TRUSTED CI

THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

trustedci.org

Trusted CI's Secure by Design

John Zage

Security Engineer, Trusted CI

RVTEC

October 21st, 2024

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

A Brief Introduction to Trusted CI

John Zage

Security Engineer, Trusted CI

RVTEC

October 21st, 2024

TRUSTED CI

THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Trusted CI:
The NSF Cybersecurity Center of Excellence

Our mission: Trusted CI enables trustworthy NSF science by partnering with cyberinfrastructure (CI) operators to build and maintain effective cybersecurity programs, publishing resources that are valuable to the broader NSF community, and supporting the processes, tools, and knowledge to secure NSF research progress.

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

I | NCSA

PSC
PITTSBURGH SUPERCOMPUTING CENTER

BERKELEY LAB

ASU Arizona State University

SUSTAINABLE HORIZONS INSTITUTE

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://trustedci.org/

Highlights of The Past Five Years of Trusted CI

Development of the ***Trusted CI Framework*** and Trusted CI ***Framework Implementation Guide*** *(FIG)*

Establishment of **five Framework Adoption Cohorts** (ARF participated in 2023)

Impact the 2022 NSF **Research Infrastructure Guide (RIG)**, which references the FIG and closer alignment with the Trusted CI Framework (§6.3).

Through deep foci in specific domains, gained insights into **trustworthy data**, **software assurance**, **operational technology**, and **security by design** — developed the *Trusted CI Guide to Securing Software*, the *Roadmap for Securing Operational Technology*, and *OT Vendor Procurement Matrix.*

Worked with CCRV and RCRV on **Secure by Design**

Hosted the (growing) annual **NSF Cybersecurity Summit** to now **over 150 attendees** each year.

Six month engagement with ARF in 2019

NSF Cybersecurity Summit

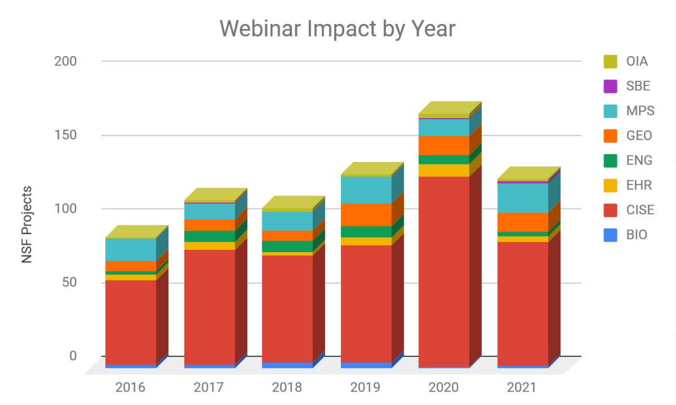
- October 20-24, 2025 at Boulder, CO
- Program agenda is community-driven based on responses to community polling, session proposal submissions, and trending topics
- Summit format includes:
  - Plenary sessions
    - Presentations
    - Panel discussions
    - Lightning talks
  - Workshops and training
  - BoFs and "Community of Practice" meetings
- Videos of sessions available online

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

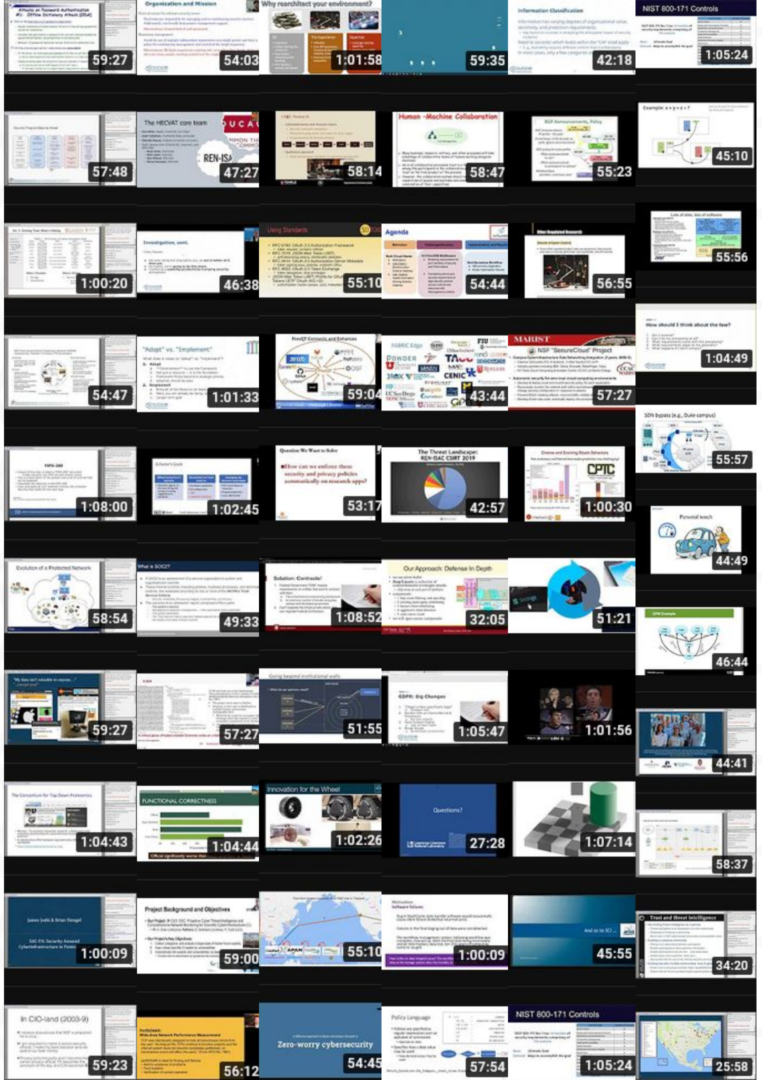
https://trustedci.org/summit

Trusted CI Webinars

- Provides readily available cybersecurity services tailored to the NSF science community
- Webinars are presented live on the 4th Monday of the month
- Visit https://www.trustedci.org/webinars for recordings and presentation materials



TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE



The Trusted CI Framework

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

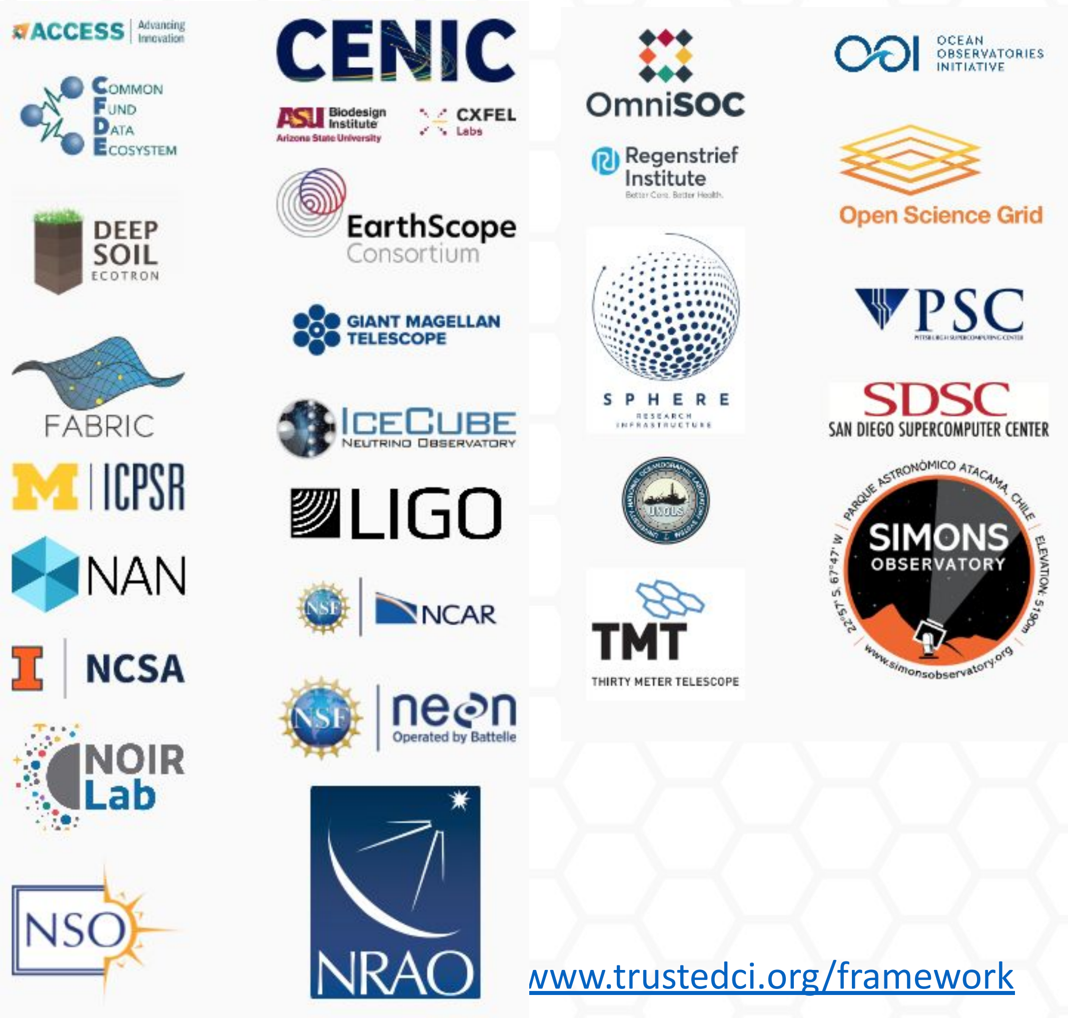
- 16 clear and concise requirements.
- Based on best practices and evidence of what works.
- Designed to be universal and timeless.

It focuses on foundational decisions about:
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 Adopters


ACCESS Advancing Innovation
Common Fund Data Ecosystem
Deep Soil Ecotron
FABRIC
M ICPSR
NAN
I NCSA
NOIR Lab
NSO
CENIC
ASU Biodesign Institute Arizona State University
CXFEL Labs
EarthScope Consortium
Giant Magellan Telescope
IceCube Neutrino Observatory
LIGO
NSF NCAR
NSF neon Operated by Battelle
NRAO
OmniSOC
Regenstrief Institute Better Care. Better Health.
SPHERE Research Infrastructure
UNOLS
TMT Thirty Meter Telescope
OOI Ocean Observatories Initiative
Open Science Grid
PSC Pittsburgh Supercomputing Center
SDSC San Diego Supercomputer Center
Simons Observatory Parque Astronómico Atacama, Chile 22°57' S, 67°47' W Elevation: 5190m www.simonsobservatory.org

www.trustedci.org/framework

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

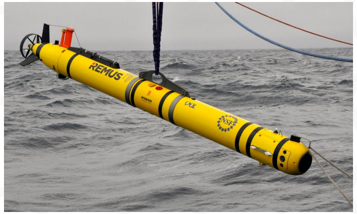
Ambassadors to Major Facilities

To better support the cybersecurity needs of the NSF Major Facilities, Trusted CI now assigns a staff member as an "ambassador" to each facility. This helps Trusted CI maintain connections with all the facilities, including an up-to-date understanding of cybersecurity needs.

https://www.trustedci.org/ambassadors

Security by Design of NSF Major Facilities

- 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.
  - Support acceptance testing of the NSF-funded Regional Class Research Vessels (RCRVs) at Oregon State University
  - Support Scripps Institution of Oceanography's design of the California Coastal Research Vessel (CCRV).
  - Support the Ocean Observatories Initiative (OOI)'s refresh of its fleet of gliders and other AUVs
  - Engage with the U.S. Antarctic Program (USAP)'s design of the Antarctic Research Vessel (ARV)
- Trusted CI will continue to support these and other interested NSF facilities with CI undergoing design, construction, or refresh to support security early in the process.



U.S. Antarctic Program

OCEAN OBSERVATORIES INITIATIVE

U.S. Academic Research Fleet

https://blog.trustedci.org/2023/01/announcing-2023-trusted-ci-annual.html

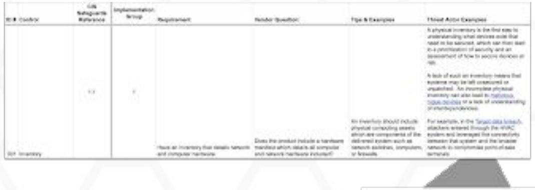
Security by Design of NSF Major Facilities

In late 2023, Trusted CI published the **Operational Technology Procurement Vendor Matrix** to assist those in leadership roles during the procurement process.

Intended to help formulate questions for vendors to discuss security controls on OT devices associated with research CI.

The Matrix includes controls, control requirements, questions for vendors, tips, mappings to standards (e.g., CIS), and real-world examples justifying controls.

Sept. 2024: **Version 2** published including additional columns, including mappings to MITRE ATT&CK, and ISO/IEC 27002 and 62443; also ***Guide to Using the Trusted CI OT Procurement Matrix***



ID #	Control	CIS Safeguards Reference	Implementation Group	Requirement	Vendor Question	Tips & Examples	Threat Actor Examples
001	Inventory	1.1	1	Have an inventory that details network and computer hardware	Does the product include a hardware manifest which details all computer and network hardware included?	An inventory should include physical computing assets which are components of the delivered system such as network switches, computers, or firewalls.	A physical inventory is the first step to understanding what devices exist that need to be secured, which can then lead to a prioritization of security and an assessment of how to secure devices at risk. A lack of such an inventory means that systems may be left unsecured or unpatched. An incomplete physical inventory can also lead to malicious, rogue devices or a lack of understanding of interdependencies. For example, in the Target data breach, attackers entered through the HVAC system and leveraged the connectivity between that system and the broader network to compromise point-of-sale terminals.

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

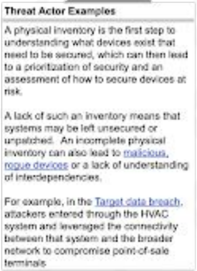
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Image source: Ghazi, Mohammed & Mohamed, Hashim & Ali, Mohammed (2020). Ransomware Attack: Rescue-checklist Cyber Security Awareness Program. Artificial Intelligence Advances. 1. 10.30564/aia.v1i1.1962.



Threat Actor Examples

A physical inventory is the first step to understanding what devices exist that need to be secured, which can then lead to a prioritization of security and an assessment of how to secure devices at risk.

A lack of such an inventory means that systems may be left unsecured or unpatched. An incomplete physical inventory can also lead to malicious, rogue devices or a lack of understanding of interdependencies.

For example, in the Target data breach, attackers entered through the HVAC system and leveraged the connectivity between that system and the broader network to compromise point-of-sale terminals.

zenodo.org/records/13830599

zenodo.org/records/13743314

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

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

women in cybersecurity WiCyS

Software Sustainability Institute

OSG

MIDWEST BIG DATA HUB

MINORITY SERVING-CYBERINFRASTRUCTURE CONSORTIUM in partnership with INTERNET2

CICompass

ACCESS

REN-ISAC

OmniSOC

RRCoP

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

Slack

Email 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

NSF Cybersecurity Summit

October 20-24, 2025 | Boulder, CO
https://www.trustedci.org/summit

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

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

Experiences from SIO (CCRV), OSU (RCRV), and OOI in Cybersecure-by-Design with their collaborations with Trusted CI's Secure By Design Team

2024 RVTEC

John Zage, moderator

October 21st, 2024

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Panelists

- **Christopher Romsos (OSU)**: RCRVs
- **Jon Meyer (SIO)**: CCRV
- **Craig Risien (OSU)**: OOI

Chris Romsos

Chris Romsos is a Systems Engineer for the Regional Class Research Vessel Project at Oregon State University where he's contributed to the scientific design and specifications for the RCRVs and now works with the vessel transition team.

Jon Meyer

Jon Meyer is Information Systems Manager within Shipboard Technical Support at Scripps Institution of Oceanography, helping lead SIO's oceanographic fleet in collecting and distributing high quality data from our oceans, worldwide, including security.

Craig Risien

Craig Risien is the project manager for the NSF Ocean Observatories Initiative (OOI) data center that Oregon State University has operated and maintained since July 2021. He is currently working with the OOI CI Systems team and Dell EMC to design and build a new data center that will support OOI through September 2028.

Procurement Vendor Matrix Examples from RCRV

Vendor Name	ID# and Question	Answer
Vendor 1	10. Can accounts be disabled, including unused default accounts?	No. They can only be added or removed in development.
Vendor 2	3. Will the product receive software security patches throughout the product's intended lifecycle?	Can be setup on email updates for software/firmware updates
Vendor 2	10. Can accounts be disabled, including unused default accounts?	No OS on devices, Only one access into WinDiscovery/ password

Procurement Vendor Matrix Examples from RCRV

Vendor Name	ID# and Question	Answer
Vendor 3	3. Will the product receive software security patches throughout the product's intended lifecycle?	Yes, for IPTV server. STB are using unsupported Android version.
Vendor 3	14. When connected to the internet, can the product software be configured to automatically apply security updates?	System is not connected to the Internet