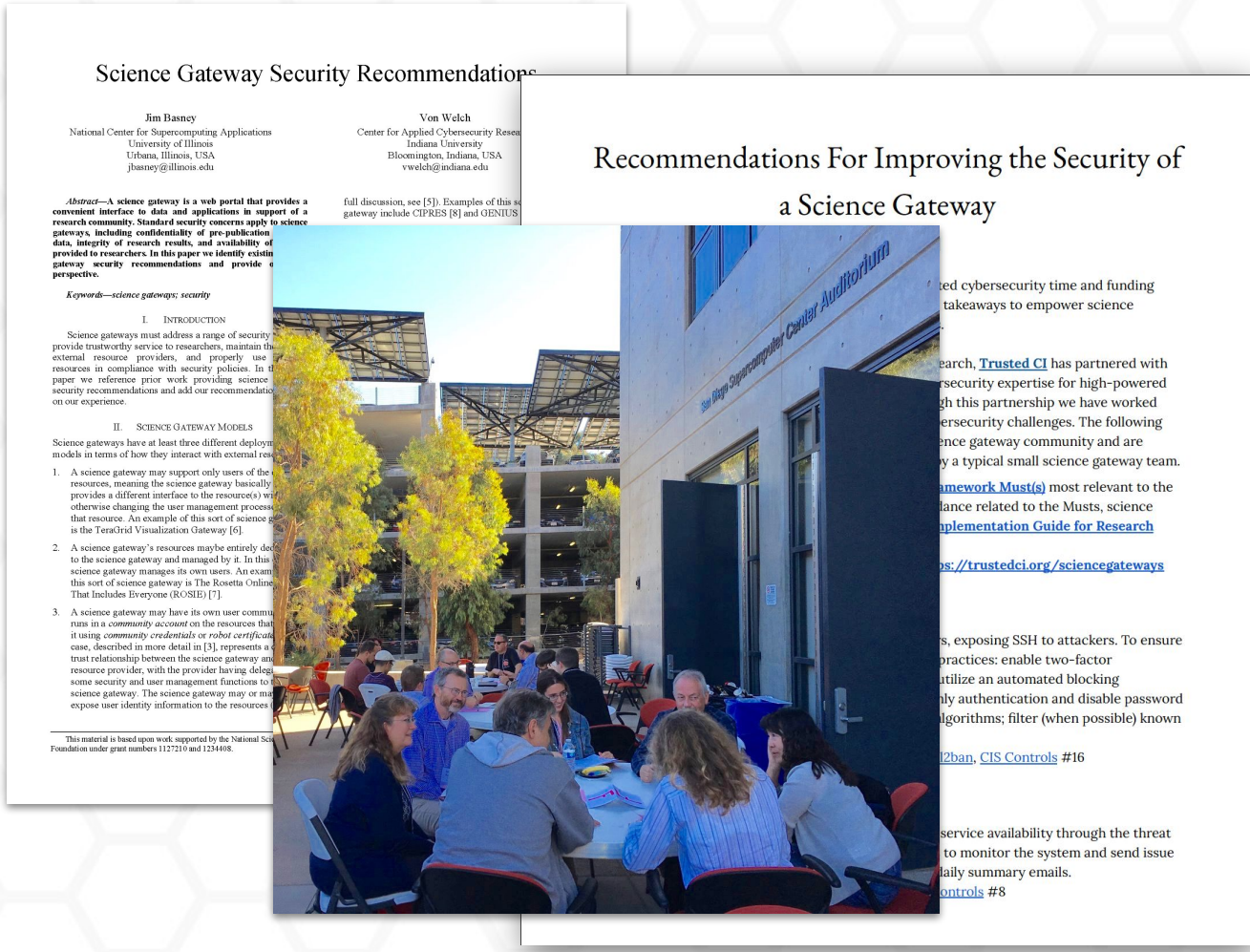
Partnership with Science Gateways Community Institute (SGCI) since 2016

Participation at Gateways conference and SGCI Focus Weeks

Engagements with ChemCOmpute, COIN-OR, COSMIC2, CyberGIS, Data@Risk, EarthCube, Galaxy, GenAPP, GISandbox, Hydroshare, Ike Wai, I-TASSER, SciGaP, SeedMeLab

September 2021: "Recommendations For Improving the Security of a Science Gateway"

SGCI
Science Gateways Community Institute

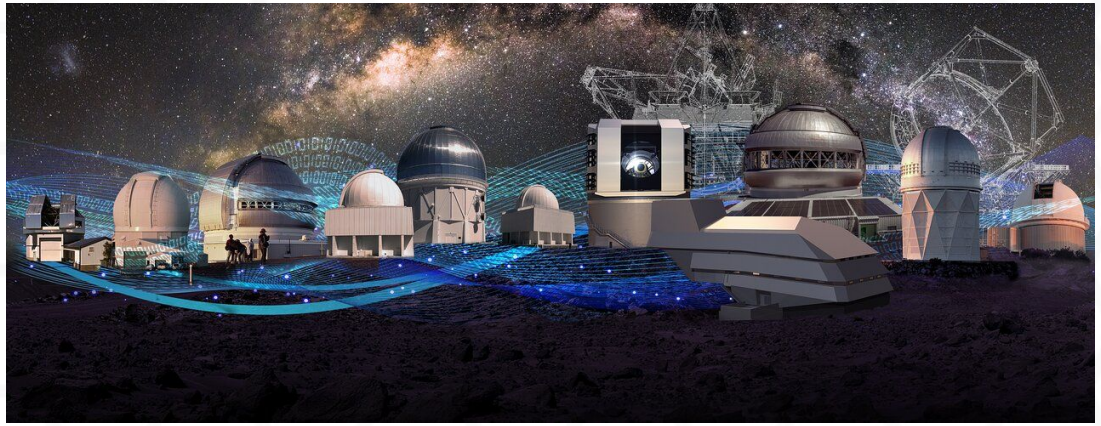


TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

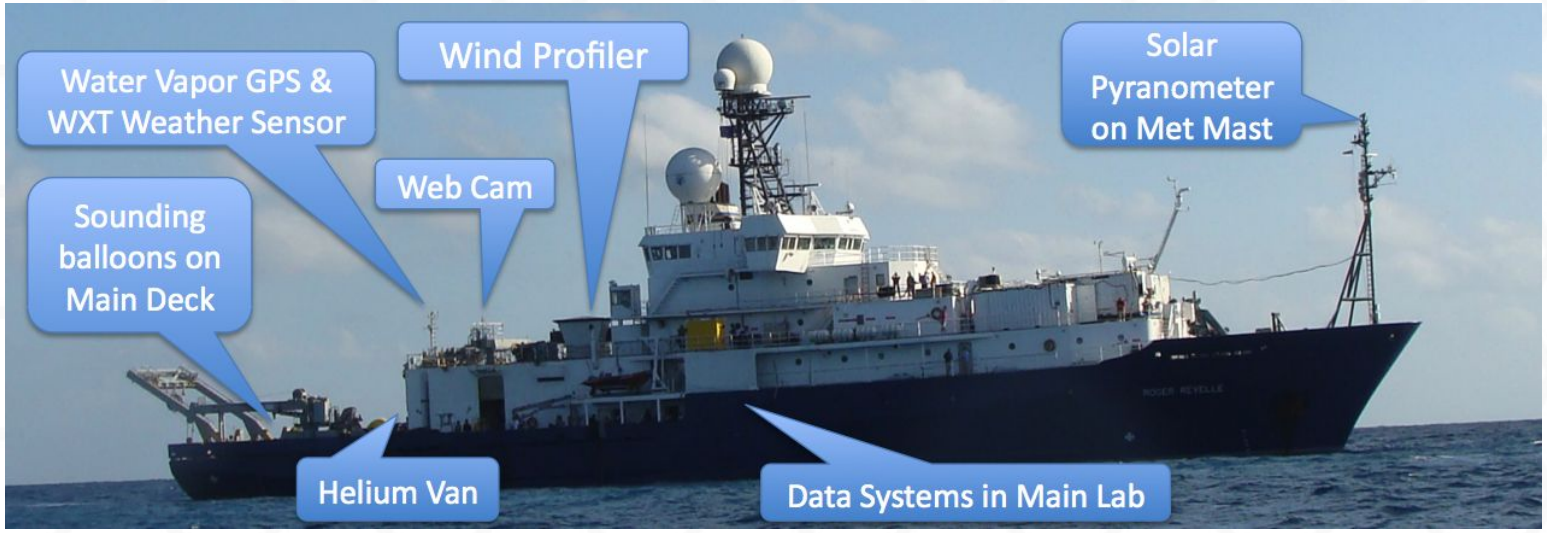
Science DMZ Security

- Partnered with EPOC, University of Arkansas / DART project
  on Science DMZ focused engagement
- Created reusable template security documents related to Science DMZs
- Published Security of Science DMZ whitepaper
  - https://hdl.handle.net/2022/27007
  - Help senior leadership to understand security of Science DMZs
  - Summarize and expand on security recommendations
  - Provide links to more resources

Scientific OT



Scientific Support OT



Also:

- Building HVAC
- Cranes
- Winches
- Antenna controllers
- Electronic door controls
- Environmental monitoring

OT Security Study Findings

- Security is a missing element for OT procurement requirements.
- Organizational “siloing” between IT security personnel and OT operators.
- Some host institutions (e.g., universities) can help MFs with IT/OT security but even they may not have OT security expertise appropriate to instruments in MFs.
- Newer OT (acquired in the past five years) — is increasingly “software defined” — contains exactly the same vulnerabilities as traditional IT systems.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Findings of the 2022 Trusted CI Study on the Security of Operational Technology in NSF Scientific Research

July 13, 2022

Status: Draft Report v1.0

Distribution: Public

Emily K. Adams, Daniel Gunter, Ryan Kiser, Mark Krenz, Sean Peisert, Susan Sons, and John Zage

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, and 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/