TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE
trustedci.or

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

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

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

Regulated vs Open Science

Research with regulated data is guided b compliance

E.g. HIPAA, FISMA, NIST 800-17

Open science is not guided by complianc

E.g. Astronomy, climate, physics geology

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

If no medical school, probably majority.

This talk focuses on open science

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

yth:
Open Science Does Not Need Cybersecurity”

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

ot true, you do need cybersecurity.

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Trusted and Reproducible Results

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

ntegrity First

r Open Science, integrity of ta is often most important pect of cybersecurity.

nfidentiality is important for ancial data, regulated data, tellectual property, etc.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://www.cbsnews.com/news/global-warming-climate-change-study-again-questioned-again-defended/

our 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

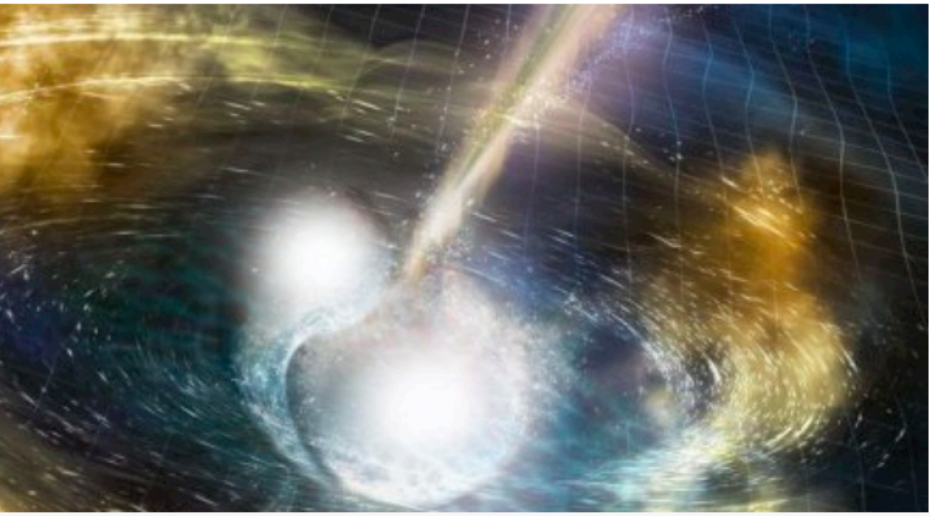
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

hreat of Unavailable Instruments

ber attack threatened WA astrophysicists' shot at avitational waves, colliding neutron stars

LAS PERPITCH

TED TUE 17 OCT 2017, 6:44 PM AEDT



:00

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

IEWS

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

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

http://mobile.abc.net.au/news/2017-10-17/cyber-attack-almost-costs team-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.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

yberinfrastructure != Enterprise IT

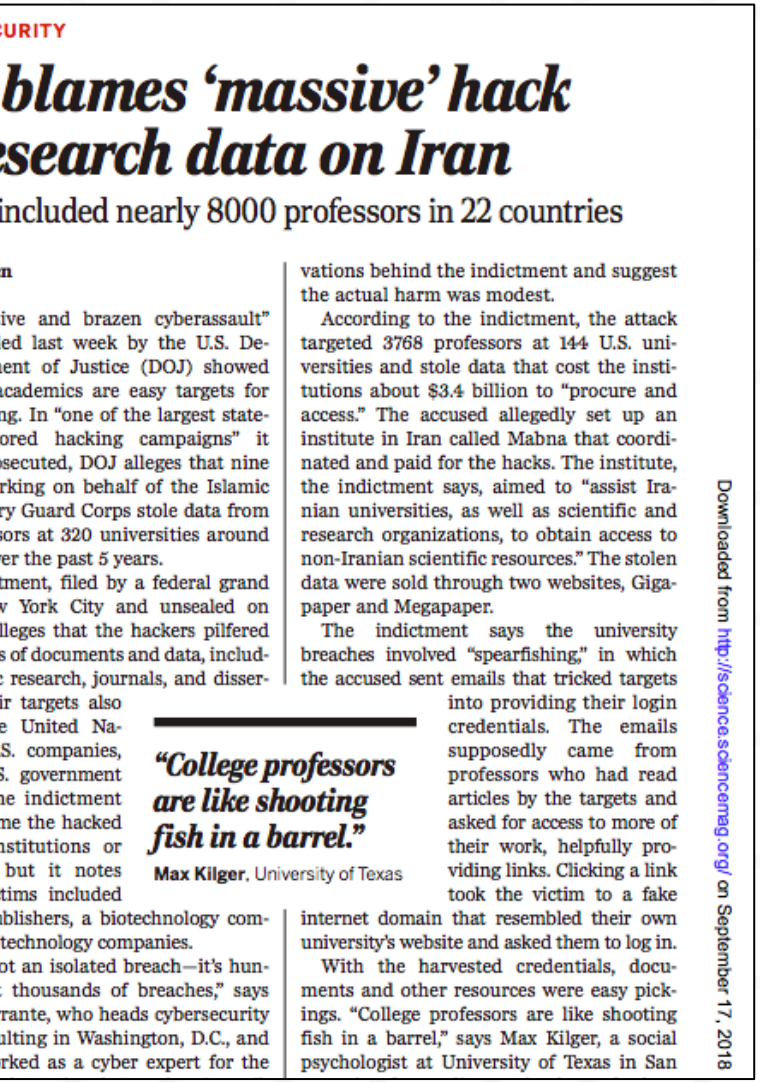
ecure Shell access to shared computers.

loading virtual machines, code, etc.

ience Gateways, Science DMZs

stributed, high performance files systems, networks, etc.

eputational Harm Will Erode Our Autonomy



CURITY

blames 'massive' hack esearch data on Iran

included nearly 8000 professors in 22 countries

n

ive and brazen cyberassault" ed last week by the U.S. De- ent of Justice (DOJ) showed academics are easy targets for ng. In "one of the largest state- ored hacking campaigns" it secuted, DOJ alleges that nine rking on behalf of the Islamic ry Guard Corps stole data from sors at 320 universities around er the past 5 years.

tment, filed by a federal grand w York City and unsealed on lleges that the hackers pilfered s of documents and data, includ- research, journals, and disser- ir targets also e United Na- S. companies, S. government he indictment me the hacked nstitutions or but it notes tims included blishers, a biotechnology com- technology companies.

ot an isolated breach—it's hun- thousands of breaches," says rrante, who heads cybersecurity lting in Washington, D.C., and rked as a cyber expert for the vations 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

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

re-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

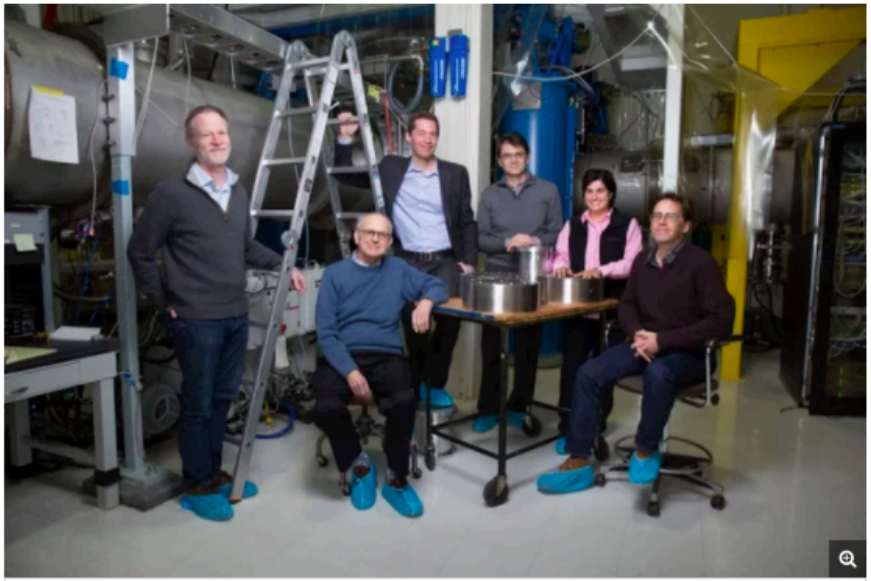
138

67

MORE

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

Subscribe >

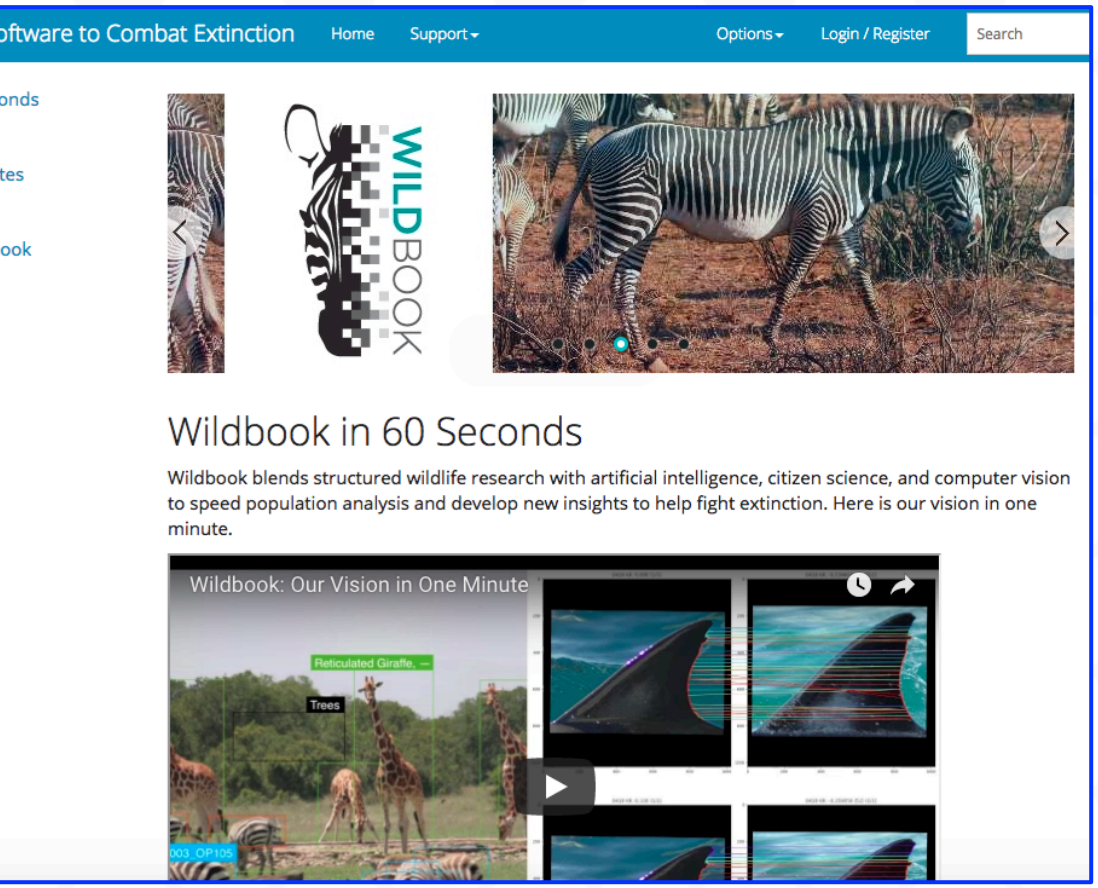


Members of the MIT LIGO team (from left to right): David Shoemaker, Rainer Weiss, Matthew Evans, Erotokritos Katsavounidis, Nergis Mavalvala and Peter Fritschel. Rainer Weiss stated on Oct. 3, 2017 that the LIGO collaboration will make an exciting announcement on Oct. 16.

Credit: Bryce Vickmark/MIT

https://www.space.com/38367-gravitational-wave-announcemen coming.html

thical Concerns
.g. Endangered Species



http://wildbook.org/

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

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

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.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

NCSA

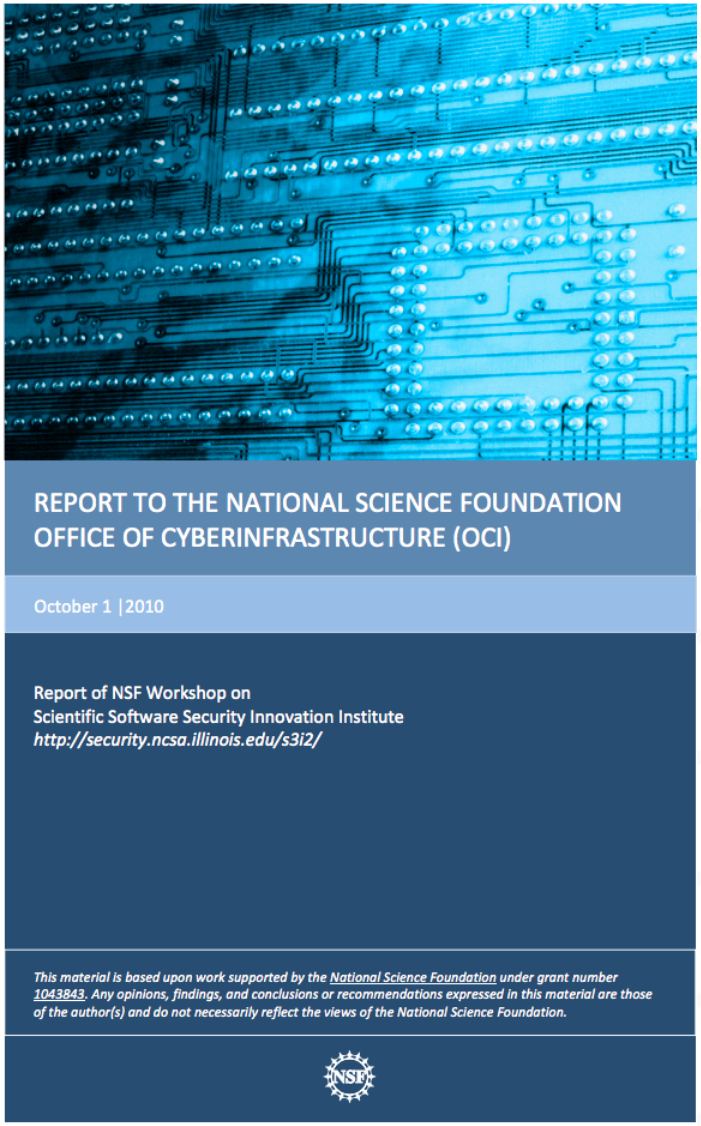
PITTSBURGH SUPERCOMPUTING CENTER

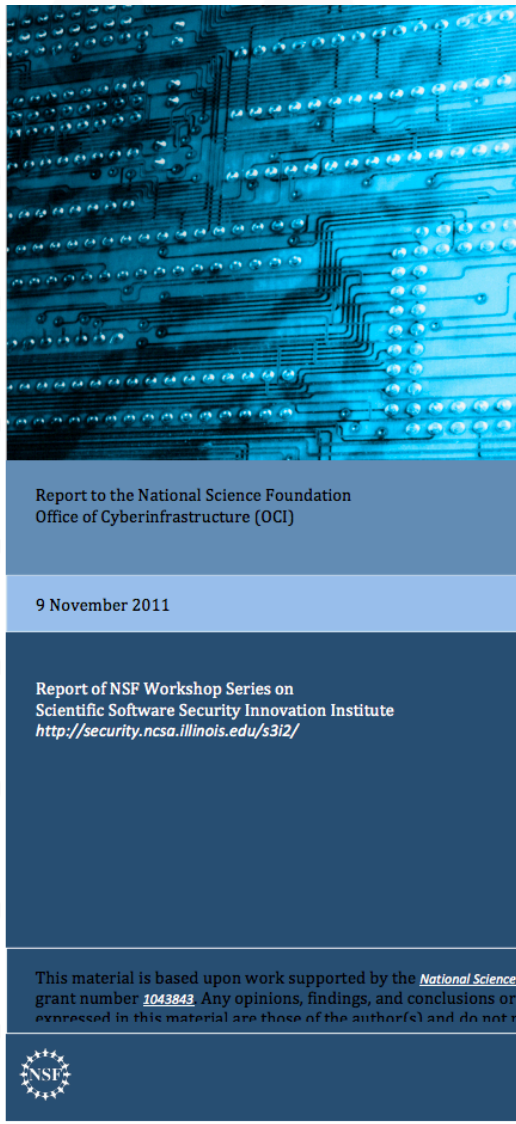
THE UNIVERSITY of WISCONSIN MADISON

don't make the hnology. help you make se of it.

med in 2012

ed on community call eadership and lance rather than nology





TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

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.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

The Trusted CI Broader Impacts Project Report:

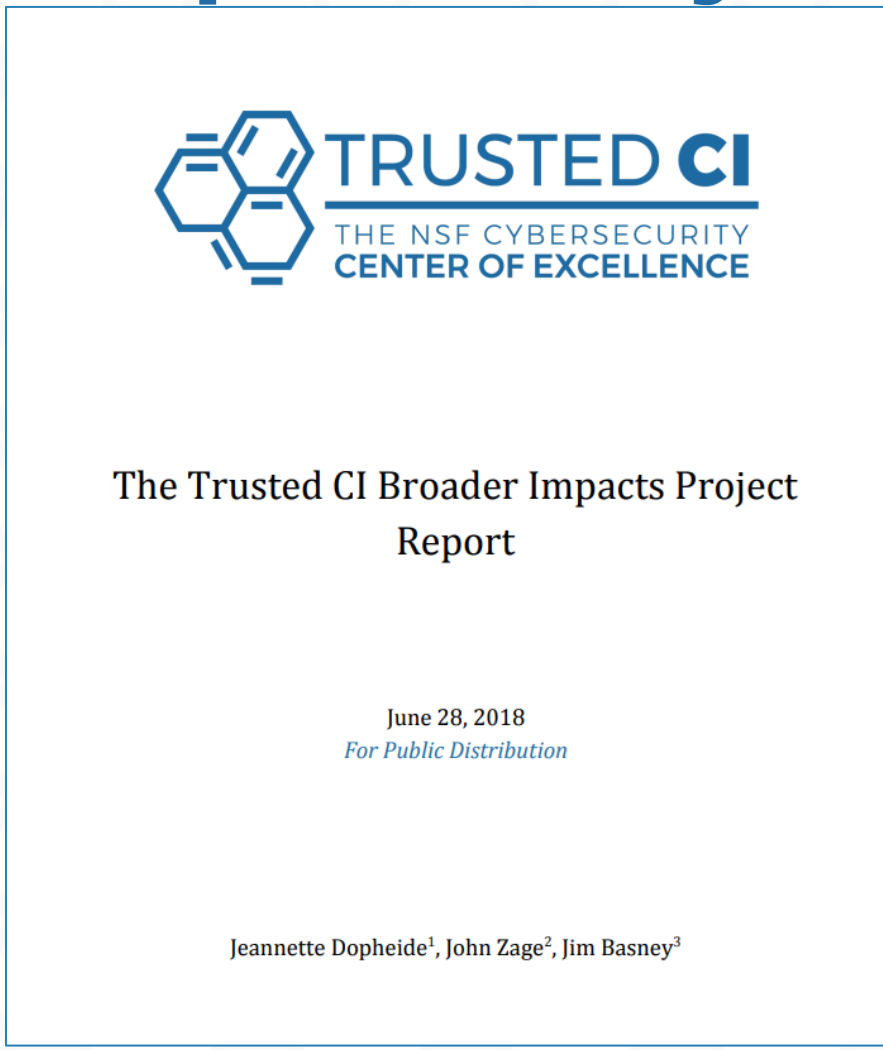
Trusted CI has impacted over 190 NSF projects since inception in 2012.

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.



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

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

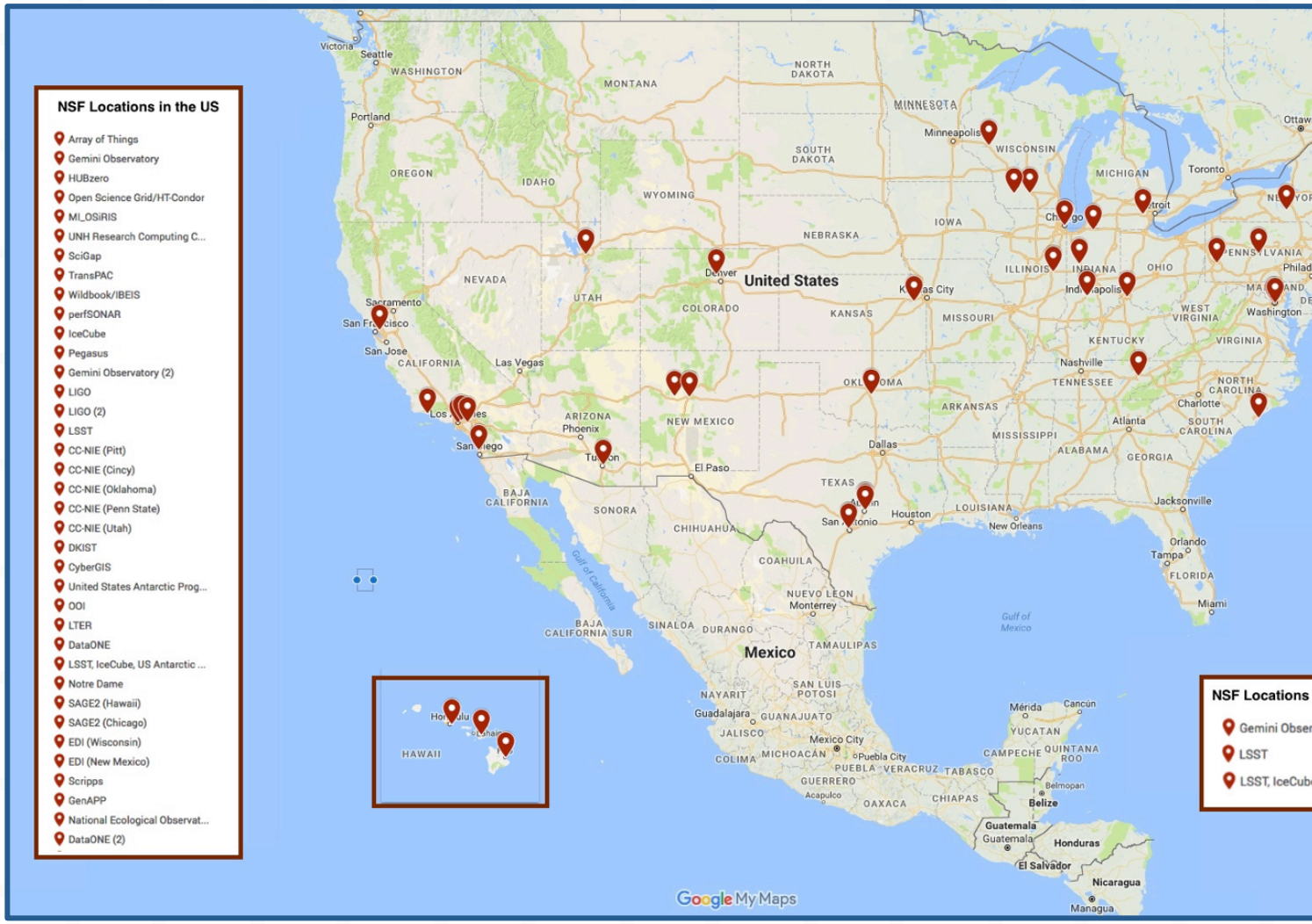
Engagements: One-on-one Collaborations

We take applications every six months.

Currently accepting applications for first half of 2019:

trustedci.org/application/

Deadline: Oct 1



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

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/

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Annual NSF Cybersecurity Summit
rustedci.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
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

usted CI 5-year Vision and Strategic Pla

SF cybersecurity ecosystem, formed of
le, practical knowledge, processes, and
rinfrastructure, that enables the NSF
munity to both manage cybersecurity risks
oroduce trustworthy science in support of
s vision of a nation that is the global leader
search and innovation."

is for Trusted CI going forward.

want your feedback!

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

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

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

Other Trusted CI Services

yberinfrastructure Vulnerabilities

test news on security vulnerabilities tailored
r cyberinfrastructure community.

ustedci.org/vulnerabilities/

pecialized Information for Identity and ccess Management, Science Gateways, oftware Development

stedci.org/iam/

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

stedci.org/software-assurance/

Large Facilities Security Team

Working group of security representatives fro
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

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

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

Trusted CI:
Extended through 2019
and Expanded

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

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)

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

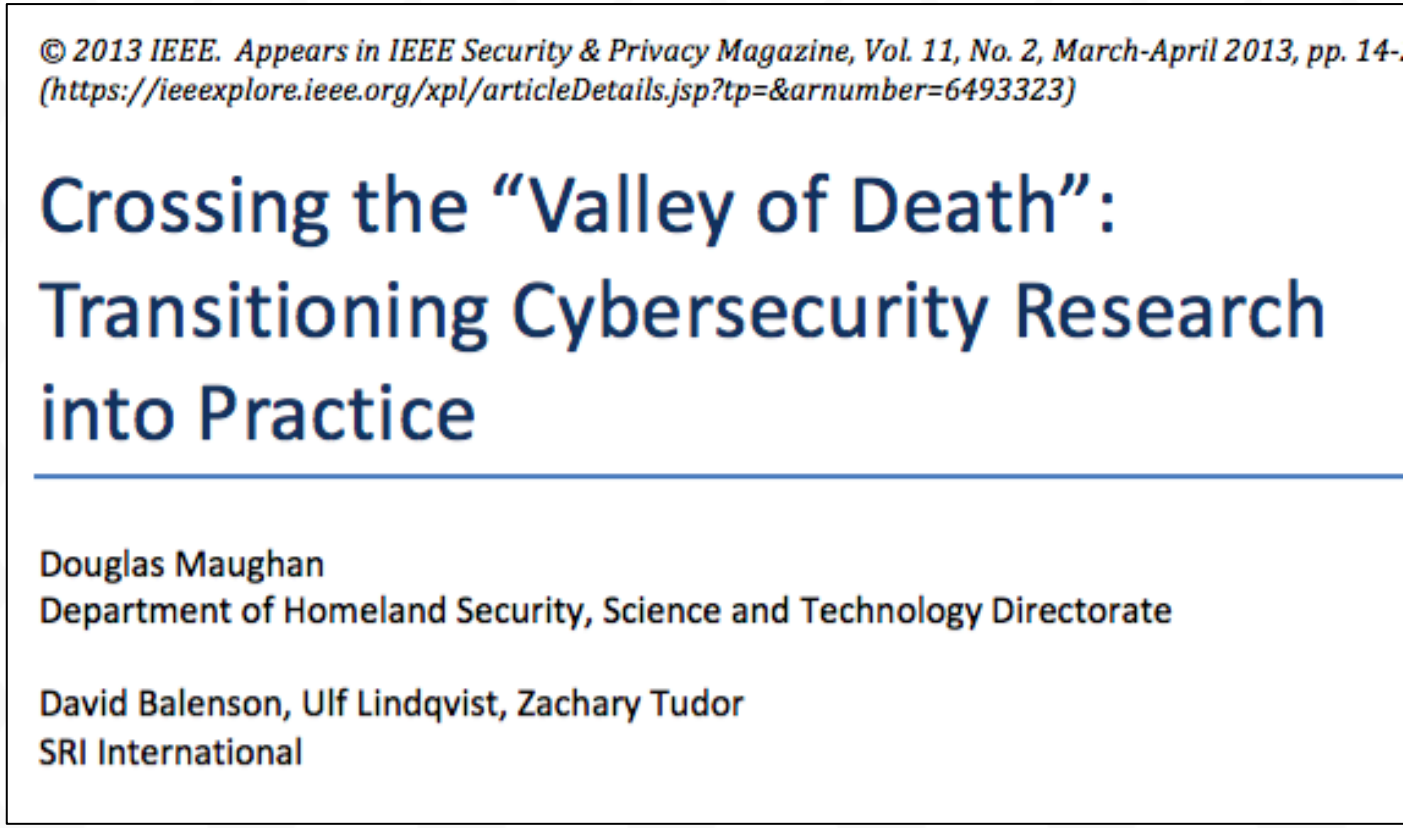
NCSA

PITTSBURGH SUPERCOMPUTING CENTER

THE UNIVERSITY of WISCONSIN MADISON

ybersecurity 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-
(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
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Trusted CI Cybersecurity TTP Strategy

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

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

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

A Network of Cybersecurity Fellows

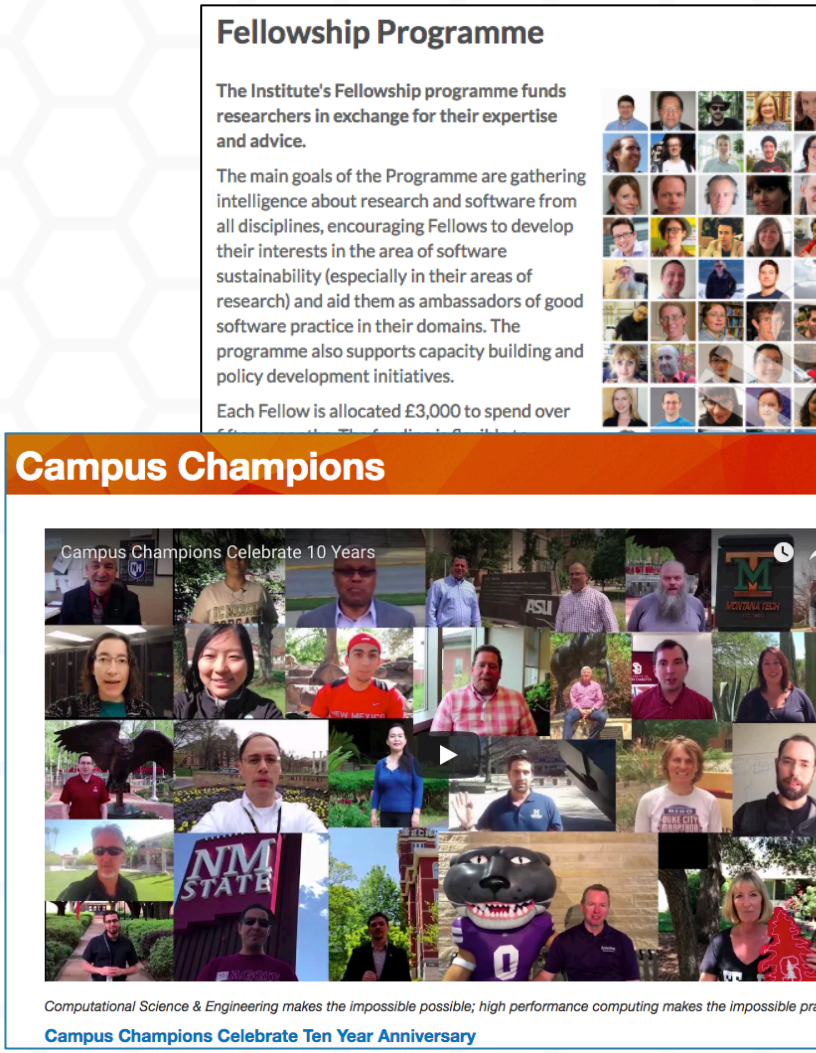
Goal is to broaden Trusted CI's impact:

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

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

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.



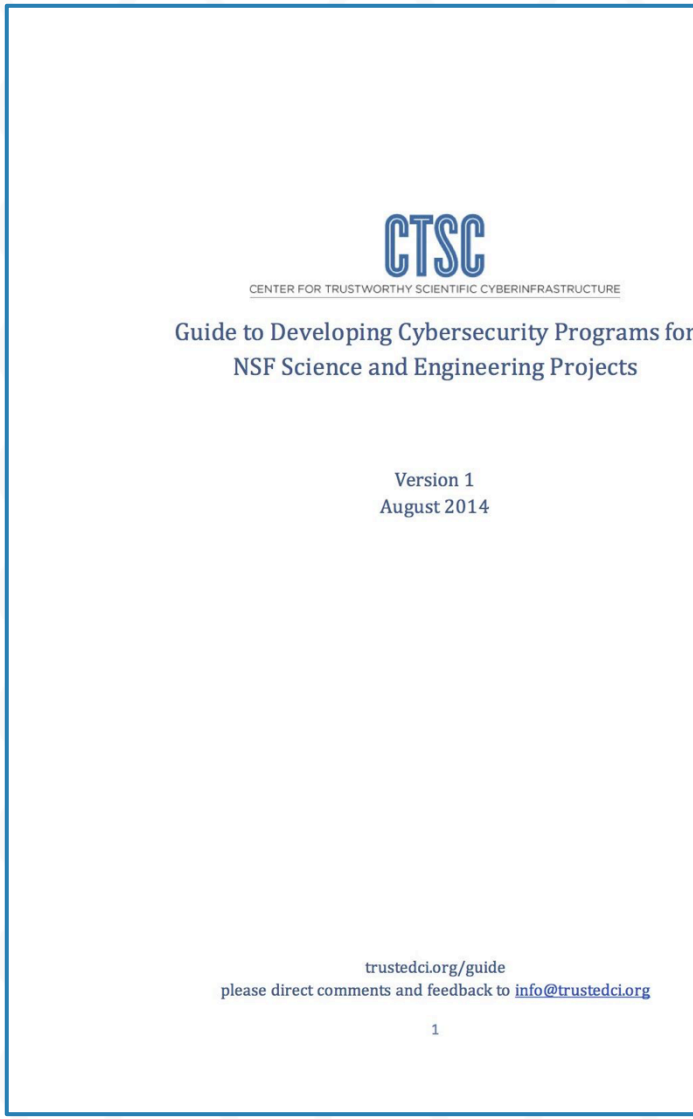
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

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.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE


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

1

ResearchSOC

Research Security Operations Center

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

esearchSOC

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

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

PITTSBURGH
SUPERCOMPUTING
CENTER

UC San Diego

In Summary

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

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.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

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 National Science Foundation or any other organization.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Contact Trusted CI

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

https://trustedci.org/help/

ywelch@iu.edu

See also:

https://trustedci.org/situational-aware

https://trustedci.org/webinars/

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

http://blog.trustedci.org/

info@trusedci.org

@TrustedCI

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

NCSA

PITTSBURGH SUPERCOMPUTING CENTER

THE UNIVERSITY of WISCONSIN MADISON