Trusted CI Update

Jim Basney
Director and PI, Trusted CI

Internet2 Technology Exchange

December 8, 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: Impacts

Updated impact as of March 2022:

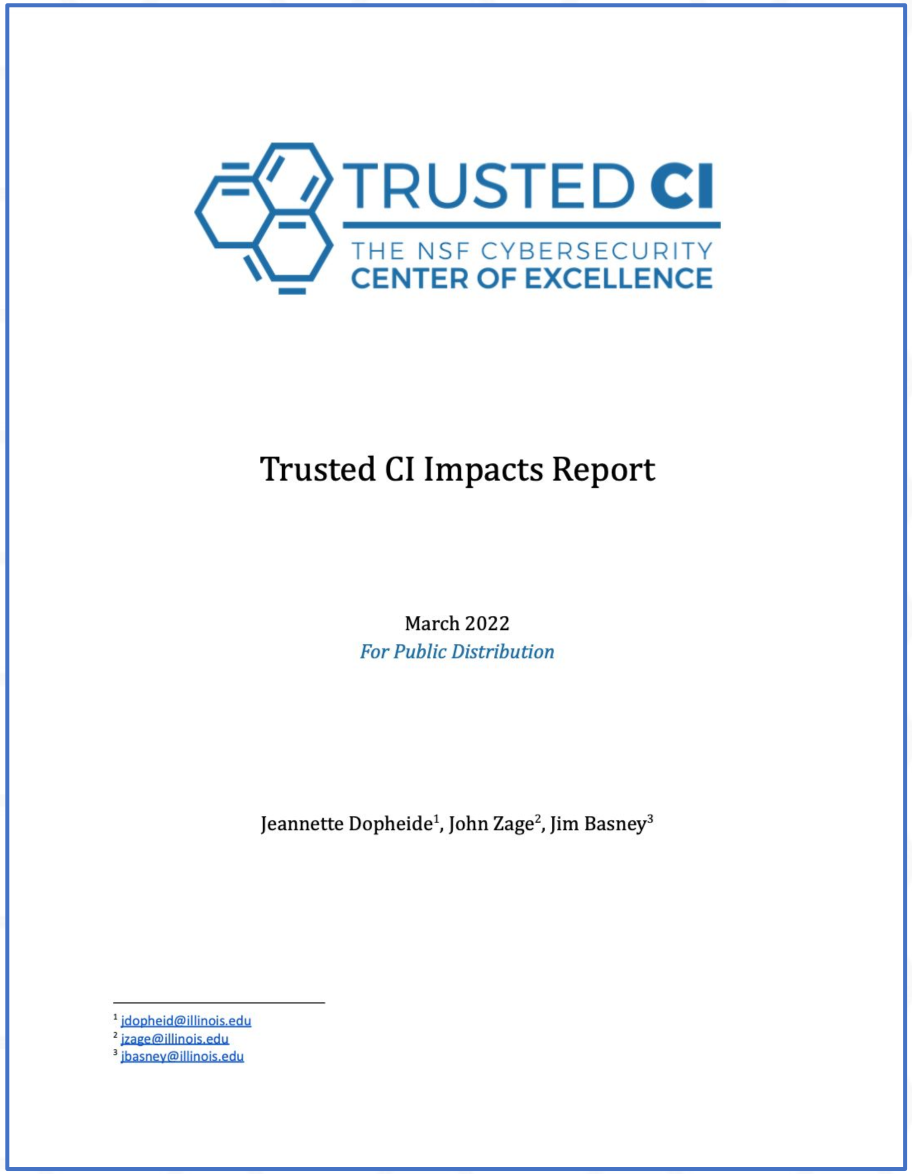
Trusted CI has positively impacted over 500 NSF projects since inception in 2012.

Members of more than 380 NSF projects have attended our NSF Cybersecurity Summit.

Members of more than 250 NSF projects have attended our monthly webinars.

We have provided more than 500 hours of training to the community.

We've had 64 engagements with NSF funded projects, including ten NSF Large Facilities.



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]

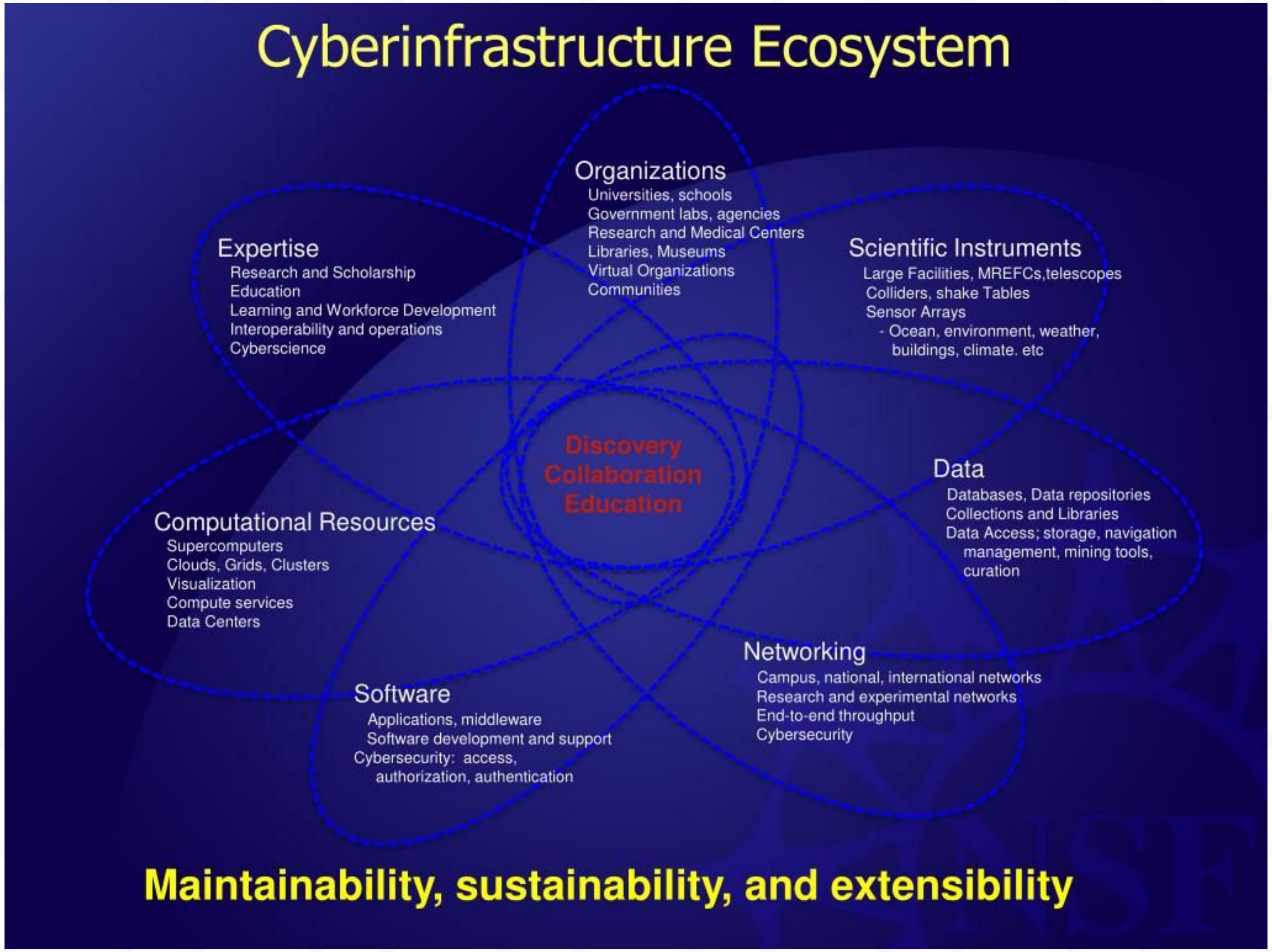
[1] jdopheid@illinois.edu
[2] jzage@illinois.edu
[3] jbasney@illinois.edu

Dopheide, Jeannette, Zage, John, & Basney, Jim. (2022). Trusted CI Impacts Report (2022). Zenodo. https://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



Cyberinfrastructure Ecosystem

Organizations
Universities, schools
Government labs, agencies
Research and Medical Centers
Libraries, Museums
Virtual Organizations
Communities

Expertise
Research and Scholarship
Education
Learning and Workforce Development
Interoperability and operations
Cyberscience

Scientific Instruments
Large Facilities, MREFCs,telescopes
Colliders, shake Tables
Sensor Arrays
- Ocean, environment, weather, buildings, climate. etc

Discovery
Collaboration
Education

Data
Databases, Data repositories
Collections and Libraries
Data Access; storage, navigation management, mining tools, curation

Computational Resources
Supercomputers
Clouds, Grids, Clusters
Visualization
Compute services
Data Centers

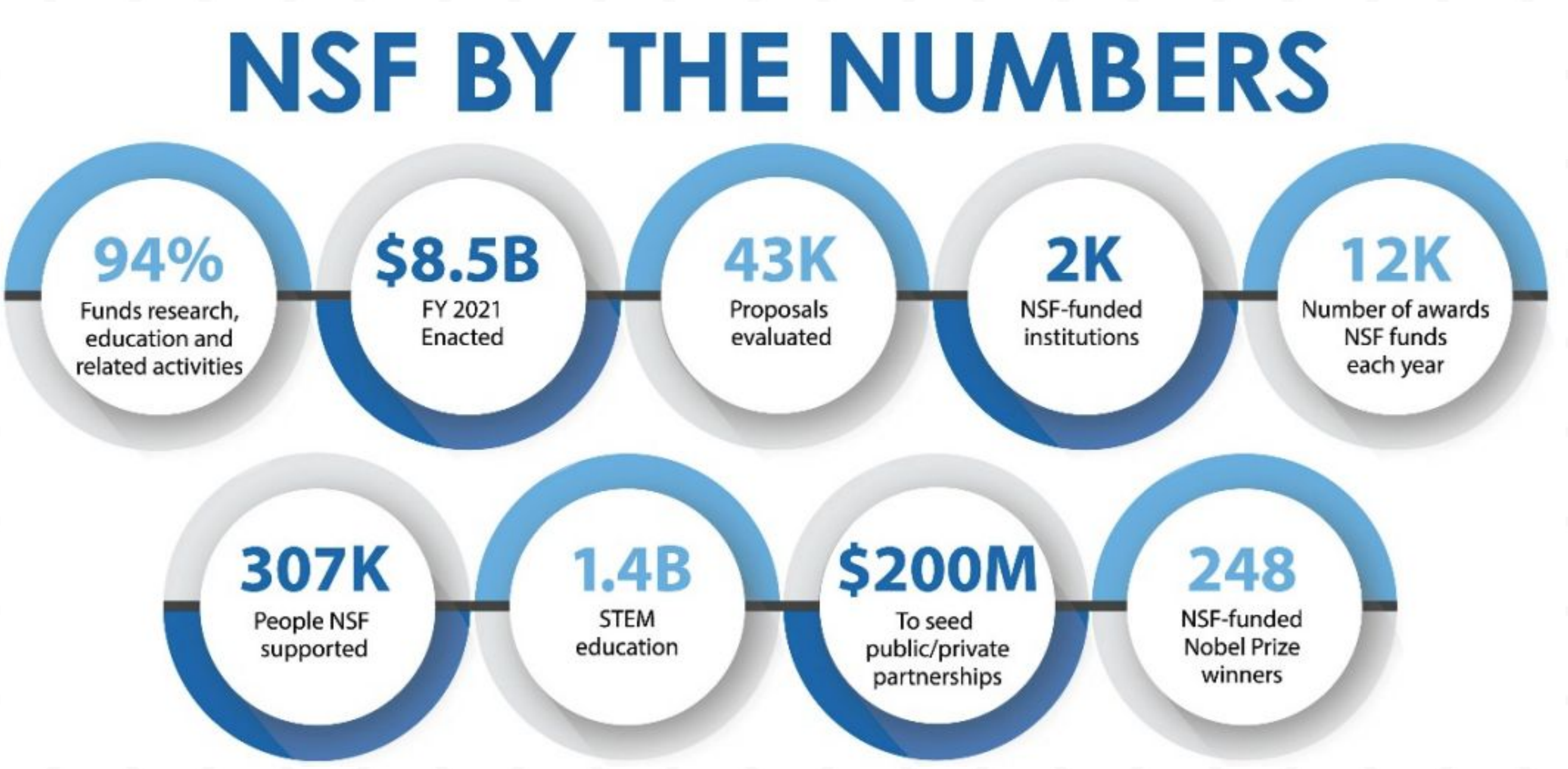
Networking
Campus, national, international networks
Research and experimental networks
End-to-end throughput
Cybersecurity

Software
Applications, middleware
Software development and support
Cybersecurity: access, authorization, authentication

Maintainability, sustainability, and extensibility

Image credit: NSF

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE



NSF BY THE NUMBERS

94%
Funds research, education and related activities

$8.5B
FY 2021 Enacted

43K
Proposals evaluated

2K
NSF-funded institutions

12K
Number of awards NSF funds each year

307K
People NSF supported

1.4B
STEM education

$200M
To seed public/private partnerships

248
NSF-funded Nobel Prize winners

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)

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 position https://beta.nsf.gov/careers/openings/od/od/od-2022-87834

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.

"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.

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

The Value of the NSF Approach

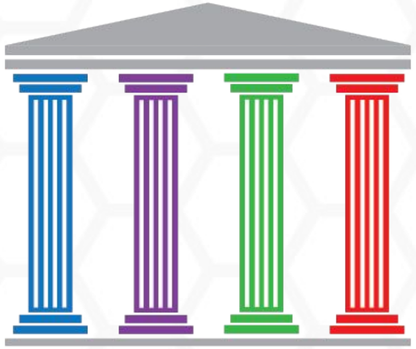
NSF’s approach allows NSF projects the flexibility to shape their cybersecurity program to best support their science mission.

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

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

Framework Adopters

Example Framework Adopters:

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

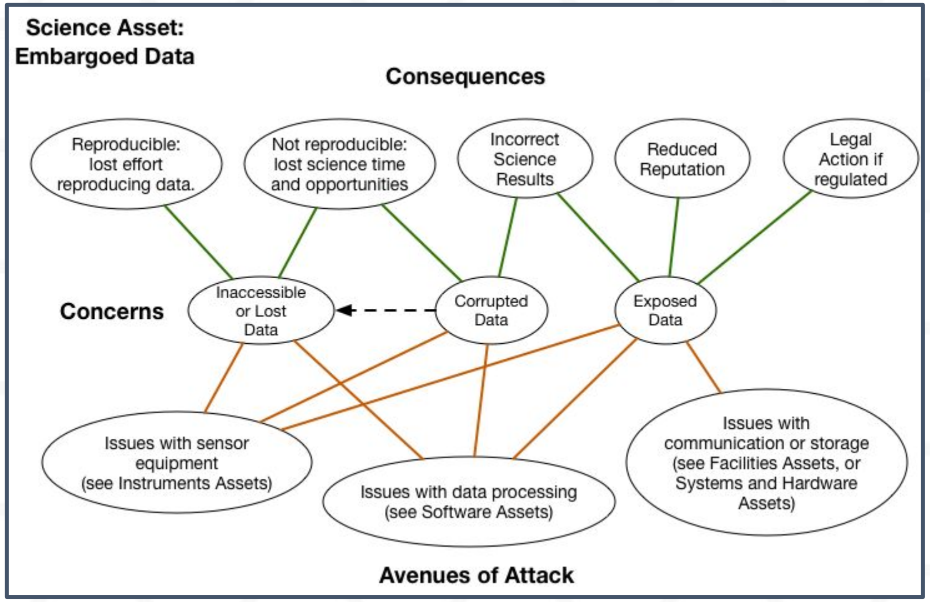
https://www.trustedci.org/framework

Open Science Cyber Risk Profile (OSCRP)

OSCRP helps science projects understand cybersecurity risks to their science infrastructure and facilitates discussing those risks with their campus security office.

2022 updates include Science DMZ, Software Assurance, Operational Technology, and Cloud Computing elements.

https://trustedci.org/oscrp/



Science Asset:
Embargoed Data
Consequences
Reproducible: lost effort reproducing data.
Not reproducible: lost science time and opportunities
Incorrect Science Results
Reduced Reputation
Legal Action if regulated
Concerns
Inaccessible or Lost Data
Corrupted Data
Exposed Data
Issues with sensor equipment (see Instruments Assets)
Issues with data processing (see Software Assets)
Issues with communication or storage (see Facilities Assets, or Systems and Hardware Assets)
Avenues of Attack

Example mapping from OSCRP of cybersecurity attacks to scientific consequences.

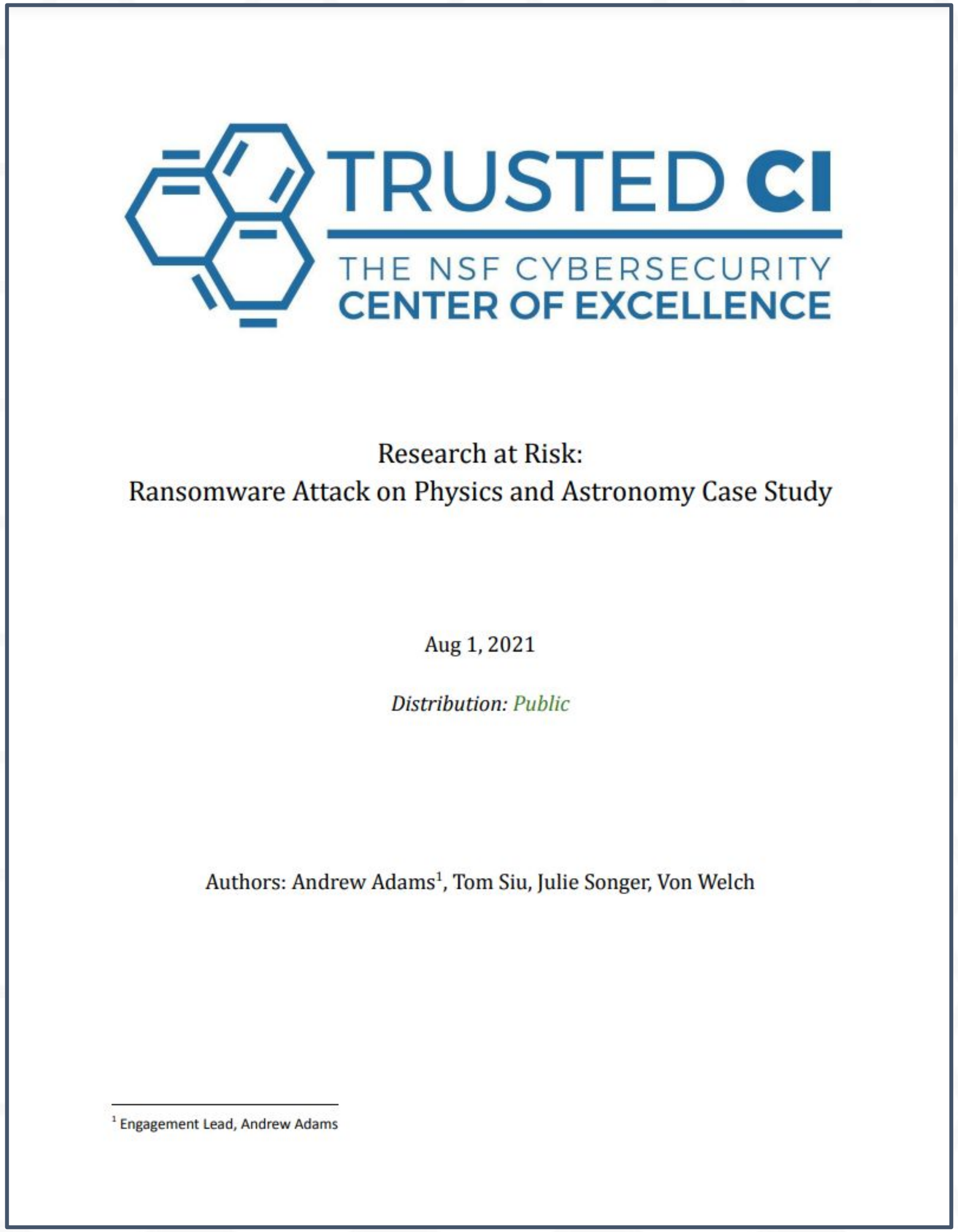
TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

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

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

Software Assurance

https://www.trustedci.org/software-assurance

2021 Annual Challenge

Interviewed six large CI project who develop scientific software to understand their practices surrounded software security. Produced a "Findings" document report on the state of the art.

To provide direction in developing secure software, we produced the initial version of the "Guide to Securing Scientific Software". This is a living document with ongoing development this year.

Software Secure Training

Free and open online resources (cc'd in English & Spanish), including extensive hands-on exercises and instructor materials:

`https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/`

Teach tutorials at conferences, workshops, labs, and government agencies.

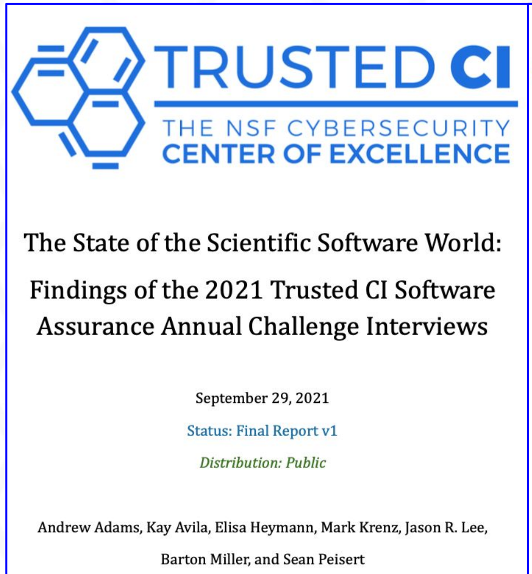
In-depth vulnerability assessment

Have done multiple project engagements.

Development new techniques to automate such assessments.

Ransomware

Developing comprehensive threat model of ransomware attacks.



TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

The State of the Scientific Software World:

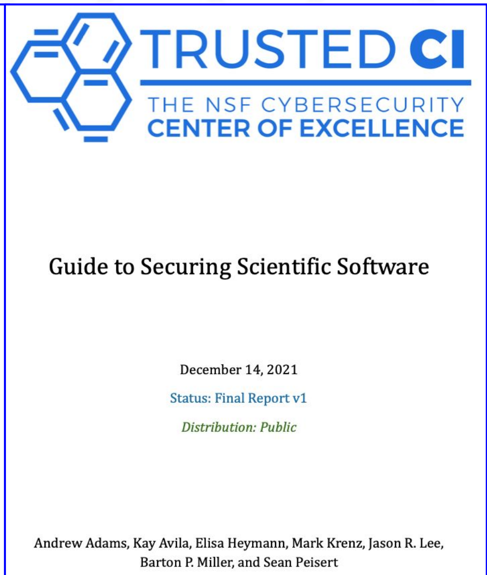
Findings of the 2021 Trusted CI Software Assurance Annual Challenge Interviews

September 29, 2021

Status: Final Report v1

Distribution: Public

Andrew Adams, Kay Avila, Elisa Heymann, Mark Krenz, Jason R. Lee, Barton Miller, and Sean Peisert



TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Guide to Securing Scientific Software

December 14, 2021

Status: Final Report v1

Distribution: Public

Andrew Adams, Kay Avila, Elisa Heymann, Mark Krenz, Jason R. Lee, Barton P. Miller, and Sean Peisert

Science Gateways Security

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

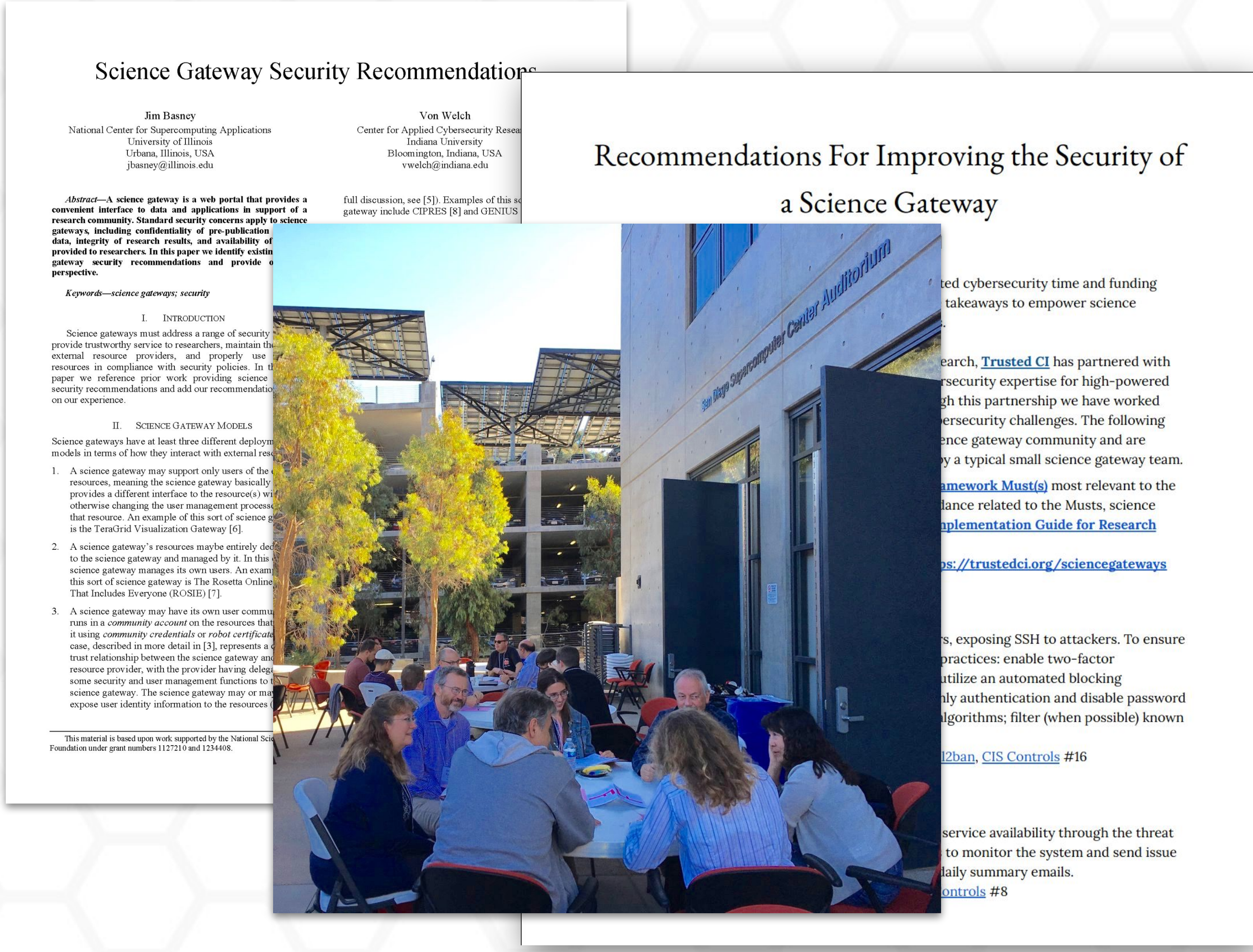
Partnership with Science Gateways Community Institute (SGCI) since 2016

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



Science Gateway Security Recommendations

Jim Basney
National Center for Supercomputing Applications
University of Illinois
Urbana, Illinois, USA
jbasney@illinois.edu

Von Welch
Center for Applied Cybersecurity Resea
Indiana University
Bloomington, Indiana, USA
vwelch@indiana.edu

Abstract—**A science gateway is a web portal that provides a convenient interface to data and applications in support of a research community. Standard security concerns apply to science gateways, including confidentiality of pre-publication data, integrity of research results, and availability of provided to researchers. In this paper we identify existin gateway security recommendations and provide o perspective.**

***Keywords*—science gateways; security**

I. Introduction

Science gateways must address a range of security provide trustworthy service to researchers, maintain the external resource providers, and properly use resources in compliance with security policies. In th paper we reference prior work providing science security recommendations and add our recommendatio on our experience.

II. Science Gateway Models

Science gateways have at least three different deploym models in terms of how they interact with external reso

1. A science gateway may support only users of the resources, meaning the science gateway basically provides a different interface to the resource(s) wi otherwise changing the user management processe that resource. An example of this sort of science g is the TeraGrid Visualization Gateway [6].
2. A science gateway's resources maybe entirely ded to the science gateway and managed by it. In this science gateway manages its own users. An exam this sort of science gateway is The Rosetta Online That Includes Everyone (ROSIE) [7].
3. A science gateway may have its own user commu runs in a *community account* on the resources that it using *community credentials* or *robot certificate* case, described in more detail in [3], represents a trust relationship between the science gateway and resource provider, with the provider having delega some security and user management functions to t science gateway. The science gateway may or may expose user identity information to the resources (

full discussion, see [5]). Examples of this sc gateway include CIPRES [8] and GENIUS

This material is based upon work supported by the National Scie Foundation under grant numbers 1127210 and 1234408.

Recommendations For Improving the Security of a Science Gateway

ted cybersecurity time and funding takeaways to empower science

earch, **Trusted CI** has partnered with rsecurity expertise for high-powered gh this partnership we have worked ersecurity challenges. The following ence gateway community and are y a typical small science gateway team.

amework Must(s) most relevant to the lance related to the Musts, science **nplementation Guide for Research**

ps://trustedci.org/sciencegateways

s, exposing SSH to attackers. To ensure practices: enable two-factor utilize an automated blocking nly authentication and disable password lgorithms; filter (when possible) known

l2ban, CIS Controls #16

service availability through the threat to monitor the system and send issue laily summary emails.

ontrols #8

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

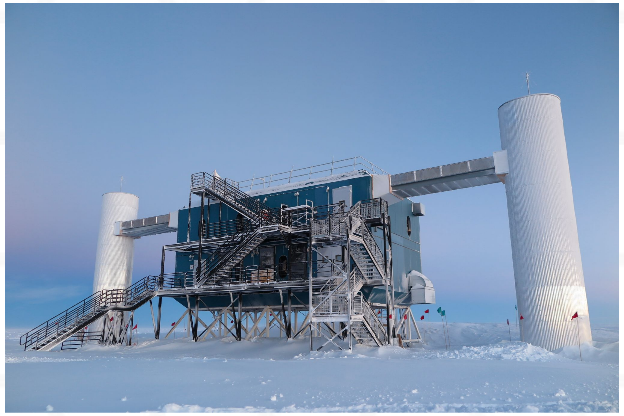
UNIVERSITY OF ARKANSAS

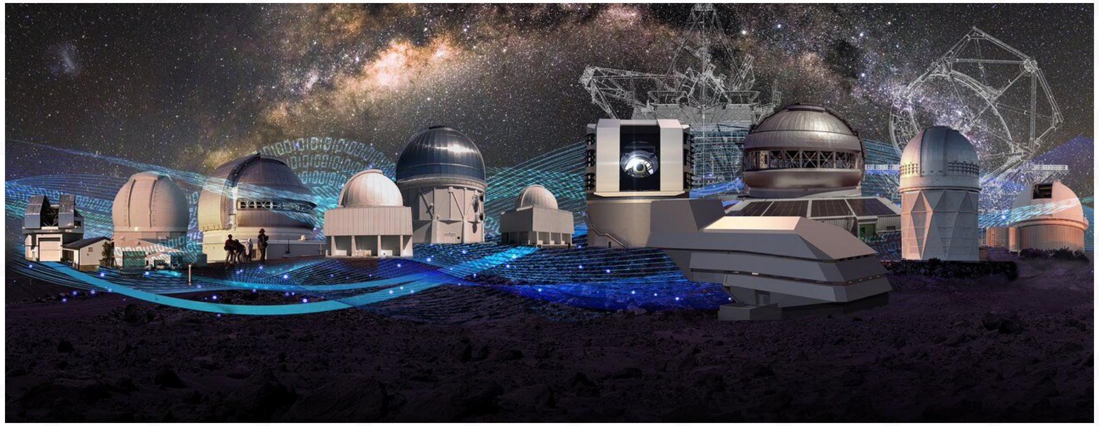
DART

ARKANSAS INC
SCIENCE & TECHNOLOGY

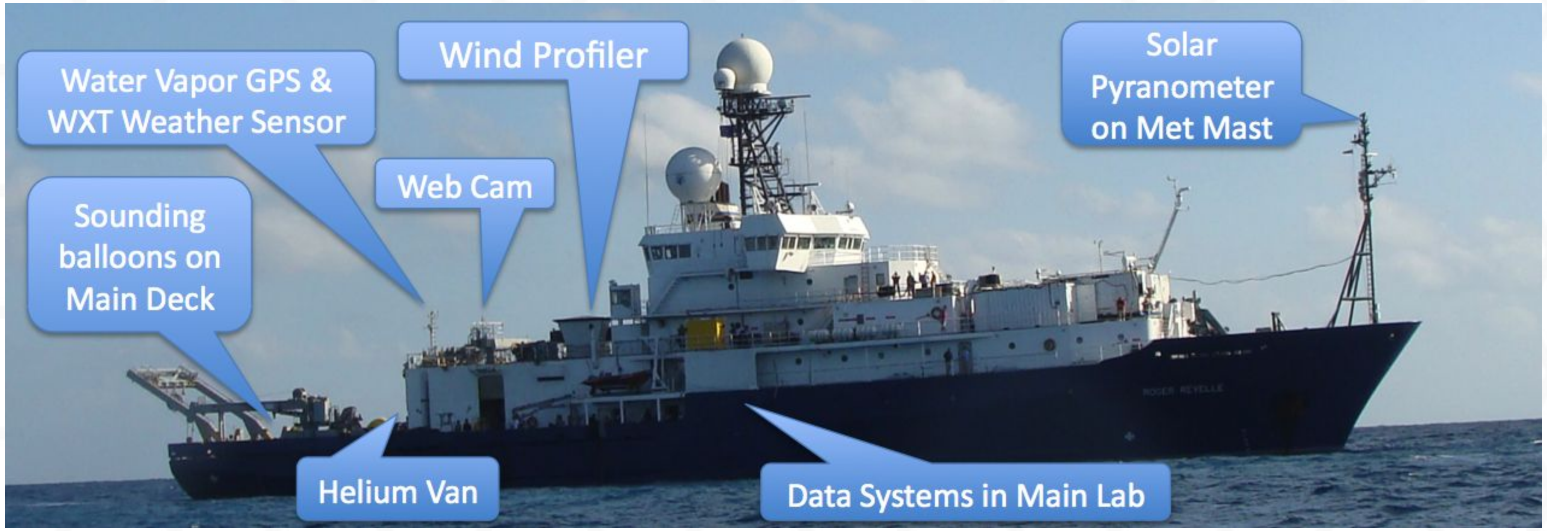
EPOC
Engagement and Performance Operations Center

Scientific OT





Scientific Support OT


Water Vapor GPS & WXT Weather Sensor
Wind Profiler
Solar Pyranometer on Met Mast
Web Cam
Sounding balloons on Main Deck
Helium Van
Data Systems in Main Lab

Also:

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

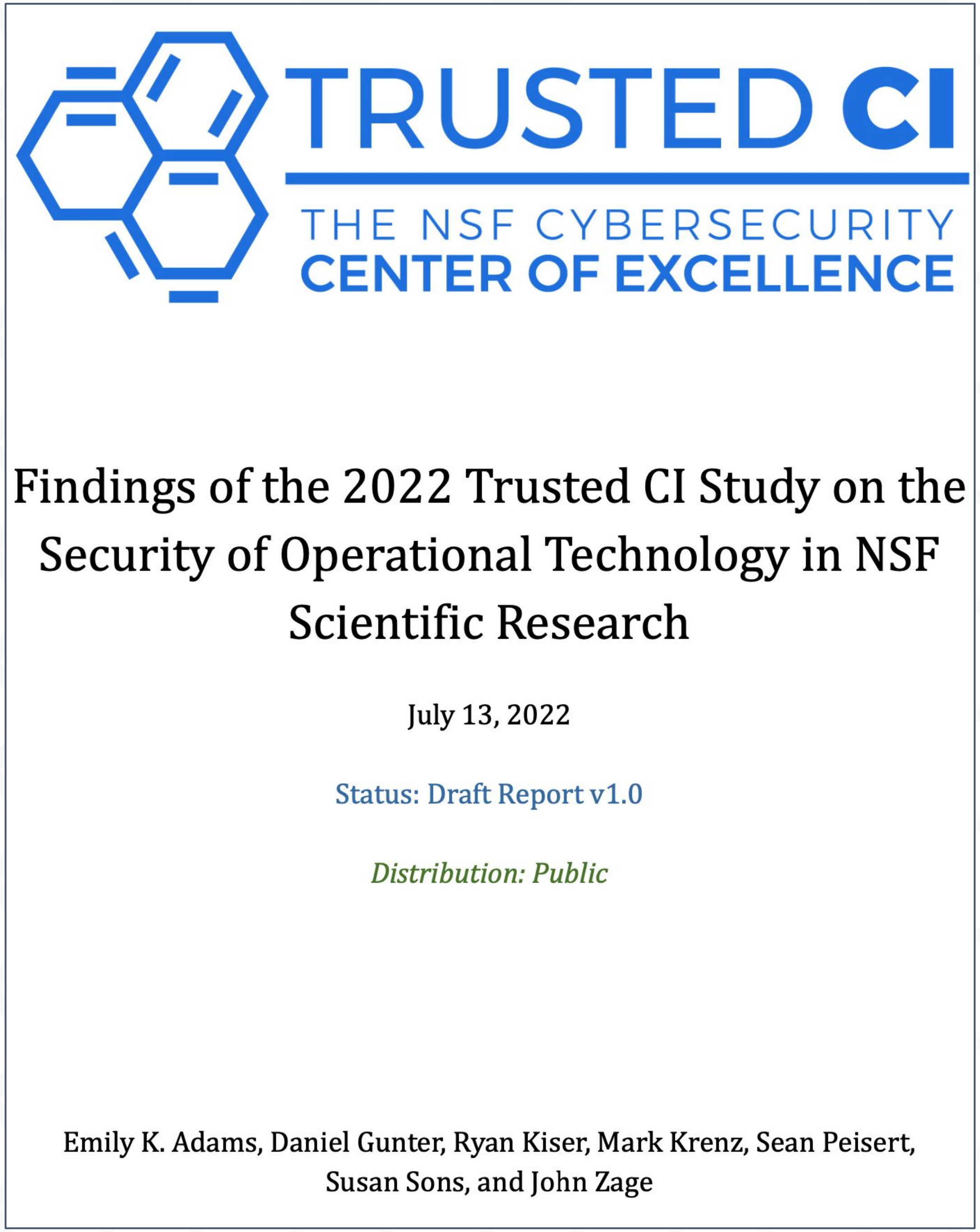
Two wind profiler radars (large white boxes) on the deck of the R/V Mirai (Ship) in the central Pacific for the Nauru99 project: one is a MWPR and the other is a 1357 MHz WPR. There is also a RASS system and an S-band vertically pointing radar (the drum antenna).

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.

https://www.trustedci.org/operational-technology

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

Trusted CI Fellows Program

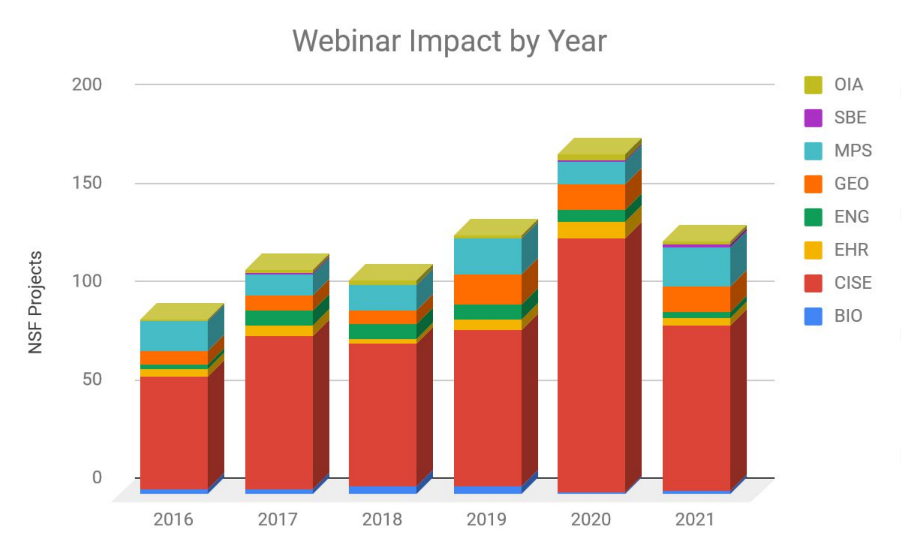
- Training cybersecurity champions
- Supporting NSF science

https://trustedci.org/fellows

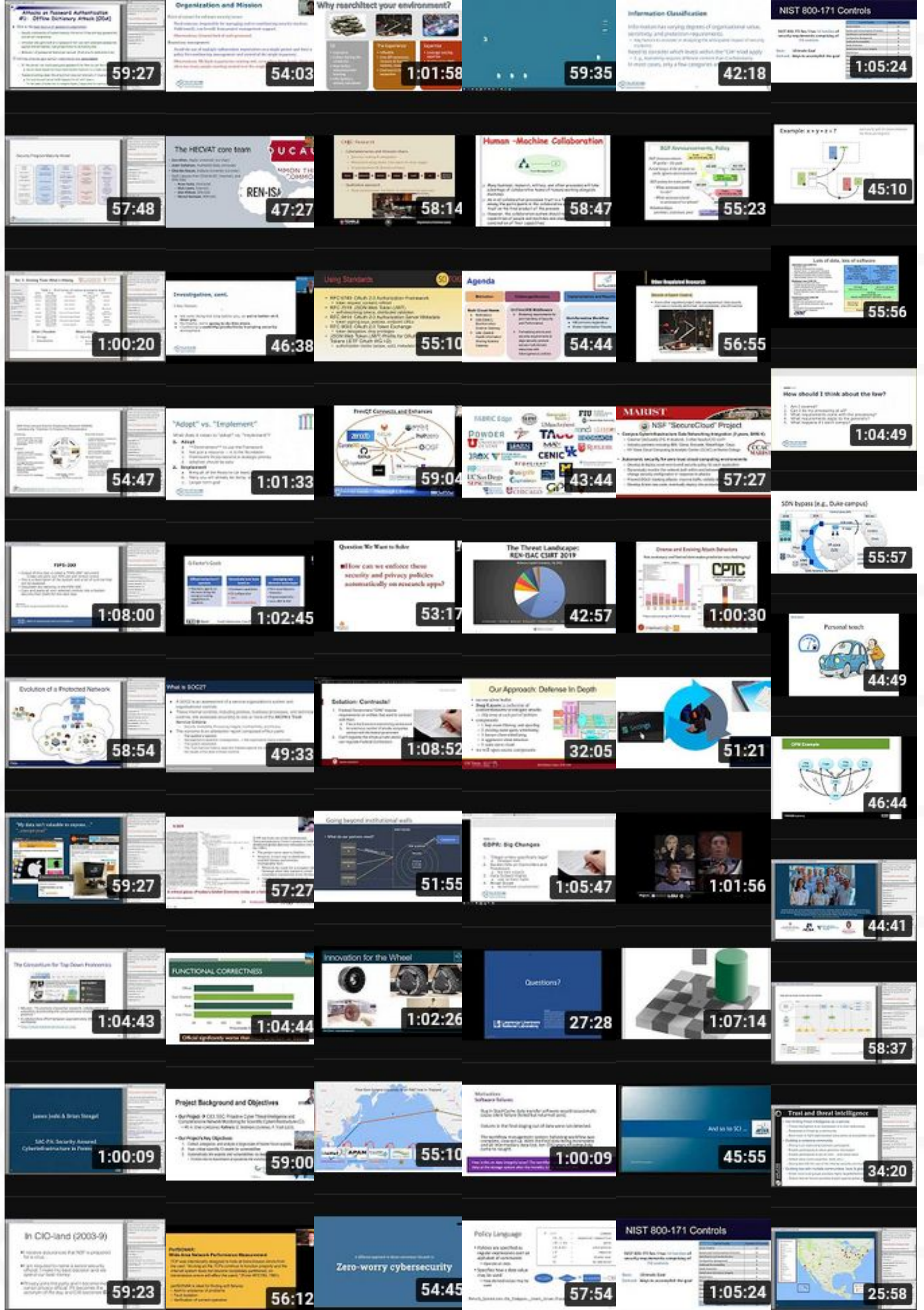
TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Trusted CI Webinars

- Call for 2023 webinar topics now open
- Visit https://www.trustedci.org/webinars for recordings and presentation materials



TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE



Annual NSF Cybersecurity Summit

One day of training and workshops.

1.5 days of plenary sessions.

Lessons learned and success from community.

October 18-20, 2022 in Bloomington, Indiana and online.

October 2023 in Berkeley, California.

https://trustedci.org/summit/

Trusted CI Partners

https://trustedci.org/partners

THE QUILT

FABRIC

SGCI Science Gateways Community Institute

InCommon®

PATh

NORTHEAST BIG DATA INNOVATION HUB

EDUCAUSE HEISC

EPOC Engagement and Performance Operations Center

Software Sustainability Institute

OSG

MIDWEST BIG DATA HUB

women in CYBERSECURITY WiCyS

CICompass

ACCESS

REN-ISAC

ResearchSOC

MINORITY SERVING–CYBERINFRASTRUCTURE CONSORTIUM In partnership with INTERNET2

ESnet ENERGY SCIENCES NETWORK

WISE COMMUNITY

TRUSTED CI THE NSF CYBERSECURITY CENTER OF EXCELLENCE

SOUTH BDHUB

CPP SFS

WEST BIG DATA INNOVATION HUB

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/

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Trusted CI License Statement

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE