# Trusted CI's approach to security for open science projects

**Jim Basney**

jbasney@ncsa.illinois.edu

13th FIM4R Workshop: Federated Identity Management for Research Collaborations

February 11, 2019

TRUSTED CI

THE NSF CYBERSECURITY CENTER OF EXCELLENCE

# Trusted CI:
## The NSF Cybersecurity Center of Excellence

Our mission: to provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

NCSA

INTERNET2®

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

PITTSBURGH SUPERCOMPUTING CENTER

BERKELEY LAB

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

https://trustedci.org/

# Trusted CI: Impacts

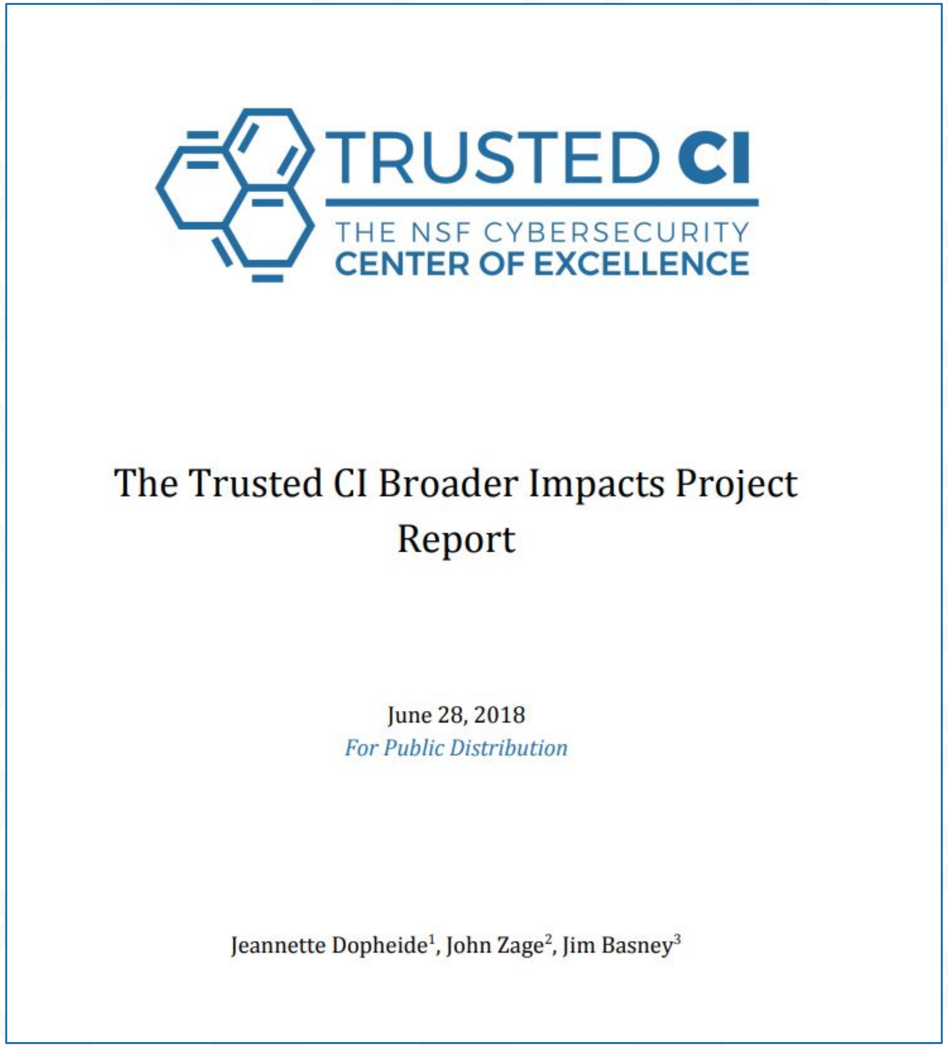
Trusted CI has impacted over 190 NSF projects since inception in 2012.

More than 150 members of NSF projects attended our NSF Cybersecurity Summit.

Seventy NSF projects attended our monthly webinars.

We have provided more than 250 hours of training to the community.

Thirty-five engagements, including nine NSF Large Facilities.



TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

The Trusted CI Broader Impacts Project Report

June 28, 2018
*For Public Distribution*

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

https://hdl.handle.net/2022/22148

# Community-driven Guidance

Security Best Practices for Academic Cloud Service Providers

https://trustedci.org/cloud-service-provider-security-best-practices/

Operational Security

https://trustedci.org/guide

Identity Management Best Practices

https://trustedci.org/iam

Open Science Cyber Risk Profile

https://trustedci.org/oscrp/

CTSC
CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

Guide to Developing Cybersecurity Programs for
NSF Science and Engineering Projects

Version 1
August 2014

CTSC
CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

Securing Commodity IT in Scientific CI Projects
Baseline Controls and Best Practices

Version 2.0
st 2014

CTSC
CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

Identity Management Best Practices
A CTSC Blog Series

November 2015
*For Public Distribution*

Jim Basney

*Identity Management Best Practices* | CTSC

Agave Platform
Cornell University
Center for Advanced Computing
CYVERSE
Jetstream
TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Security Best Practices for Academic
Cloud Service Providers

Version 1.0

http://hdl.handle.net/2022/22123

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

# Annual NSF Cybersecurity Summit

One day of training and workshops.

Agenda driven by call for participation.

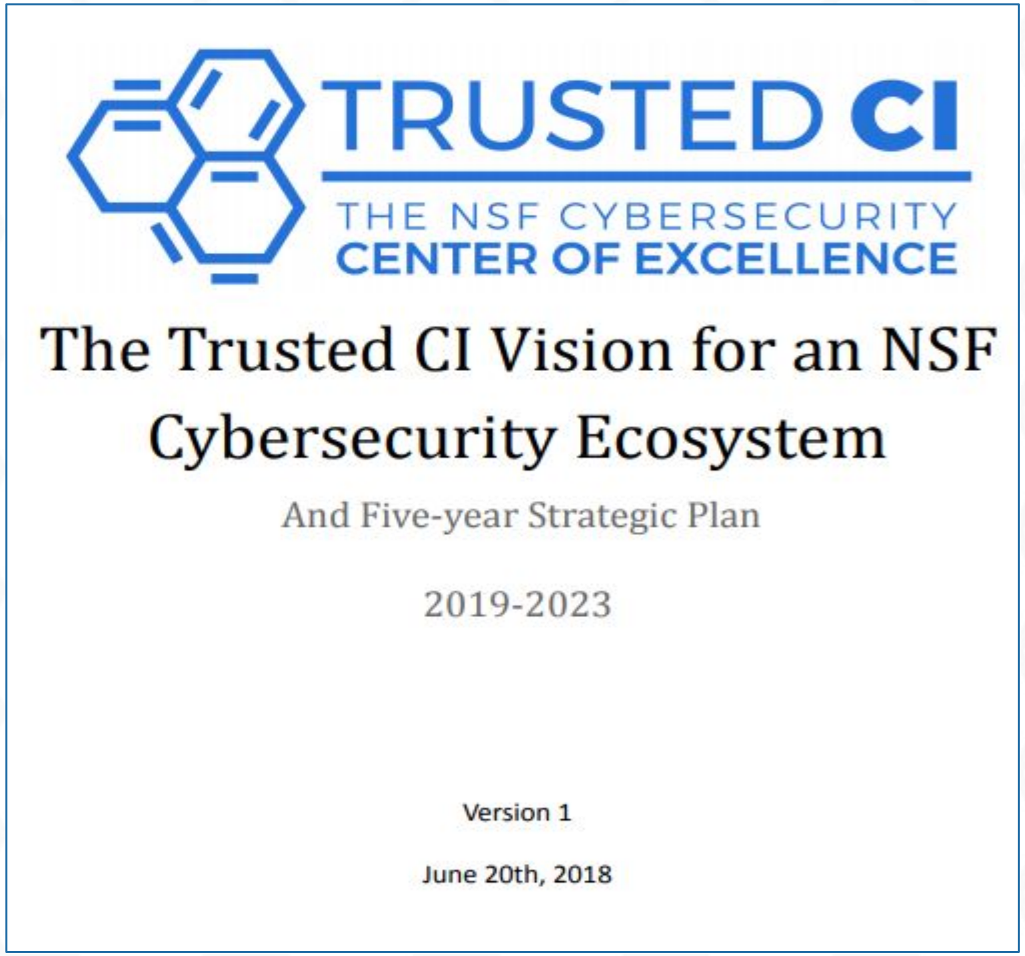
Lessons learned and success from community.

Will be in San Diego in 2019.

https://trustedci.org/summit/

# Trusted CI 5-year Vision and Strategic Plan

"A NSF cybersecurity ecosystem, formed of people, practical knowledge, processes, and cyberinfrastructure, that enables the NSF community to both manage cybersecurity risks and produce trustworthy science in support of NSF's vision of a nation that is the global leader in research and innovation."



TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

The Trusted CI Vision for an NSF Cybersecurity Ecosystem

And Five-year Strategic Plan

2019-2023

Version 1

June 20th, 2018

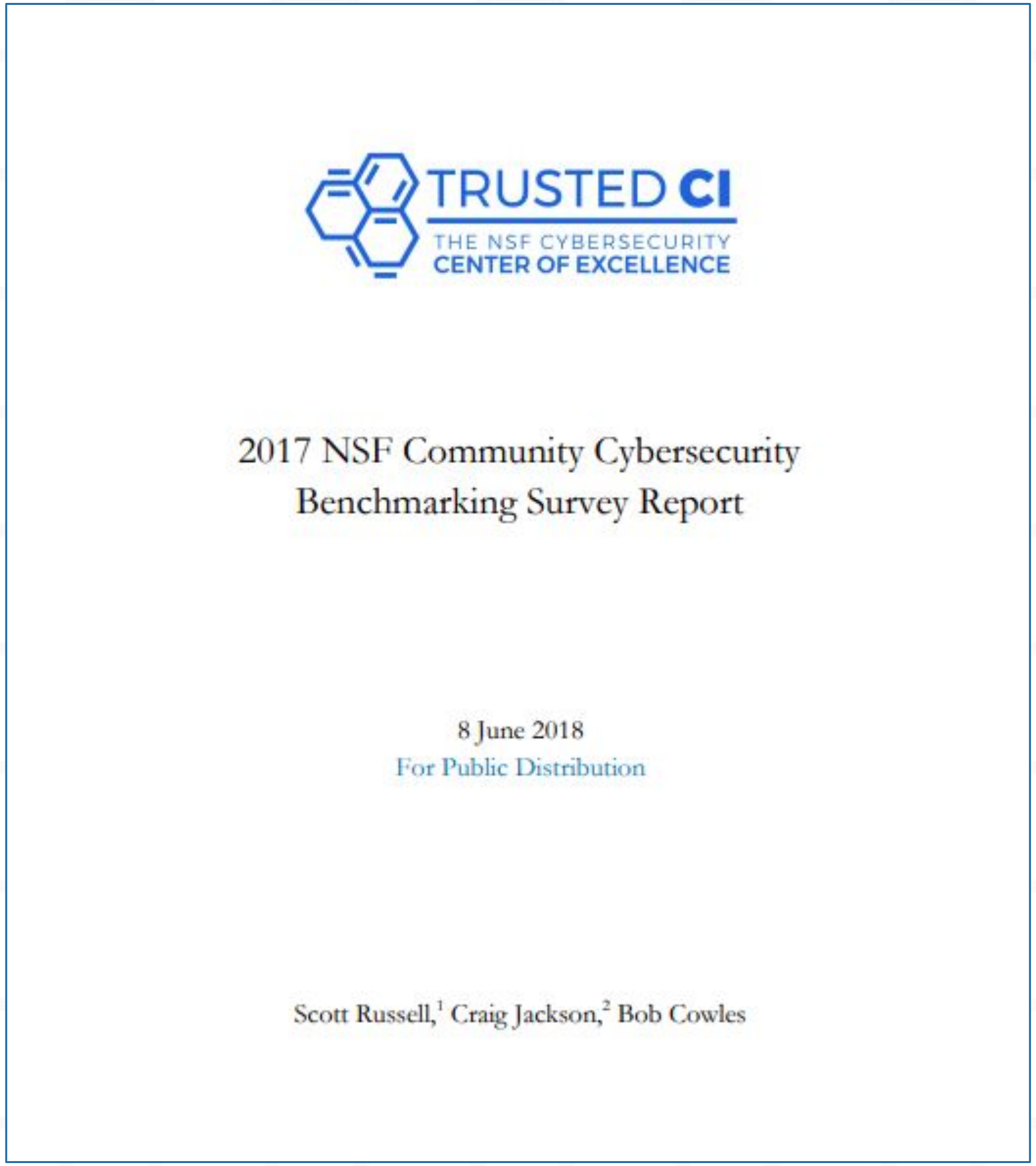
https://hdl.handle.net/2022/22178

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

# Community Benchmarking

Some select results:

- Respondents’ cybersecurity budgets vary widely.
- Respondents inconsistently establish cybersecurity officers.
- Residual risk acceptance is inconsistently practiced.



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

2017 NSF Community Cybersecurity Benchmarking Survey Report

8 June 2018
For Public Distribution

Scott Russell,[1] Craig Jackson,[2] Bob Cowles

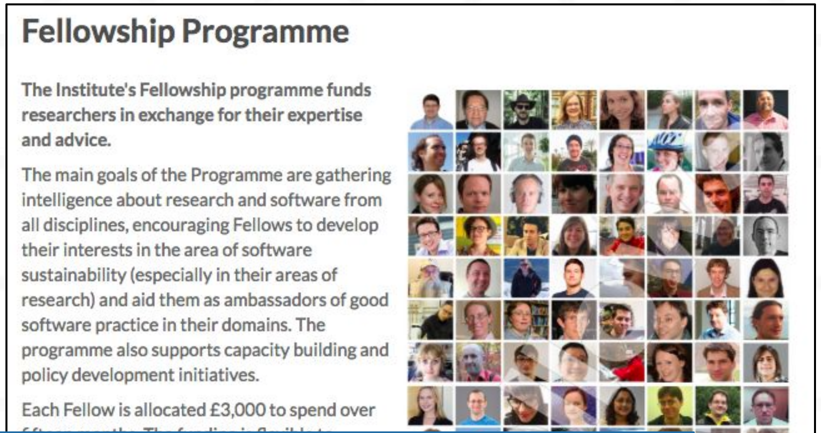
https://hdl.handle.net/2022/22171

# A Network of Cybersecurity Fellows

Fellows are liaisons between Trusted CI and communities.

Fellows receive training, travel support, and prioritized support.

Building on models from UK Software Sustainability Institute, ACI-REFs, Campus Champions.

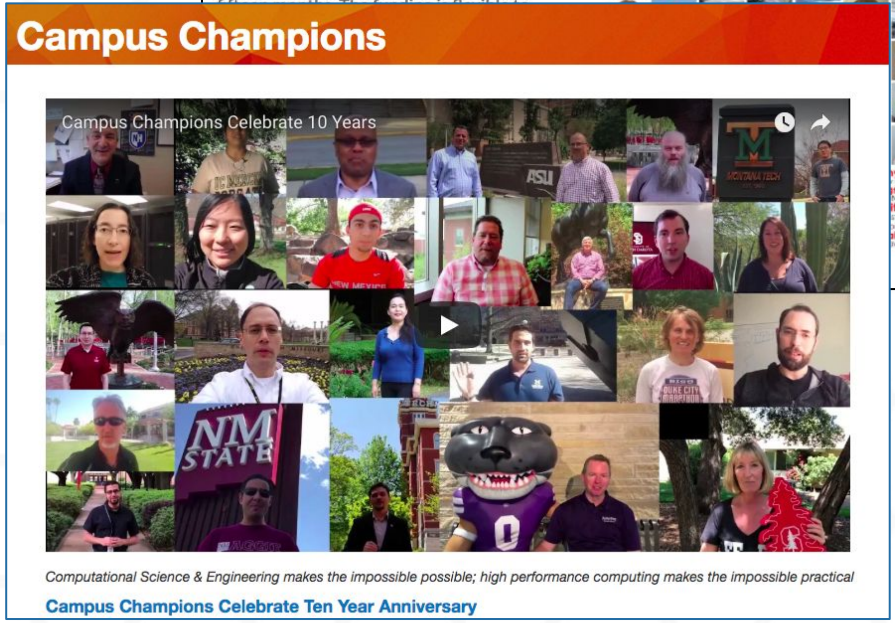


## Fellowship Programme

The Institute's Fellowship programme funds researchers in exchange for their expertise and advice.

The main goals of the Programme are gathering intelligence about research and software from all disciplines, encouraging Fellows to develop their interests in the area of software sustainability (especially in their areas of research) and aid them as ambassadors of good software practice in their domains. The programme also supports capacity building and policy development initiatives.

Each Fellow is allocated £3,000 to spend over



## Campus Champions

Campus Champions Celebrate 10 Years

*Computational Science & Engineering makes the impossible possible; high performance computing makes the impossible practical*

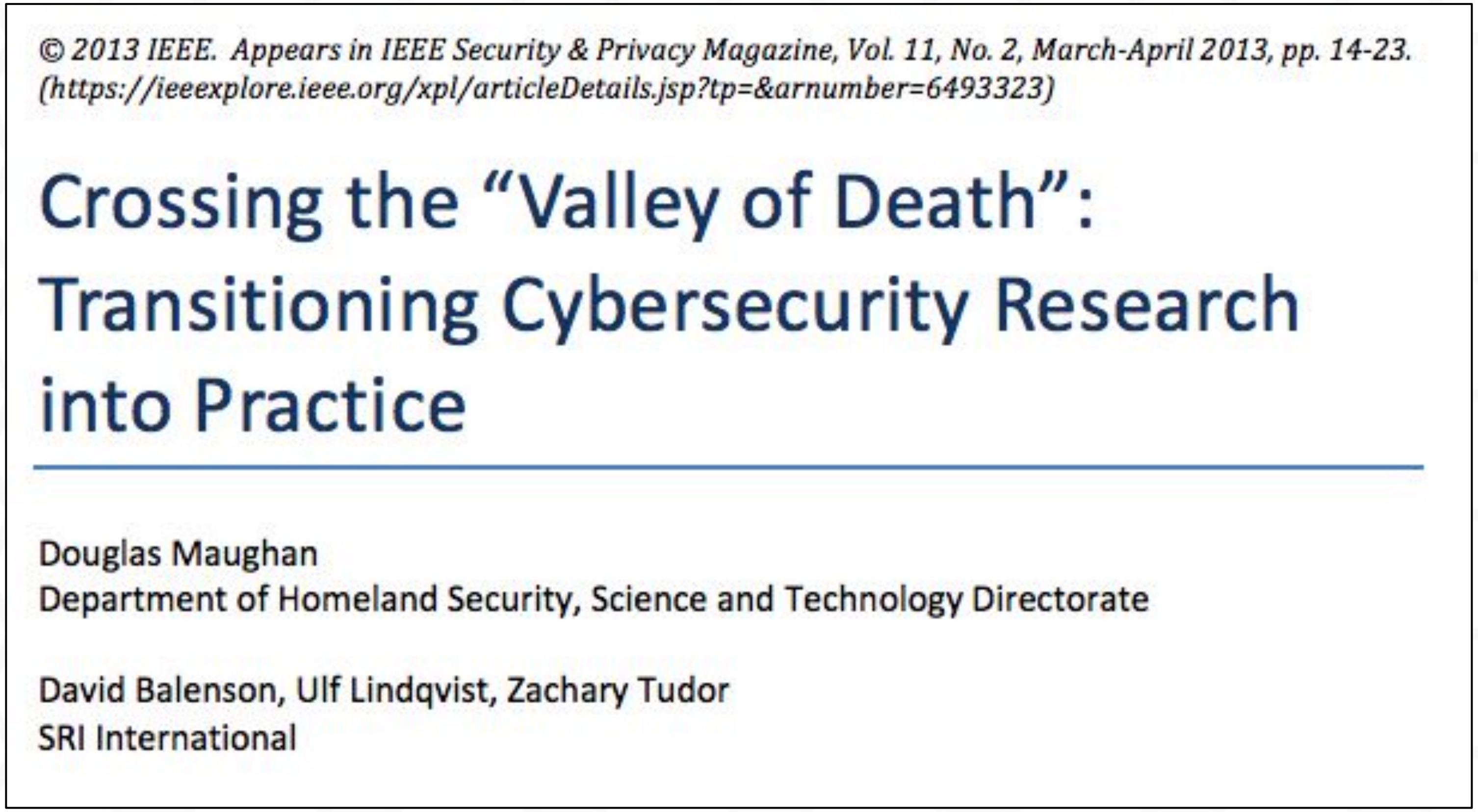
Campus Champions Celebrate Ten Year Anniversary

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

# Cybersecurity Transition to Practice (TTP)

Migrating cybersecurity research into practice is itself a research challenge with technical, human factor, and economic aspects.

contact:
TTP@trustedci.org



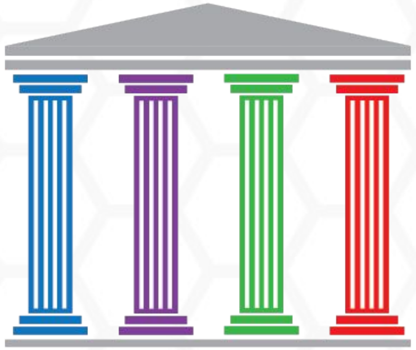
*© 2013 IEEE. Appears in IEEE Security & Privacy Magazine, Vol. 11, No. 2, March-April 2013, pp. 14-23. (https://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6493323)*

## Crossing the "Valley of Death": Transitioning Cybersecurity Research into Practice

Douglas Maughan
Department of Homeland Security, Science and Technology Directorate

David Balenson, Ulf Lindqvist, Zachary Tudor
SRI International

# The Trusted CI Framework



Framework Core:

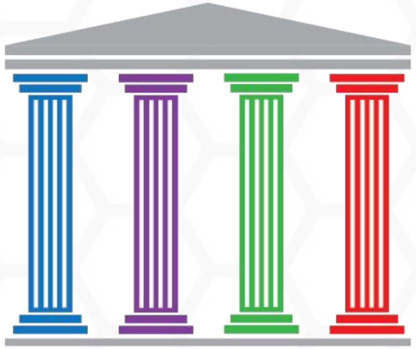
- Concise, clear minimum requirements for cybersecurity programs organized under the 4 Pillars: Mission Alignment, Governance, Resources, and Controls
- Based in general cybersecurity best practice and evidence of what works.
- Infrequent updates.

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.

**Coming soon!**

# Framework Pillars



## Mission Alignment

- Information classification, asset inventory, external requirements

## Governance

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

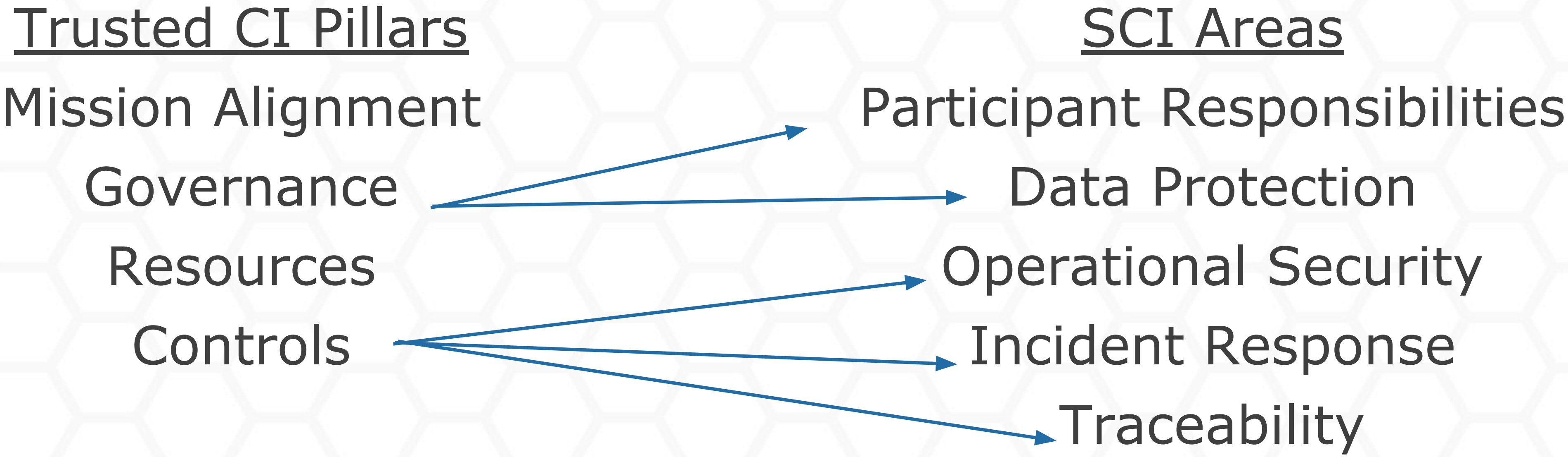
## Resources

- People, budgets, services and tools

## Controls

- Procedural, technical, administrative safeguards and countermeasures

# Harmonizing with SCI



Trusted CI Pillars

Mission Alignment

Governance

Resources

Controls

SCI Areas

Participant Responsibilities

Data Protection

Operational Security

Incident Response

Traceability

https://wise-community.org/sci/

# Open Science Cyber Risk Profile (OSCRP)

OSCRP helps leads of science projects understand cybersecurity risks to their science and prepare for discussing those risks with their campus security office.

OSCRP was created by a team of computer security experts and scientists working together through a series of example use cases, which were then generalized to form the basis of the document.

OSCRP provides a mechanism for applying controls to mission-specific assets.

https://trustedci.org/oscrp/

# OSCRP 2019 Planned Extensions

1. ***Data integrity*** issues in scientific computing, e.g., due to bit flips, are planned to be addressed.
2. ***Data privacy and confidentiality (e.g., PII, proprietary technologies)*** are planned to be explicitly addressed, including technical risk assessments.
3. Network-connected sensors and actuators (“***cyber-physical systems***”) are planned to be examined in more depth.
4. ***Mitigations*** are planned to be included.
5. Cross references with the Trusted CI Framework will be added.

# Other Trusted CI Services

**Cyberinfrastructure Vulnerabilities**

Latest news on security vulnerabilities tailored for cyberinfrastructure community.

https://trustedci.org/vulnerabilities/

**Specialized Information for Identity and Access Management, Science Gateways, Software Development**

https://trustedci.org/iam/

https://trustedci.org/science-gateway-community-institute/

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

**Large Facilities Security Team**

Working group of security representatives from NSF Large Facilities.

https://trustedci.org/lfst/

**Ask Us Anything**

No question too big or too small.

info@trustedci.org

**Follow Us**

https://trustedci.org

https://blog.trustedci.org

@TrustedCI

# Acknowledgments

Trusted CI is supported by the National Science Foundation under Grant ACI-1547272. 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