TRUSTED CI

THE NSF CYBERSECURITY CENTER OF EXCELLENCE

trustedci.org

Trusted CI Overview

Von Welch
PI and Director

InCommon Steering Committee Update

2020-02-03

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

INTERNET2

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

PITTSBURGH SUPERCOMPUTING CENTER

BERKELEY LAB

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

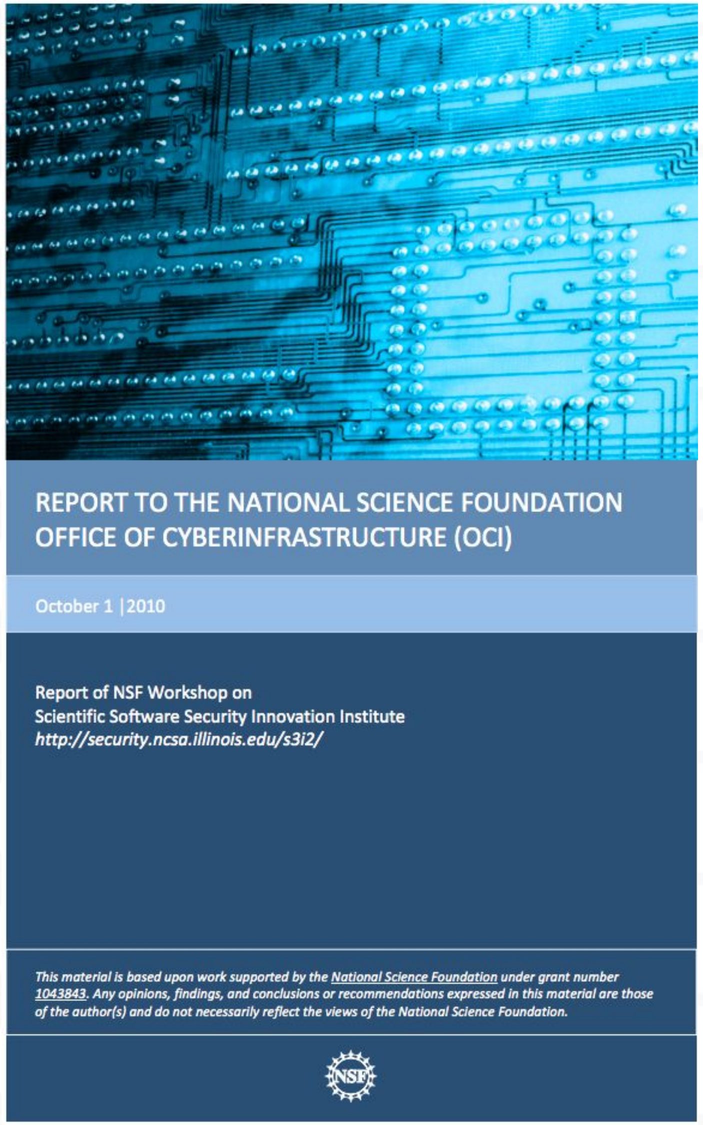
https://trustedci.org/

We don’t make the technology. We help you make sense of it.

Formed in 2012

Based on community call for leadership and guidance rather than technology

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE



REPORT TO THE NATIONAL SCIENCE FOUNDATION
OFFICE OF CYBERINFRASTRUCTURE (OCI)

October 1 |2010

Report of NSF Workshop on
Scientific Software Security Innovation Institute
http://security.ncsa.illinois.edu/s3i2/

This material is based upon work supported by the National Science Foundation under grant number 1043843. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Report to the National Science Foundation
Office of Cyberinfrastructure (OCI)

9 November 2011

Report of NSF Workshop Series on
Scientific Software Security Innovation Institute
http://security.ncsa.illinois.edu/s3i2/

This material is based upon work supported by the *National Science Foundation* under grant number *1043843*. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect

http://security.ncsa.illinois.edu/s3i2/

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

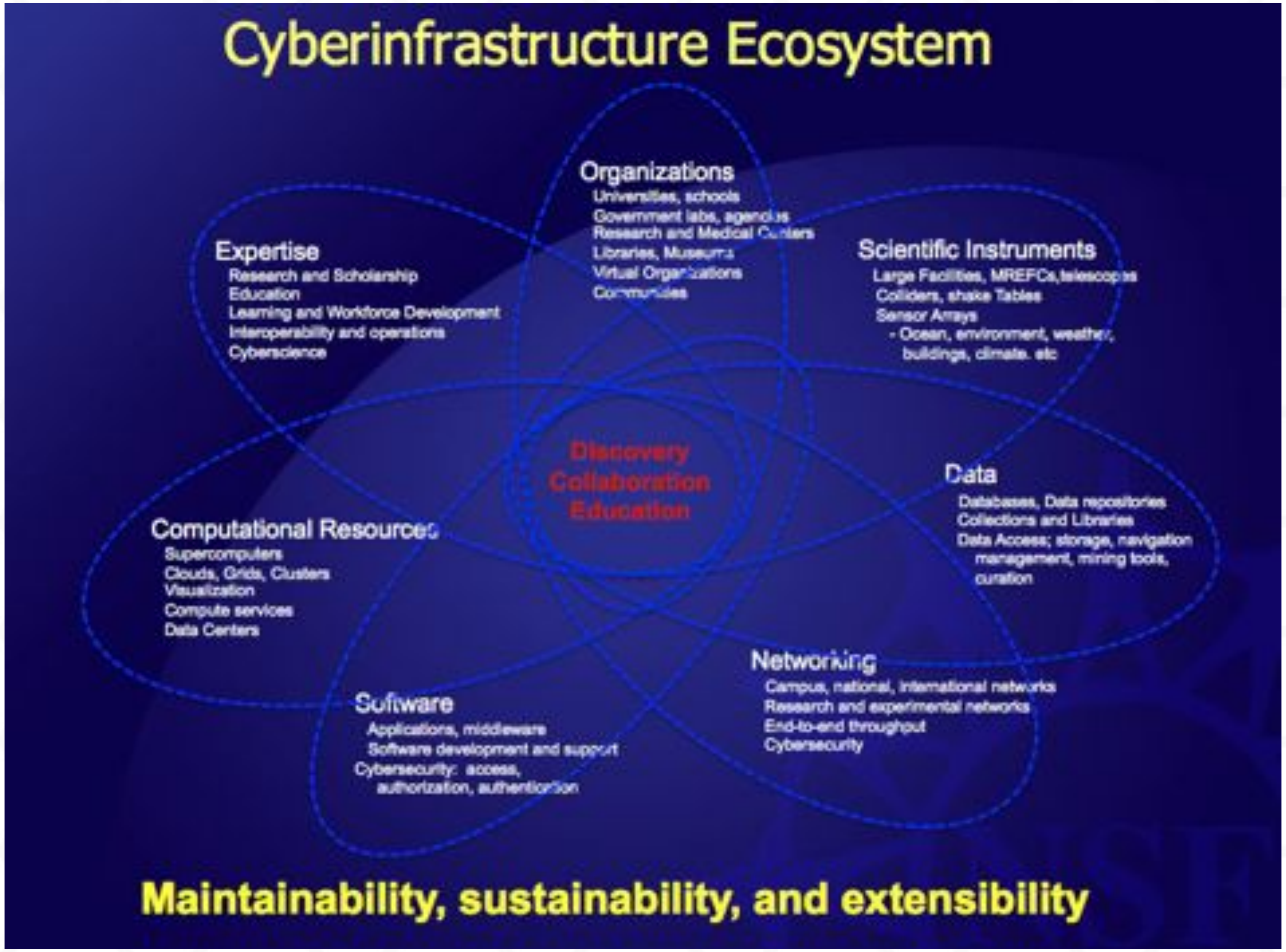
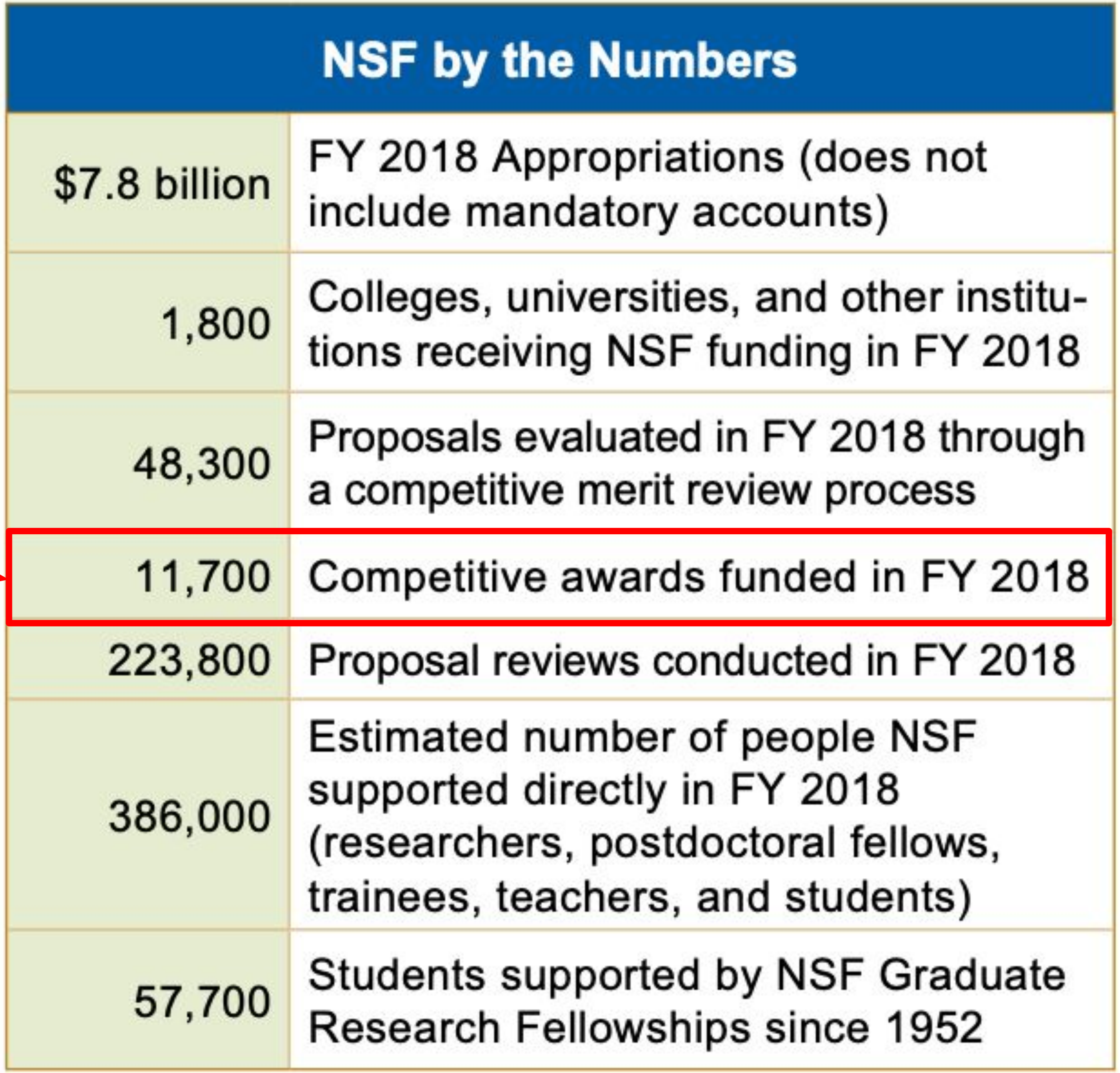

Cyberinfrastructure Ecosystem
Organizations
Universities, schools
Government labs, agencies
Research and Medical Centers
Libraries, Museums
Virtual Organizations
Communities
Expertise
Research and Scholarship
Education
Learning and Workforce Development
Interoperability and operations
Cyberscience
Scientific 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

~1,500 >$1m

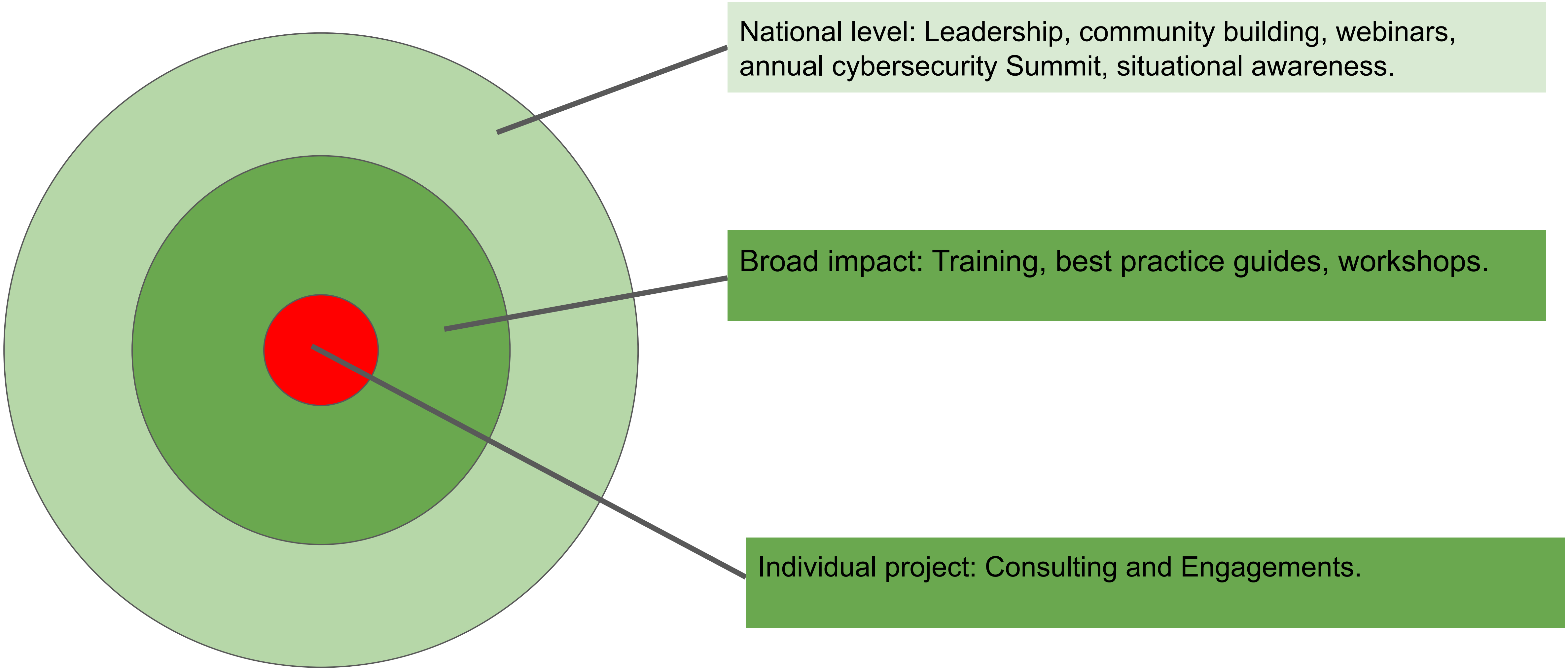


NSF by the Numbers

$7.8 billion	FY 2018 Appropriations (does not include mandatory accounts)
1,800	Colleges, universities, and other institutions receiving NSF funding in FY 2018
48,300	Proposals evaluated in FY 2018 through a competitive merit review process
11,700	Competitive awards funded in FY 2018
223,800	Proposal reviews conducted in FY 2018
386,000	Estimated number of people NSF supported directly in FY 2018 (researchers, postdoctoral fellows, trainees, teachers, and students)
57,700	Students supported by NSF Graduate Research Fellowships since 1952

https://www.nsf.gov/pubs/2019/nsf19003/nsf19003.pdf

Trusted CI: Scopes of Impact



National level: Leadership, community building, webinars, annual cybersecurity Summit, situational awareness.

Broad impact: Training, best practice guides, workshops.

Individual project: Consulting and Engagements.

Trusted CI: Impacts

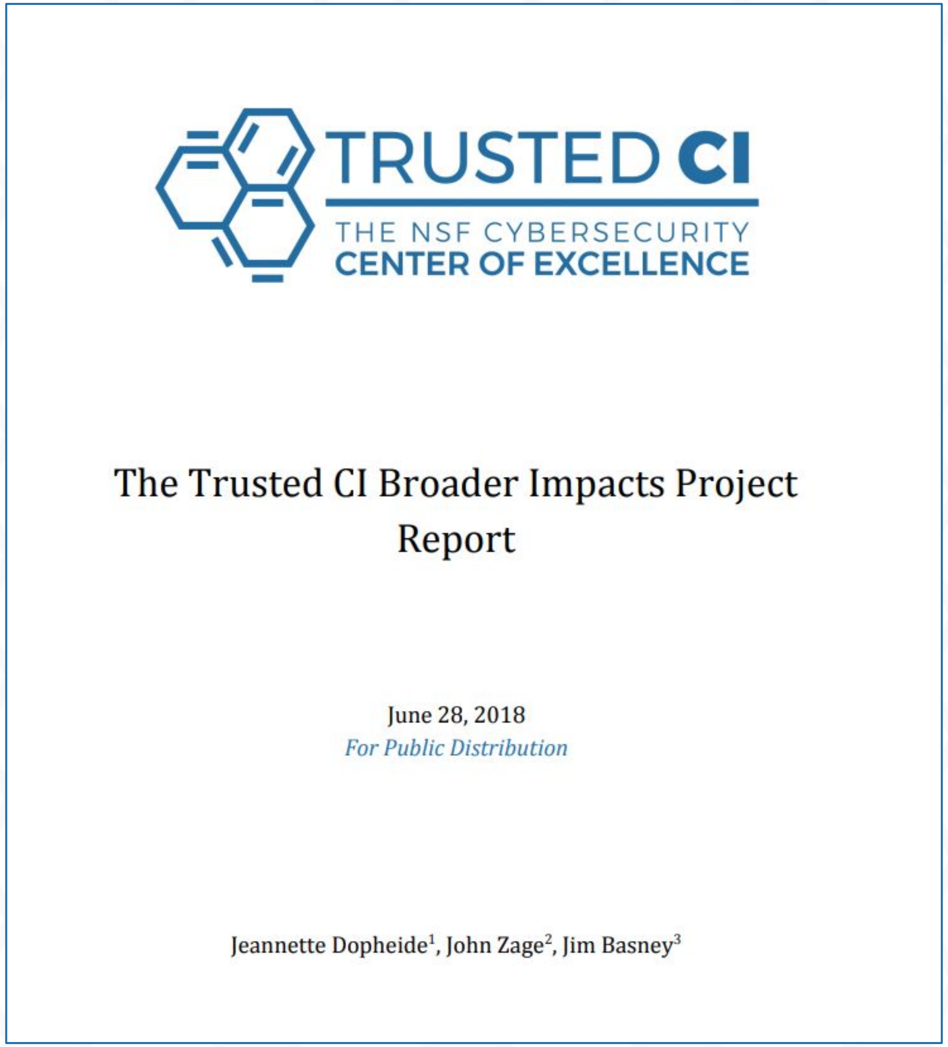
Trusted CI has positively impacted over 340 NSF projects since inception in 2012.

Members of more than 230 NSF projects have attended our NSF Cybersecurity Summit.

Members of more than 90 NSF projects have attended our monthly webinars.

We have provided more than 300 hours of training to the community.

We've had engagements with 44 projects, including ten 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

Best Practices

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

Science Gateways

- https://trustedci.org/sgci/

Software Assurance

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

Security Best Practices for Academic Cloud Service Providers

Version 1.0

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

Engagements: One-on-one Collaborations

Accept applications every six months:

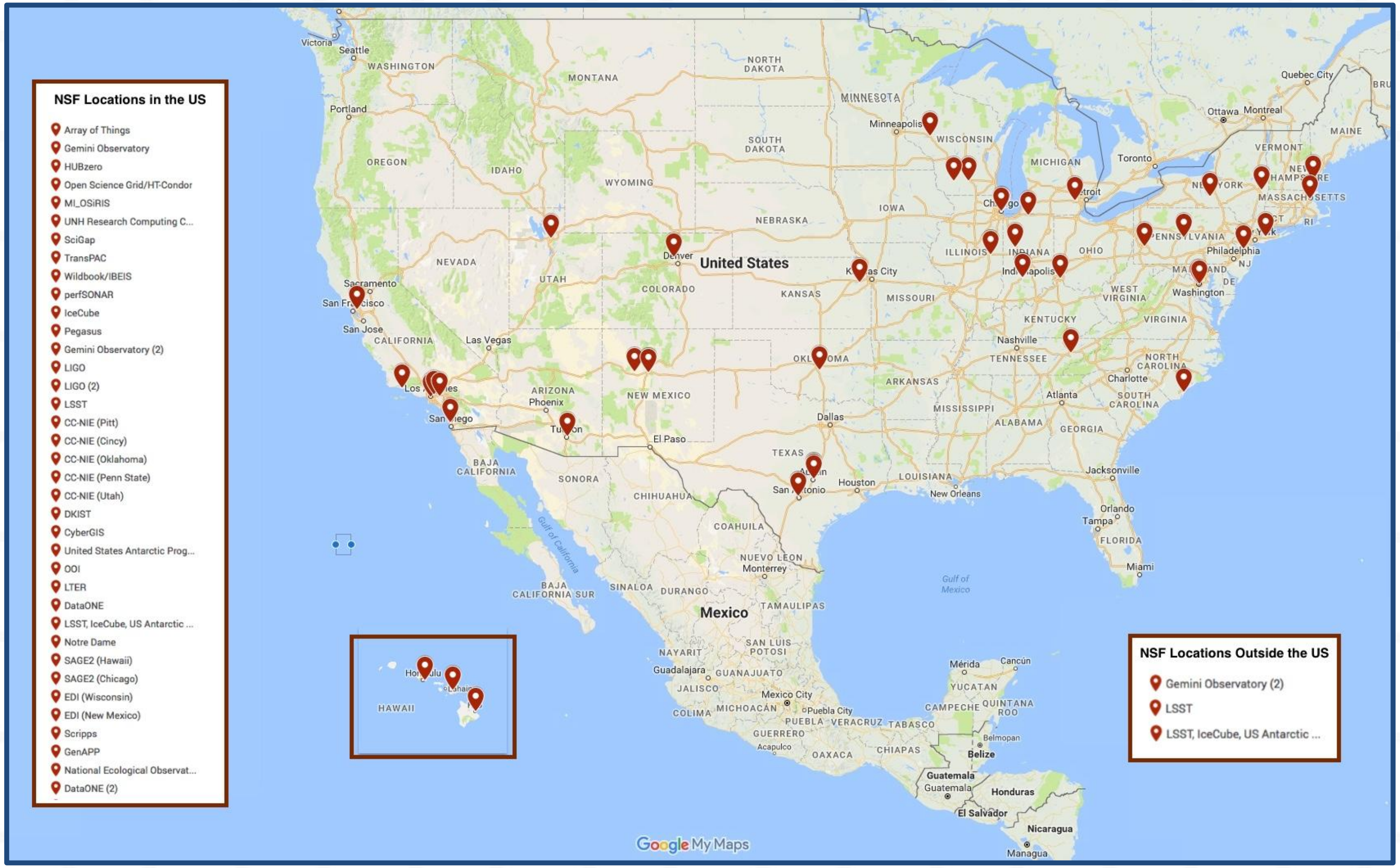
https://trustedci.org/application/

Next application window: Spring of 2020

- Creating an infosec program
- Evaluation of existing infosec program for systems and organizations.
- Software assessment
- Best infosec practices for paradigms
- Privacy

https://trustedci.org/engagedcommunities

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE



Example: Polar Geospatial Center

https://www.pgc.umn.edu/

- Supports U.S. polar scientists to complete their research goals
- Introduces new, state-of-the-art techniques from the geospatial field to effectively solve problems in the least mapped places on Earth.
- Engagement ran January-June, 2019.
- Rapidly mature PGC's cybersecurity program and develop a roadmap for future cybersecurity efforts.
- Trusted CI and PGC conducted a risk assessment of cyberinfrastructure assets, and then, driven by the results of the assessment, worked to build upon these results to improve PGC's security program.
- Leveraged Trusted CI Guide (https://trustedci.org/guide) to Developing Cybersecurity Programs for NSF Science and Engineering Projects and related materials.

Example: Array of Things
https://arrayofthings.github.io/

- Deploying 500 Array of Things (AoT) nodes to measure data on Chicago’s environment, infrastructure and activity.
- Support scientific investigation of solutions to urban challenges ranging from air quality to urban flooding.
- The ultimate goal of this innovative community technology platform is to help make cities cleaner, healthier and more livable.
- Engagement focused on cybersecurity and privacy implications.
- Reviewed system designs in the context of cybersecurity and privacy, providing security policy development guidance, and organizing expert discussions to inform privacy requirements and policies.

Annual NSF Cybersecurity Summit

One day of training and workshops.

Lessons learned and success from community.

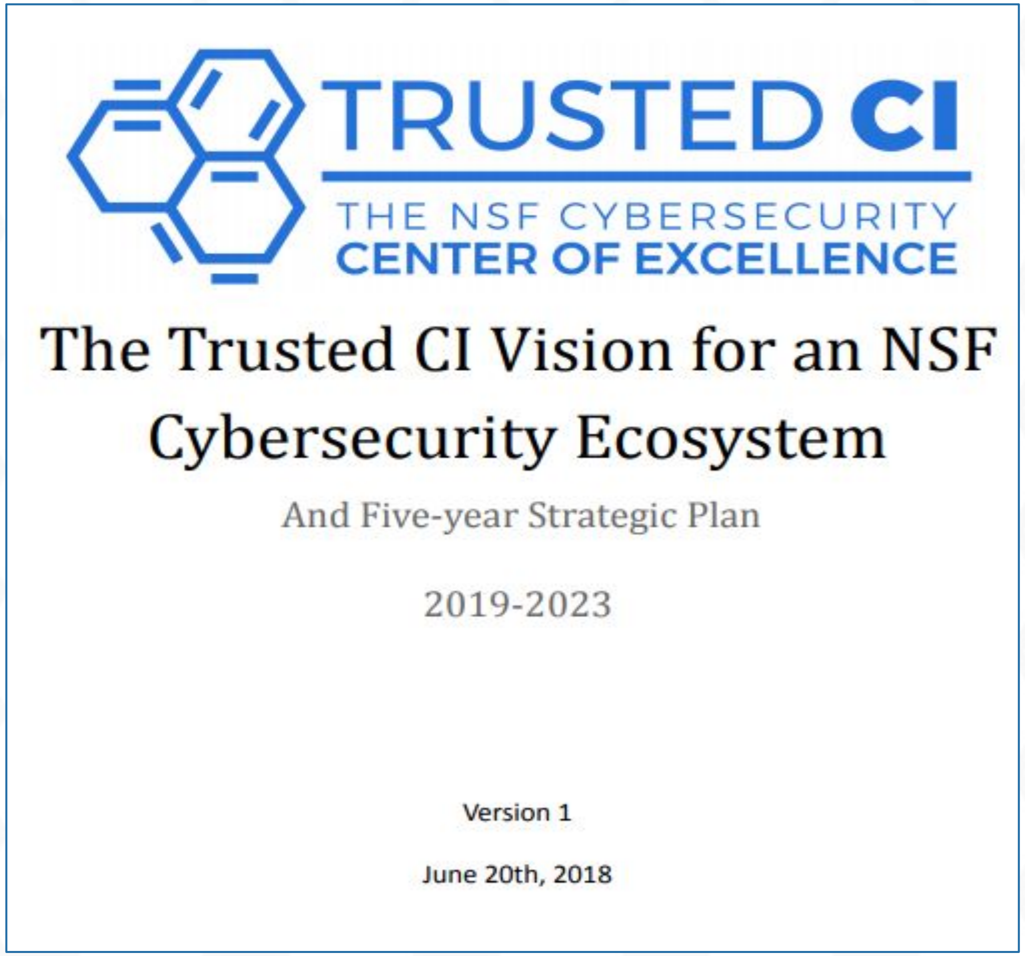
Sep 22-24, 2020 in Bloomington IN

https://trustedci.org/summit/

Agenda driven by call for participation which will be publish in Summer of 2020.

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

Annual Challenge 2020: Data Integrity

Annual Challenge: a cybersecurity challenge to reproducible, trustworthy science that is unlikely to be addressed without our leadership.

“...data integrity is a particular challenge for trustworthy, reproducible science...large data sizes are surpassing protections in our current IT infrastructure. Data integrity is also not well addressed in many cybersecurity control sets (e.g., NIST 800-171 is focused on confidentiality)...there is no community consensus on the risks to scientific results, or guidance to projects for protecting integrity.”

--Federal Cybersecurity R&D Strategic Plan

Meeting the Challenge: The Process

- Survey key science projects
- Understand the spectrum of concerns
- Understand current practices
- Analyze the results
- Produce broadly-applicable guidance for projects, CI developers

https://trustedci.org/2020-trustworthy-data

Participating Data Hubs/Organizations

- Midwest Big Data Hub
- Northeast Big Data Hub
- South Big Data Hub
- West Big Data Hub
- Indiana Geological and Water Survey
- Ostrom Data Initiative

Quilt and Regional Network Collaboration

- Is consortium of regional networks from across the US
- Members are higher ed institutions of all sizes.
- Train the Trainers session & materials to be presented at annual meeting.

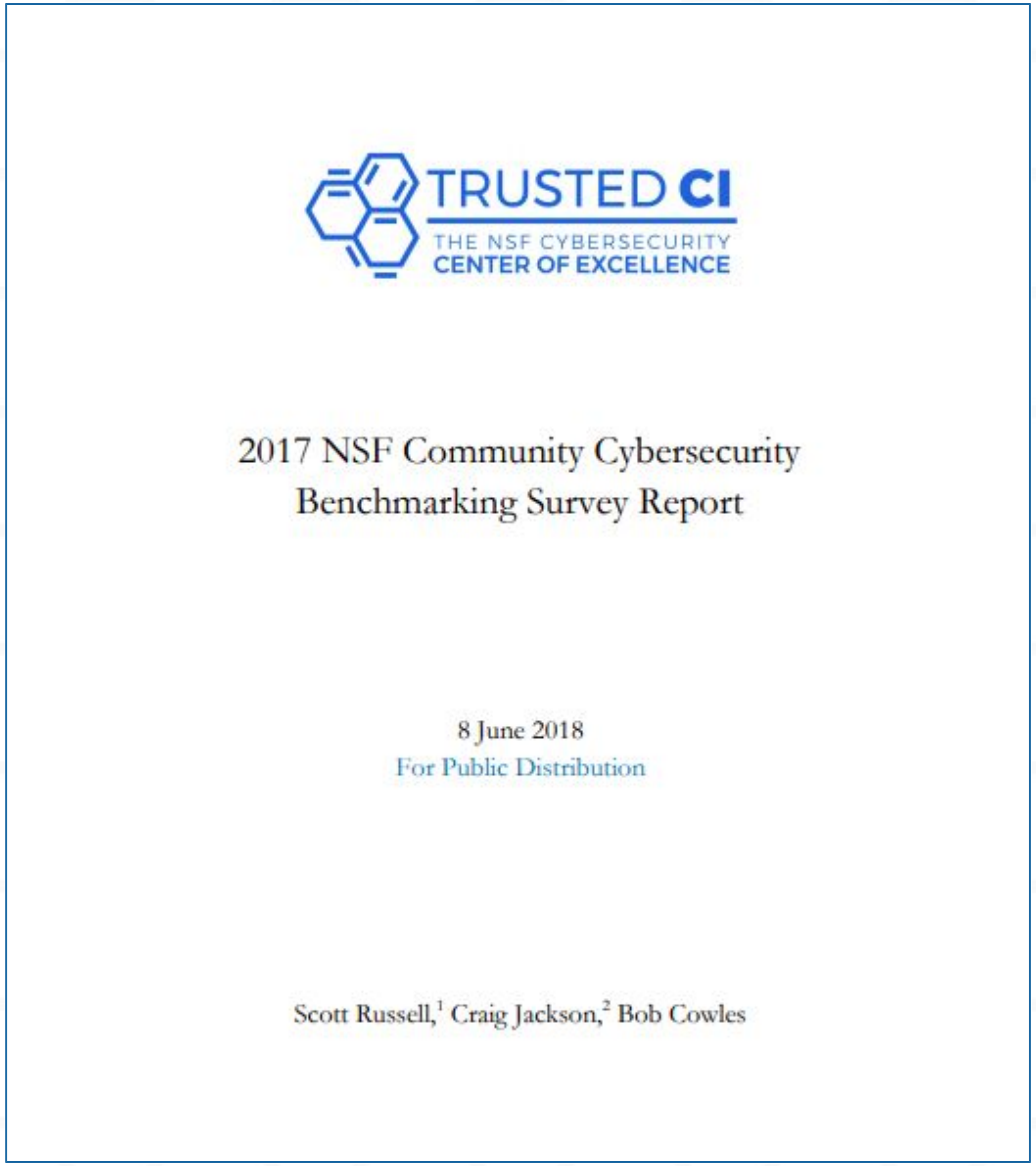
Topic for 2020:

Research facilitation for information security professionals.

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

2019 Trusted CI Cybersecurity Fellows

Fellows are liaisons between Trusted CI and their communities.

Fellows receive training, travel support, and prioritized support.

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

https://trustedci.org/fellows

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Cybersecurity Transition to Practice (TTP)

Enabling researcher and practitioner collaboration to accelerate cybersecurity research to practice in industry, academia, government, or open source via

- matchmaking
- business model coaching
- workshops

https://trustedci.org/ttp

from the ground floor as part of your overall strategy. Why this focus on diversity, and how do you envision that your company could work with cybersecurity researchers and their CIO's as you develop and enhance the capabilities of Armored Things.

- Question for Ed Aractingi: Ed, you've come a fair distance to be with us today. Could you tell us about your engagement with Internet2 related to Internet of Things, and also how you envision working with faculty and companies to create opportunities for cybersecurity research to accelerate?

Cybersecurity Research Acceleration Workshop and Showcase, Indianapolis, IN
October 11, 2017

Goals:

1. NSF cybersecurity research deployed in at least one NSF Large or Medium Facility
2. NSF cybersecurity research transitioned to at least one commercial entity, government facility (agency or lab), or academia
3. Increased participation of under-represented minorities in cybersecurity TTP

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

The Trusted CI Framework

https://trustedci.org/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.

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.

Planned 2019 extensions: Data integrity, Network-connected sensors and actuators ("cyber-physical systems"), and Mitigations

https://trustedci.org/oscrp/

Trusted CI and Inclusivity

Cybersecurity requires diverse perspectives and cybersecurity community suffers from a lack of diversity.

Trusted CI works to address it through its workforce development, outreach, and community building efforts by explicitly seeking out and encouraging underrepresented groups to apply and striving for inclusive demographics.

2018 NSF Cybersecurity Summit Student Program

Trusted CI Partners

https://trustedci.org/partners

THE QUILT

NORTHEAST BIG DATA INNOVATION HUB

SGCI Science Gateways Community Institute

InCommon®

Open Science Grid

Engagement and Performance Operations Center (EPOC)

EDUCAUSE HEISC

MIDWEST BIG DATA HUB

women in cybersecurity WiCyS

Software Sustainability Institute

XSEDE

REN-ISAC

ResearchSOC

CI CoE PILOT

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 10am ET.

https://trustedci.org/webinars

Follow Us

https://trustedci.org

https://blog.trustedci.org

@TrustedCI

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/

TRUSTED CI

THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Trusted CI PEARC19 Experiences Paper

Trusted CI Experiences in Cybersecurity and Service to Open Science. In PEARC'19: Practice and Experience in Advanced Research Computing, July 28-August 1, 2019, Chicago, IL, USA. ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3332186.3340601

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Acknowledgments

Trusted CI is supported by the National Science Foundation under Grants 1547272, 1920430, 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/

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

ResearchSOC

Research Security Operations Center

The second NSF-funded cybersecurity center serving the NSF science community.

ResearchSOC complements Trusted CI

ResearchSOC

- Operational services and related training for NSF CI
- Community of Practice and Threat Intelligence Network
- Enabling Cybersecurity Research
- Outreach to Higher Ed Infosec regarding research CI

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

- Creating comprehensive cybersecurity programs
- Community building and leadership
- Training and best practices
- Tackling specific challenges of cybersecurity, software assurance, privacy, etc.

ResearchSOC

PITTSBURGH SUPERCOMPUTING CENTER

UC San Diego

Operational cybersecurity services for research.

Building on existing services (OmniSOC, STINGAR) and expertise to bolster the NSF cybersecurity community’s incident response capabilities.

Ramping up in 2019, initial clients in 2020, sustaining in 2021.

https://researchsoc.iu.edu/

NSF award 1840034

Trusted CI License Statement

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Thanks!

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Trusted CI is supported by the National Science Foundation under Grants 1547272, 1920430, and 1920430. The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.