

# Welcome to the Trusted CI Cybersecurity Workshop

**Jim Basney**  
Director, Trusted CI

September 16, 2022

# Cybersecurity Workshop Agenda

Start time	Title and description	Presenter(s)
1:30	<b>Welcome and session overview</b>	<b>Jim Basney</b> , Trusted CI Director
1:40	<b>JASON advisory report on Cybersecurity at NSF Major Facilities</b>	<b>Jim Ulvestad</b> , NSF Senior Advisor for Research Security
2:10	<b>Cybersecurity in the Research Infrastructure Guide (RIG)</b>	<b>Dr. Robert Beverly</b> , NSF Program Director
2:40	<b>Panel: Building Cybersecurity Programs at NSF Major Facilities</b>	<b>Moderator:</b> Scott Russell, Trusted CI <b>Panelists:</b> Craig Risien (OOI), Doug Ertz (GAGE), Wade Craig (NRAO), Craig Jackson (IU CACR / Trusted CI)
3:15	Break	
3:30	<b>Ransomware roundtable</b>	<b>Ryan Kiser</b>
4:00	<b>Insider edition: What ResearchSOC <i>really</i> does with NSF facilities</b>	<b>Susan E. Sons</b> , Executive Director of OmniSOC and ResearchSOC
4:25	<b>Closing</b>	<b>Jim Basney</b> , Trusted CI Director



# 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.



<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

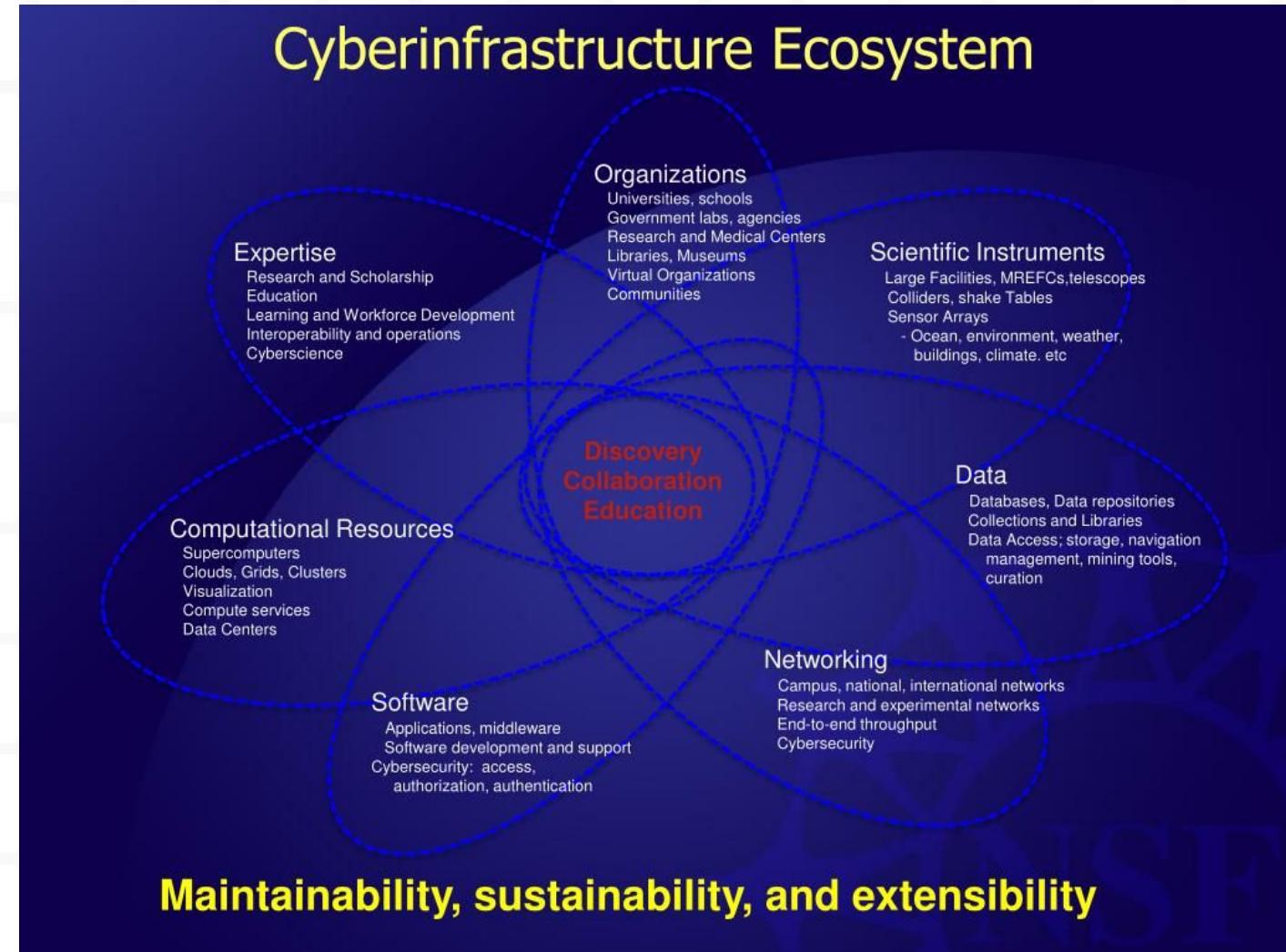


Image credit: NSF

# 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.

No registration fee.

<https://trustedci.org/summit/>





# The Trusted CI Framework

<https://trustedci.org/framework>

- Guidance for cybersecurity programs organized under 4 Pillars: **Mission Alignment**, **Governance**, **Resources**, and **Controls**
- Vetted by and tailored to the open science community.
- Adoption supported through six month cohorts
- Since January 2022, over half of NSF's Major Facilities have completed a cohort engagement or are currently participating in a cohort: GAGE, LIGO, NEON, NOIRLab, NRAO, NSO, OOI, and SAGE.
- Call for participation now open for 2023 1H Cohort:

<https://www.trustedci.org/framework/cohort>

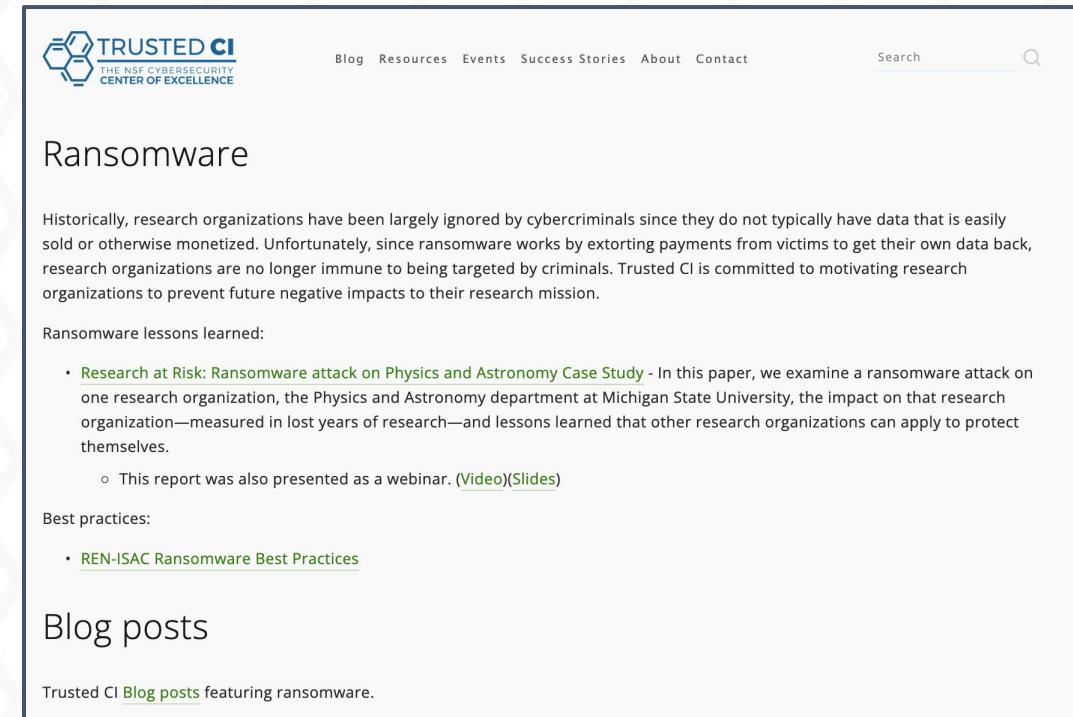
# Growing Ransomware Risk to Science

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>



The screenshot shows the Trusted CI website's header with the logo and navigation links: Blog, Resources, Events, Success Stories, About, Contact, and a Search bar. The main content area is titled "Ransomware". It includes a paragraph about the historical impact of ransomware on research organizations and Trusted CI's commitment to prevent future negative impacts. Below this is a section titled "Ransomware lessons learned:" with a bullet point about a research paper on a Physics and Astronomy department attack. It also mentions a webinar with video and slides. A "Best practices:" section lists a link to REN-ISAC Ransomware Best Practices. Finally, a "Blog posts" section indicates that Trusted CI has blog posts featuring 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.

# MSU Physics and Astronomy Case Study

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

Department estimated impact on science measured in years of lost productivity.

Report available at: <https://hdl.handle.net/2022/26638>

Webinar recording: [https://youtu.be/\\_Ay2jUxthfw](https://youtu.be/_Ay2jUxthfw)

Slides: <http://hdl.handle.net/2142/112812>



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

Aug 1, 2021

*Distribution:* **Public**

Authors: Andrew Adams<sup>1</sup>, Tom Siu, Julie Songer, Von Welch

<sup>1</sup> Engagement Lead, Andrew Adams

# Annual Challenge: Operational Technology

- Year 3 focuses on investigating the use of Operational Technology(OT) at NSF major scientific research facilities
- OT is the use of hardware and software to monitor and control physical processes, devices, and infrastructure
- Increasingly important in the context of science and research leveraging instruments like telescopes, biological and chemical reactors, sonar, and even vehicles used in scientific discovery
- Annual Challenge team is engaging with IT and OT personnel discussing operations at a variety of NSF Major Research Facilities

Develop a multi-year roadmap of security recommendations to advance the security of scientific operational technology for NSF facilities



# Next: Jim Ulvestad

# Trusted CI Cybersecurity Workshop Closing

**Jim Basney**  
Director, Trusted CI

September 16, 2022

# Thanks!

# 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](mailto: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](mailto: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, and 1920430. 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/>

