



TRUSTED CI

THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

| trustedci.org

Cybersecurity to Enable Science: Hindsight and Vision from the NSF Cybersecurity Center of Excellence

Von Welch

Director, Trusted CI
PI, ResearchSOC
Director, IU CACR

NSF OAC Webinar

September 20th, 2018

My Talk

1. Why Cybersecurity for Open Science? What is unusual about cybersecurity for Open Science?
2. The NSF Cybersecurity Center of Excellence: What can it do for you?
3. Coming Attractions: New Cybersecurity Activities



Regulated vs Open Science



Research with regulated data is guided by compliance

E.g. HIPAA, FISMA, NIST 800-171

Open science is not guided by compliance

E.g. Astronomy, climate, physics, geology

A sizeable fraction or even majority of science at a University is open

If no medical school, probably majority.

This talk focuses on open science

Myth: **“Open Science Does Not Need Cybersecurity”**

“I don’t handle confidential data, hence I don’t need cybersecurity!”

Not true, you do need cybersecurity.

Trusted and Reproducible Results

Integrity First

For Open Science, integrity of data is often most important aspect of cybersecurity.

Confidentiality is important for financial data, regulated data, intellectual property, etc.



Your Data Is Valuable to Criminals!



https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Reproducibility

If your cyberinfrastructure isn't secure from uncontrolled changes, reproducibility is at risk.

Need to manage tension between the need to patch vulnerabilities and the desire for stability to support reproducibility.

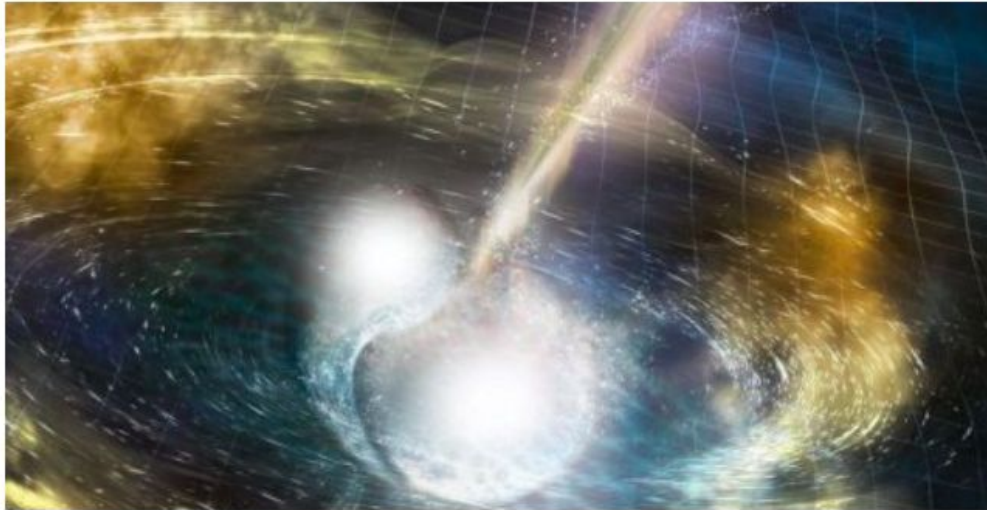
Science Productivity

Threat of Unavailable Instruments

Cyber attack threatened WA astrophysicists' shot at gravitational waves, colliding neutron stars

NICOLAS PERPITCH

UPDATED TUE 17 OCT 2017, 6:44 PM AEDT



▶ 0:00



VIDEO [0:30] In a galaxy 130 million lights years away two neutron stars collide

ABC NEWS

Astrophysicists at WA's Zadko telescope had just learned about the detection of a monumental deep space event involving two neutron stars colliding — which they had been hoping to find for years — when they came under sustained cyber attack.

At the critical and fleeting moment, they could not move their telescope to track the gigantic explosion 130 million light years away.

<http://mobile.abc.net.au/news/2017-10-17/cyber-attack-almost-costs-tea-m-look-at-colliding-neutron-stars/9055816?pfmredir=sm>

Rapid, Collaborative Projects

Research projects tend to be short-lived (3-5 years). They need to progress quickly.

It's common for research collaborations to span universities and even countries.

Researchers want to define their teams, change those definitions and share access – all unrelated to institutional directories or human resources databases.

Cyberinfrastructure != Enterprise IT

Secure Shell access to shared computers.

Uploading virtual machines, code, etc.

Science Gateways, Science DMZs

Distributed, high performance files systems, networks, etc.

Reputational Harm Will Erode Our Autonomy

CYBERSECURITY

U.S. blames 'massive' hack of research data on Iran

Targets included nearly 8000 professors in 22 countries

By Jon Cohen

A "massive and brazen cyberassault" revealed last week by the U.S. Department of Justice (DOJ) showed that academics are easy targets for hacking. In "one of the largest state-sponsored hacking campaigns" it has ever prosecuted, DOJ alleges that nine Iranians working on behalf of the Islamic Revolutionary Guard Corps stole data from 7998 professors at 320 universities around the world over the past 5 years.

The indictment, filed by a federal grand jury in New York City and unsealed on 23 March, alleges that the hackers pilfered 31.5 terabytes of documents and data, including scientific research, journals, and dissertations. Their targets also included the United Nations, 30 U.S. companies, and five U.S. government agencies. The indictment does not name the hacked academic institutions or companies, but it notes that the victims included academic publishers, a biotechnology company, and 11 technology companies.

"This is not an isolated breach—it's hundreds if not thousands of breaches," says Anthony Ferrante, who heads cybersecurity at FTI Consulting in Washington, D.C., and formerly worked as a cyber expert for the

variations behind the indictment and suggest the actual harm was modest.

According to the indictment, the attack targeted 3768 professors at 144 U.S. universities and stole data that cost the institutions about \$3.4 billion to "procure and access." The accused allegedly set up an institute in Iran called Mabna that coordinated and paid for the hacks. The institute, the indictment says, aimed to "assist Iranian universities, as well as scientific and research organizations, to obtain access to non-Iranian scientific resources." The stolen data were sold through two websites, Gigapaper and Megapaper.

The indictment says the university breaches involved "spearfishing," in which the accused sent emails that tricked targets

into providing their login credentials. The emails supposedly came from professors who had read articles by the targets and asked for access to more of their work, helpfully providing links. Clicking a link took the victim to a fake

internet domain that resembled their own university's website and asked them to log in.

With the harvested credentials, documents and other resources were easy pickings. "College professors are like shooting fish in a barrel," says Max Kilger, a social psychologist at University of Texas in San

"College professors are like shooting fish in a barrel."

Max Kilger, University of Texas

Downloaded from <http://science.sciencemag.org/> on September 17, 2018

U.S. HOUSE OF REPRESENTATIVES COMMITTEE REPOSITORY

Calendar

Committees

Document Search

Hearing: Scholars or Spies: Foreign Plots Targeting America's Research and Development

Subcommittee on Oversight (Committee on Science, Space, and Technology)

Wednesday, April 11, 2018 (10:00 AM)

2318 RHOB
Washington, D.C.

<https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108175>

<http://science.sciencemag.org/content/sci/359/6383/1450.full.pdf>

Confidential Data Even In Open Science

Pre-announcement/pre-publication

Gravitational-Wave Announcement Coming on Oct. 16: What Could It Be?

By Calla Cofield, Space.com Senior Writer | October 5, 2017 07:00am ET

f 138

t 67

F

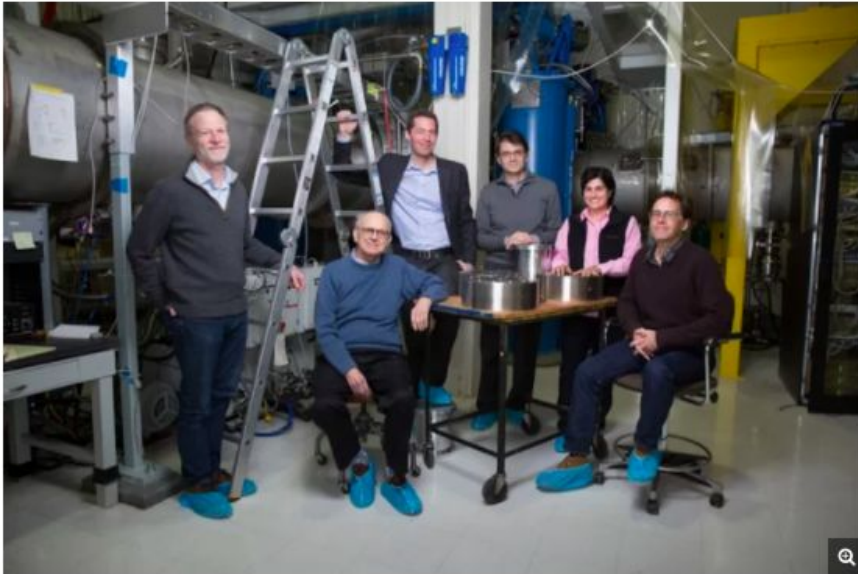
reddit

stumbleupon

MORE ▼

Get all the latest amazing astronomy pictures! Subscribe to Space.com.

Subscribe >



Members of the MIT LIGO team (from left to right): David Shoemaker, Rainer Weiss, Matthew Evans, Erotokritos Katsavounidis, Nergis Mavalvala and Peter Fritschel. Rainer Weiss stated on Oct. 3, 2017 that the LIGO collaboration will make an exciting announcement on Oct. 16.

Credit: Bryce Vickmark/MIT



<https://www.space.com/38367-gravitational-wave-announcement-coming.html>

Ethical Concerns

E.g. Endangered Species

Wildbook: Software to Combat Extinction Home Support Options Login / Register Search

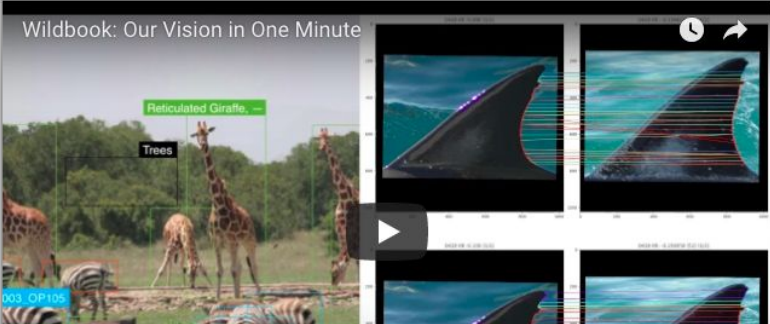
Wildbook in 60 Seconds
News
Follow Us for Updates
Why Wildbook?
Projects with Wildbook
Get Wildbook
R Package
Get Support
People
Sponsors
Screenshots
Donation
Publications
Legal



Wildbook in 60 Seconds

Wildbook blends structured wildlife research with artificial intelligence, citizen science, and computer vision to speed population analysis and develop new insights to help fight extinction. Here is our vision in one minute.

Wildbook: Our Vision in One Minute



<http://wildbook.org/>

My Talk

1. Why Cybersecurity for Open Science? What is unusual about cybersecurity for Open Science?
2. The NSF Cybersecurity Center of Excellence: What can it do for you?
3. Coming Attractions: New Cybersecurity Activities



Trusted CI: The NSF Cybersecurity Center of Excellence

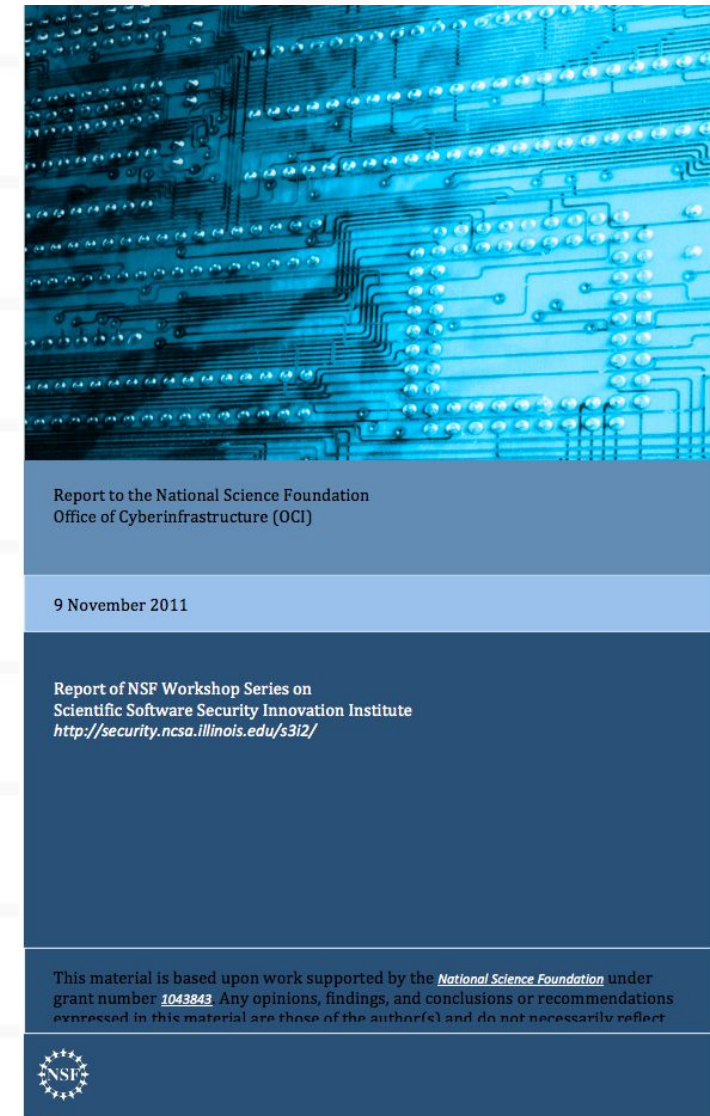
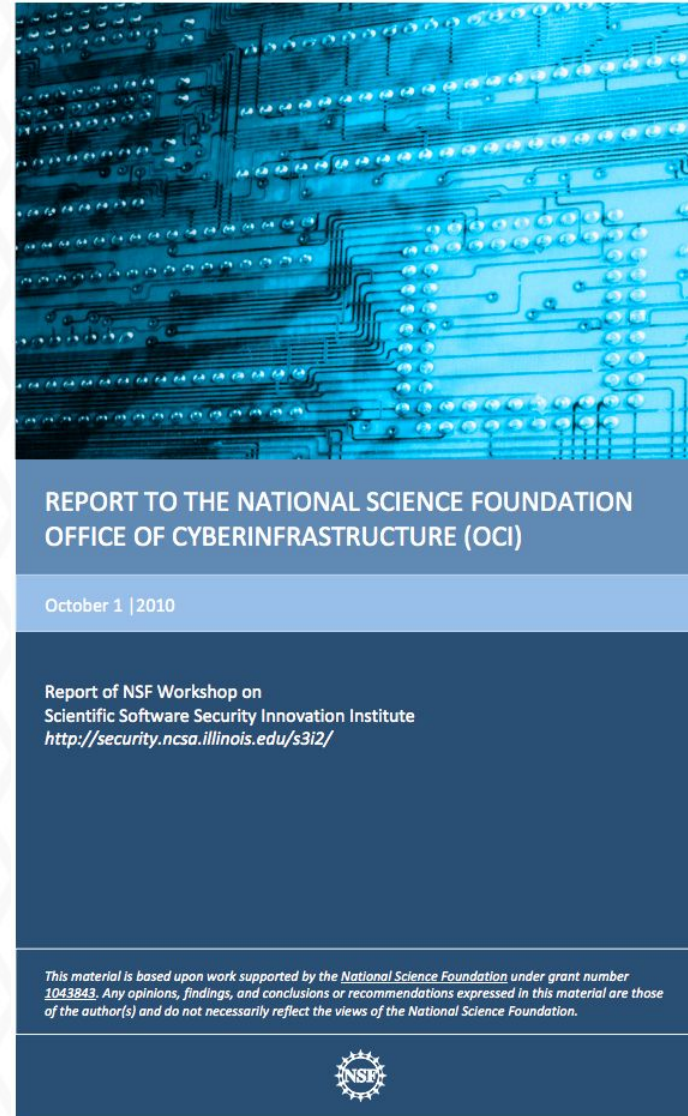
The Mission of Trusted CI is to lead in the maturation of a NSF Cybersecurity Ecosystem with the workforce, knowledge, processes, and cyberinfrastructure that enables trustworthy science and NSF's vision of a nation that is a global leader in research and innovation.



**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



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

Challenges Being Addressed by Trusted CI

We need cybersecurity that meets needs of science community for trustworthy, productive, reproducible science.

We need cybersecurity that is broadly accepted and allows community to avoid other, less appropriate frameworks.

We need cybersecurity that is reasonable to implement given challenges of unusual cyberinfrastructure and project timelines.

Given model of autonomous projects, cybersecurity leadership must be community-driven.

The Trusted CI Broader Impacts Project Report:

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.



The Trusted CI Broader Impacts Project Report

June 28, 2018
For Public Distribution

Jeannette Dopheide¹, John Zage², Jim Basney³

<http://hdl.handle.net/2022/22148>

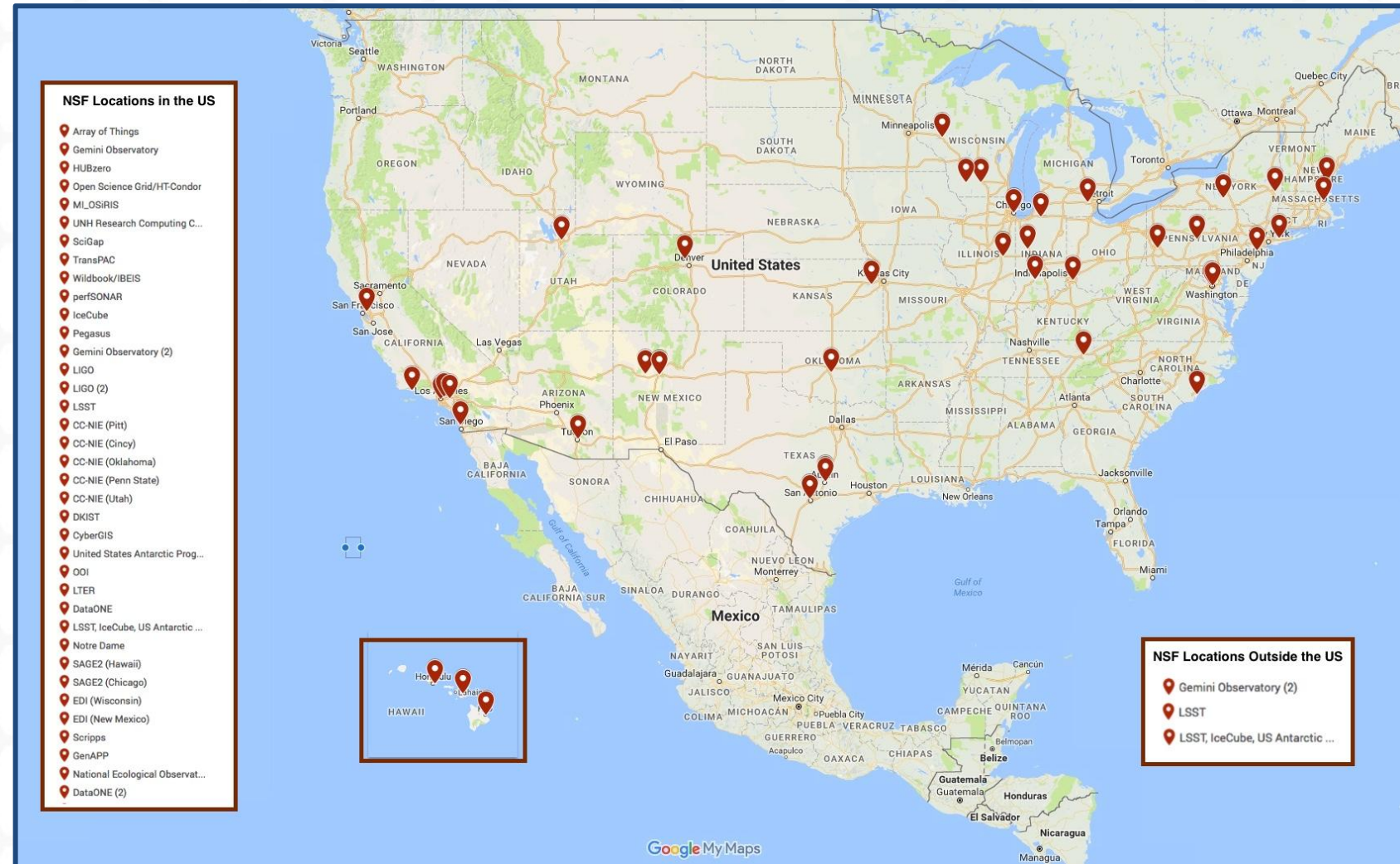
Engagements: One-on-one Collaborations

We take applications every six months.

Currently accepting applications for first half of 2019:

trustedci.org/application/

Deadline: Oct 1



Community-driven Guidance

Security Best Practices for Academic Cloud Service Providers

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

Software Engineering Guide (Coming soon)

Securing Software Supporting Science

Operational Security

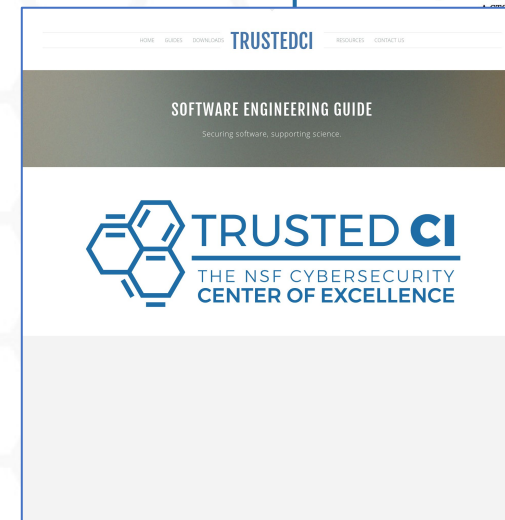
<http://trustedci.org/guide>

Identity Management Best Practices

<http://trustedci.org/iam>

Open Science Cyber Risk Profile

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



Identity Management Best Practices

Coming Series

er 2015
istribution

nsney



Annual NSF Cybersecurity Summit

trustedci.org/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.
Keep informed by joining our email lists.

trustedci.org/trustedci-email-lists/



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.”

Basis for Trusted CI going forward.

We want your feedback!



The Trusted CI Vision for an NSF Cybersecurity Ecosystem

And Five-year Strategic Plan

2019-2023

Version 1

June 20th, 2018

<http://hdl.handle.net/2022/22178>

Other Trusted CI Services

Cyberinfrastructure Vulnerabilities

Latest news on security vulnerabilities tailored for cyberinfrastructure community.

trustedci.org/vulnerabilities/

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

trustedci.org/iam/

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

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

trustedci.org

blog.trustedci.org

[@TrustedCI](https://twitter.com/TrustedCI)



My Talk

1. Why Cybersecurity for Open Science? What is unusual about cybersecurity for Open Science?
2. The NSF Cybersecurity Center of Excellence: What can it do for you?
3. Coming Attractions: New Cybersecurity Activities



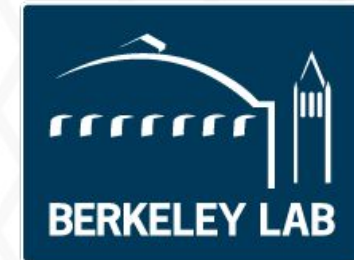
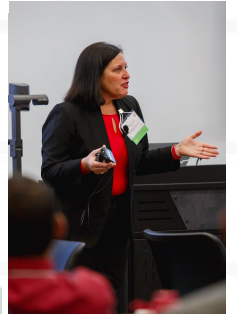
Trusted CI: Extended through 2019 and Expanded

Trusted CI in 2019

New activities:

- Cybersecurity Fellows Program
- Cybersecurity Transition to Practice
- Open Science Cybersecurity Framework

Leadership team expanded: Jim Basney (NCSA), Dana Brunson (Oklahoma State), Florence Hudson (Independent), Craig Jackson (IU), Jim Marsteller (PSC), Bart Miller (U. Wisconsin), Sean Peisert (LBNL), Von Welch (IU)



Cybersecurity Transition to Practice (TTP)

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

© 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

Trusted CI Cybersecurity TTP Strategy

Trusted CI will identify needs of the cyberinfrastructure community that could be met by research and work to foster that transition.

If you have unmet needs or research to transition, contact:
TTP@trustedci.org

A Network of Cybersecurity Fellows

Goal is to broaden Trusted CI's impact:

- Across NSF science directorates.
- Across the NSF 10 Big Ideas
 - https://www.nsf.gov/news/special_reports/big_ideas/
- Across underrepresented groups

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 60 days on their research and software sustainability activities.



Campus Champions



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

Campus Champions Celebrate Ten Year Anniversary

Open Science Cybersecurity Framework

We need cybersecurity that meets needs of science community for trustworthy, productive, reproducible science, plus is reasonable to implement and broadly accepted to avoid less appropriate frameworks.

Trusted CI will lead development, building off of current guidance for developing cybersecurity programs and community input.



CTSC

CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

Guide to Developing Cybersecurity Programs for
NSF Science and Engineering Projects

Version 1
August 2014

trustedci.org/guide
please direct comments and feedback to info@trustedci.org



ResearchSoc

Research Security Operations Center

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



ResearchSOC

ResearchSOC will build on existing services (OmniSOC, STINGAR) and expertise to bolster the NSF Cybersecurity Ecosystem by building community incident response capabilities.



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



In Summary

Cybersecurity is critical to efficient, trustworthy, reproducible science.

Trusted CI is here to help.

Look for Fellows Program, Cybersecurity Research Transition to Practice, Open Science Cybersecurity Framework, and ResearchSOC coming.

Acknowledgments

Trusted CI, the NSF Cybersecurity Center of Excellence, is supported by the National Science Foundation under Grant 1547272.

The ResearchSOC is supported by the National Science Foundation under Grant 1840034.

The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.

Contact Trusted CI

Contact us to request help,
from small questions to
month-long engagements:

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

vwelch@iu.edu

See also:

<https://trustedci.org/situational-awareness/>

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

<https://trustedci.org/ctsc-email-lists/>

<http://blog.trustedci.org/>

info@trustedci.org

[@TrustedCI](#)

