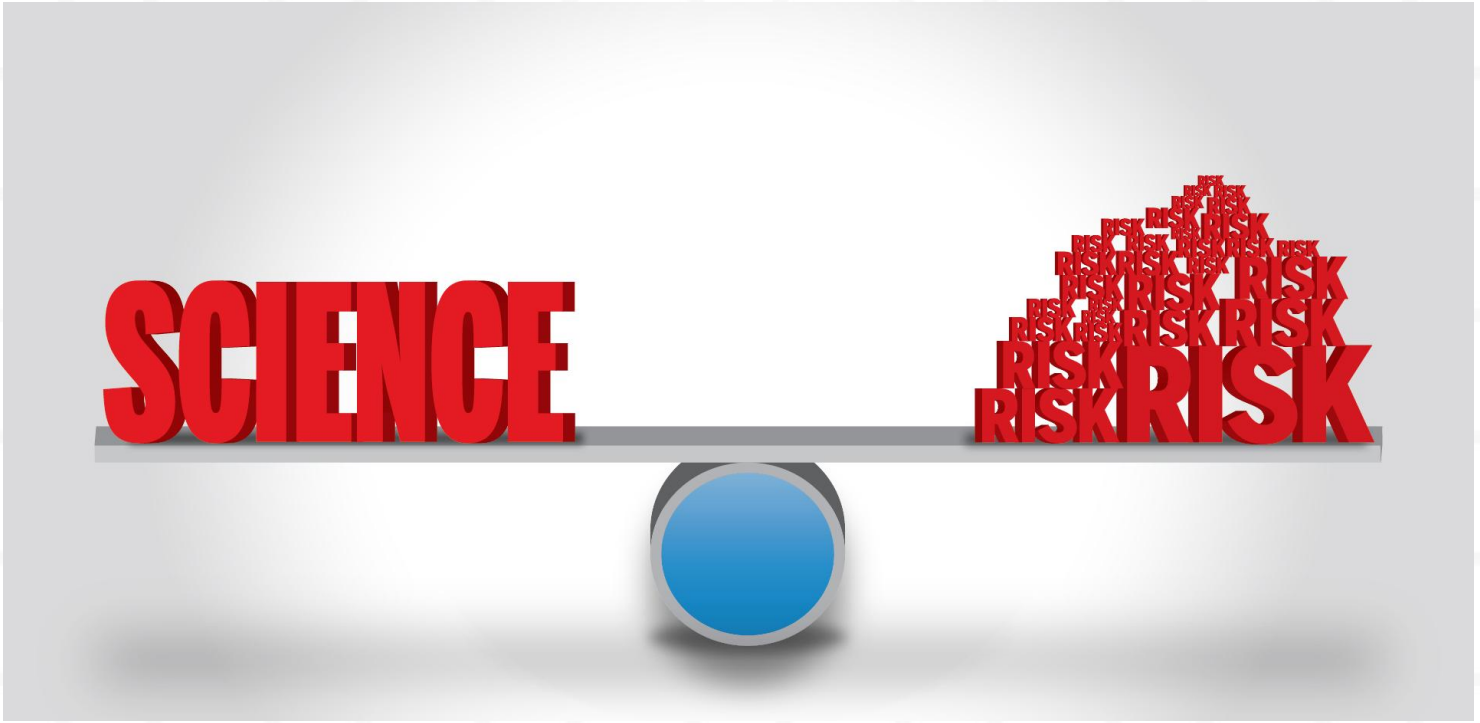

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE
trustedci.org



Perspectives from 10 Years of NSF Science Cybersecurity

DOE ASCR Workshop on Cybersecurity and Privacy for Scientific Computing Ecosystems
November 3-5, 2021

Von Welch
Director, Trusted CI: the NSF Cybersecurity Center of Excellence

Who Am I

AVP for Information Security @ Indiana University, PI and Director for Trusted CI.

Trusted CI is an NSF-funded as Cybersecurity Center of Excellence. Not part of NSF itself and the views I present are not necessarily views of NSF.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

My talk

NSF science ecosystem and cybersecurity.

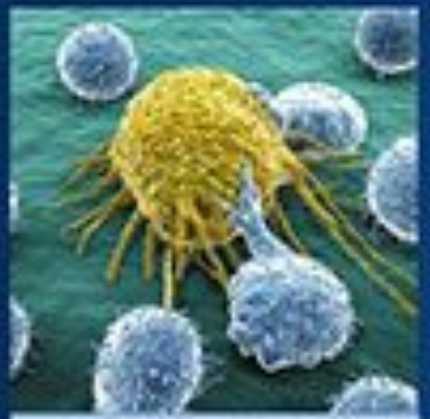
The challenge of cybersecurity for science.

Role of Trusted CI in NSF cybersecurity

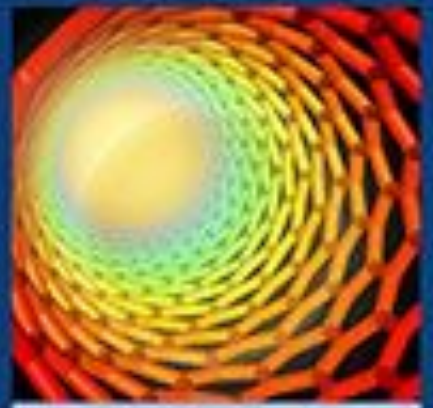
Lessons learned by Trusted CI over past decade

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

NSF Funds Research and Education across all Fields of Science and Engineering



Biological Sciences



Engineering

Mathematical & Physical Sciences

Computer & Information Science & Engineering

Geosciences (including Polar Programs)

Integrative Activities

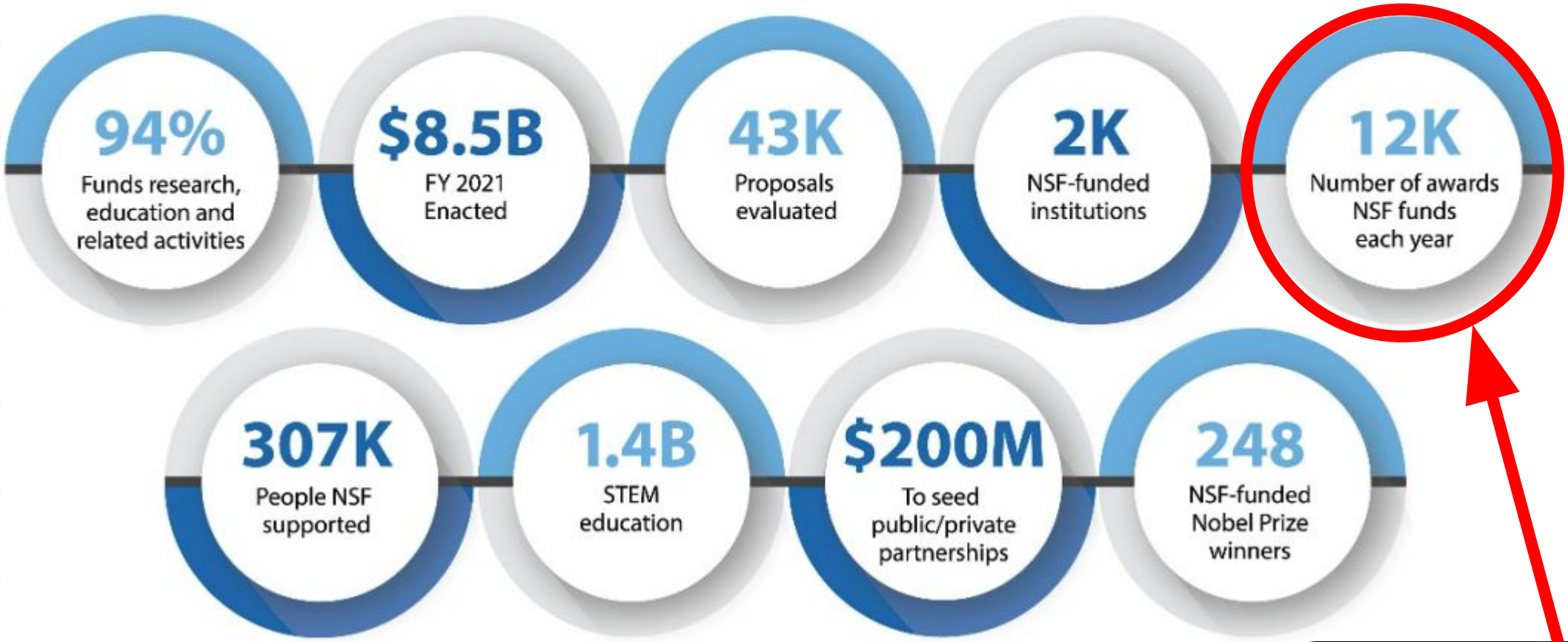
Education & Human Resources

Social, Behavioral & Economic Sciences

International Science & Engineering

https://www.nsf.gov/news/speeches/cordova/17/fc170523_fy18budget.jsp

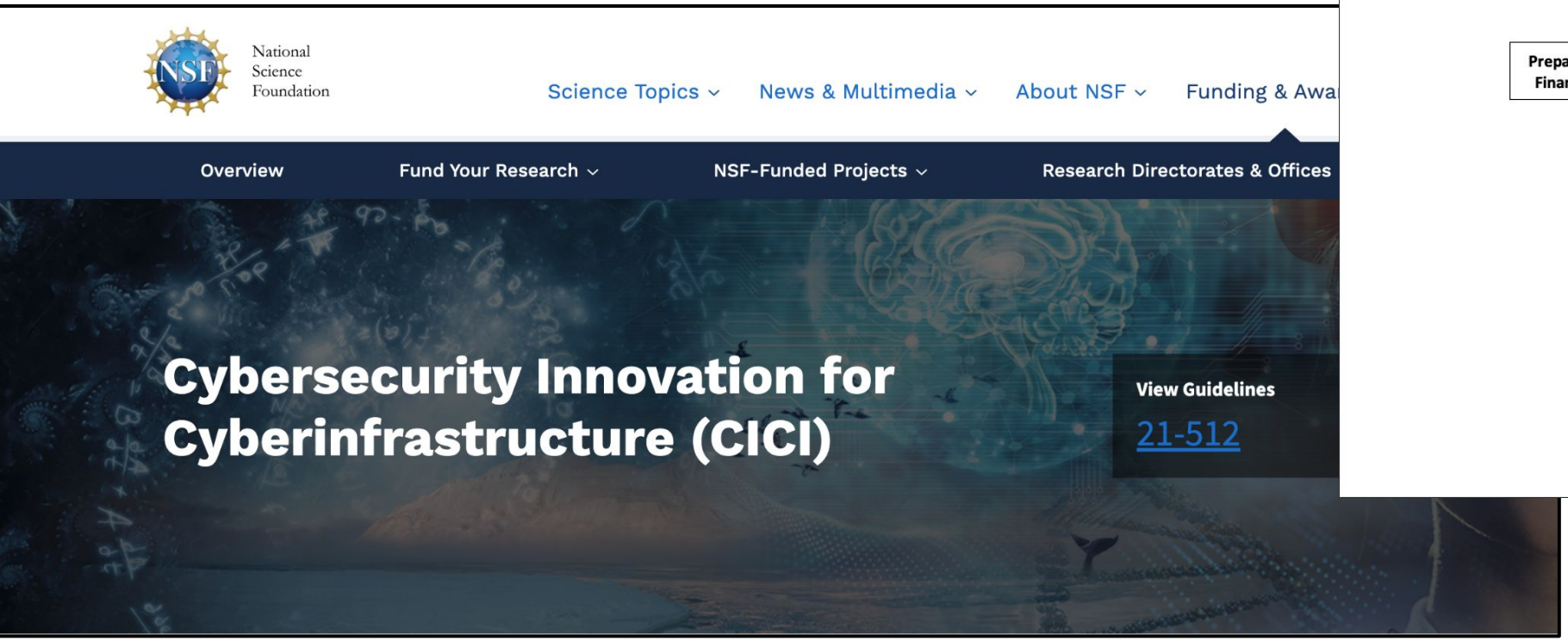
NSF BY THE NUMBERS



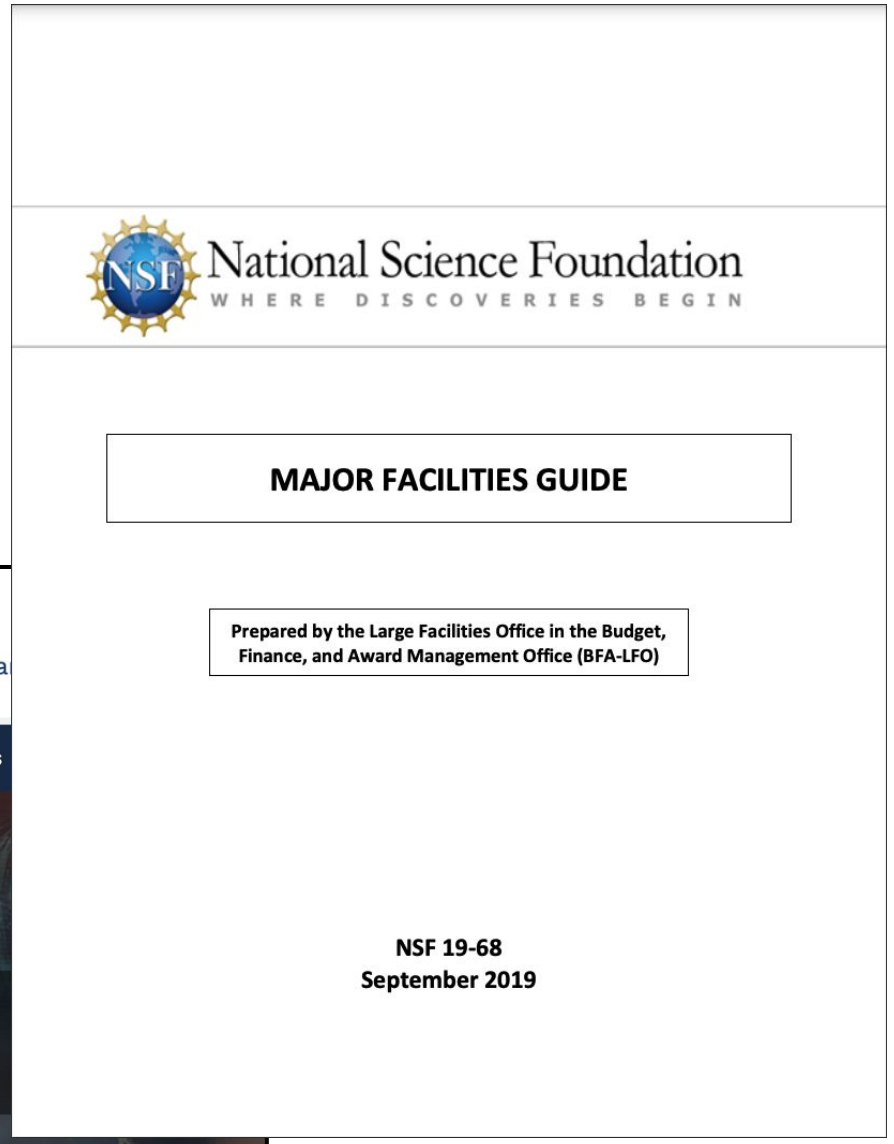
Awards > $1m:
644 in FY20
4283 active in 3/2021

https://nsf.gov/news/factsheets/Factsheet_By%20the%20Numbers_05_21_V02.pdf

NSF Approach to Cybersecurity: Project Autonomy and Incentives



https://beta.nsf.gov/funding/opportunities/cybersecurity-innovation-cyberinfrastructure-cici



https://www.nsf.gov/bfa/lfo/lfo_documents.jsp

The challenge of cybersecurity for science (And why the NSF approach is a good one.)

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Appropriate cybersecurity supports organizational mission.

Organizational mission translates into different priorities for cybersecurity.

Imagine the program for a bank and hospital: confidentiality, availability, Integrity, resilience, etc. all differently prioritized.

Adobe Stock

Cybersecurity and Science

A lot of research is regulated.

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

A lot of science is not guided by compliance

E.g. Astronomy, climate, physics, geology

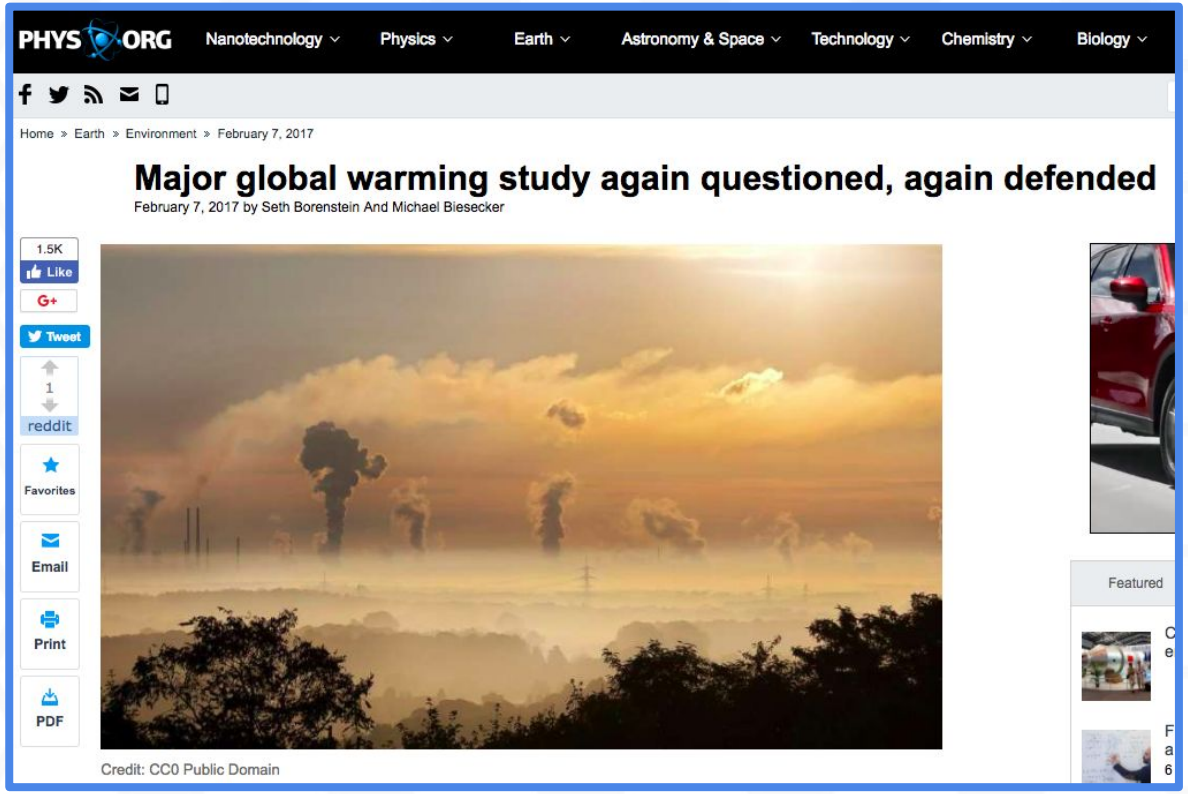
AKA Fundamental Research

Gemini South on the summit of Cerro Pachón in Chile (left) and Gemini North on the summit of Maunakea in Hawai'i (right). Image credit: Gemini/NSF/AURA

Data Integrity

Integrity of data is often most important aspect of cybersecurity for science.

Protect against manipulation and accusations of manipulation.



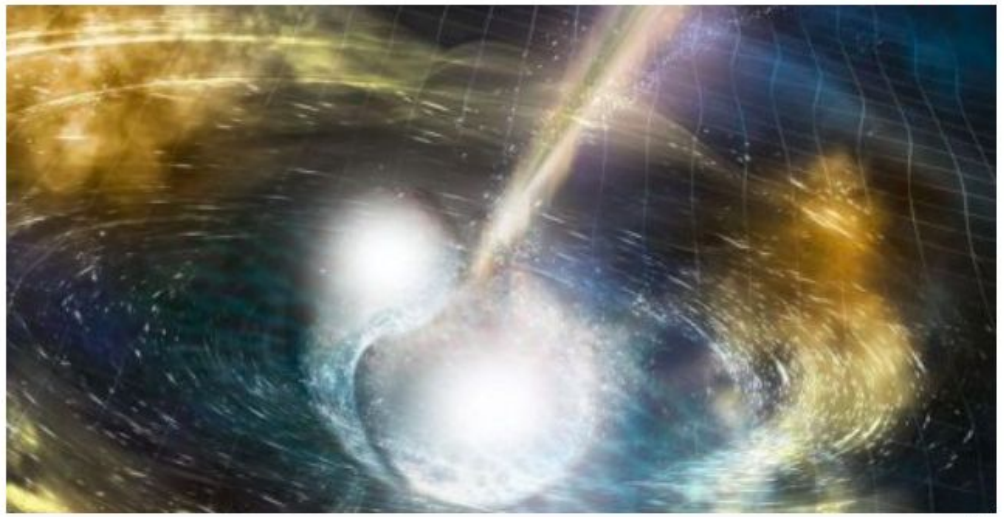
https://www.cbsnews.com/news/global-warming-climate-change-study-again-questioned-again-defended/

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

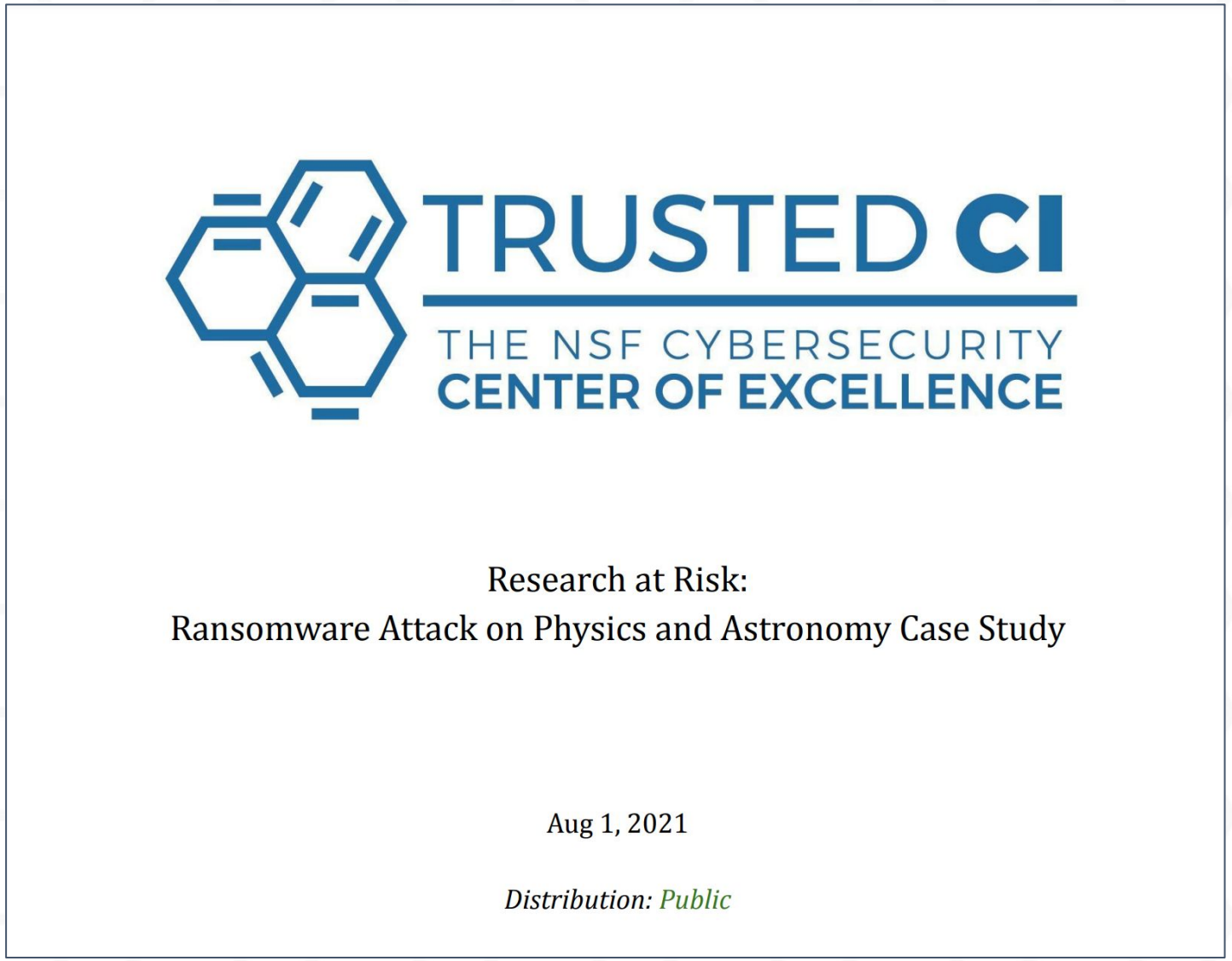
ABC NEWS

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-team-look-at-colliding-neutron-stars/9055816?pfmredir=sm

Any Data Is Valuable to Criminals if it is valuable to you!



Trusted CI and Michigan State University collaboration: "Research at Risk: Ransomware Attack on Physics and Astronomy Case Study" https://hdl.handle.net/2022/26638

Supporting Dynamic, 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.

Some history of scale…

Date	Collaboration sizes	Data volume, archive technology
Late 1950's	2-3	Kilobits, notebooks
1960's	10-15	kB, punchcards
1970's	~35	MB, tape
1980's	~100	GB, tape, disk
1990's	700-800	TB, tape, disk
2010's	~3000	PB, tape, disk

Credit: Ian Bird

Reproducibility

Complicated area of research in itself.

For example: can we reproduce what we did on computers we didn't fully control?

For more info see:

Ewa Deelman, Victoria Stodden, Michela Taufer, and Von Welch. 2019. Initial Thoughts on Cybersecurity And Reproducibility. In Proceedings of the 2nd International Workshop on Practical Reproducible Evaluation of Computer Systems (P-RECS '19). Association for Computing Machinery, New York, NY, USA, 13–15. DOI: https://doi.org/10.1145/3322790.3330593.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

US Researcher Caught Mining for Bitcoins on NSF Iron

By Tiffany Trader

June 9, 2014

The National Science Foundation has banned a researcher for using agency-funded supercomputers to mine bitcoins, a virtual currency that can be converted into traditional currencies through exchange markets. According to a recently surfaced report from the National Science Foundation Office of the Inspector General, the NSF banned the unnamed researcher after receiving reports that NSF systems at two universities had been used for personal gain.

Bitcoin mining refers to how the virtual currency is generated. Miners solve math problems that serve to verify bitcoin transactions. In exchange they are issued a certain number of bitcoins as a reward.

"The researcher misused over $150,000 in NSF-supported computer usage at two universities to generate bitcoins valued between $8,000 and $10,000," according to the March 2014 Semi Annual Report to Congress. "Both universities determined that this was an unauthorized use of their IT systems. The researcher asserted that he was conducting tests on the computers, but neither university had authorized him to conduct such tests — both university reports noted that the researcher accessed the computer systems remotely and may have taken steps to conceal his activities, including accessing one supercomputer through a mirror site in Europe."

This is the latest case of university systems being commandeered to mine for digital currency. Other notable incidents involve a researcher at Harvard and a student at Imperial College London.

https://www.hpcwire.com/2014/06/09/us-researcher-caught-mining-bitcoins-nsf-iron/

Enterprise InfoSec challenges with Research Cybersecurity

- Culture clash: conservative versus publish or perish
- Information Security Office is busy!
- Researcher is busy!
- Unusual research infrastructure
- Dynamic research collaborations
- All these things make this engagement hard!

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

About Trusted CI

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

BERKELEY LAB

WISCONSIN
UNIVERSITY OF WISCONSIN-MADISON

PITTSBURGH SUPERCOMPUTING CENTER

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

UNIVERSITY OF SOUTH ALABAMA

https://trustedci.org/

Trusted CI

...is a trusted partner, not an auditor, not selling a product.

...helps NSF projects tackle their research cybersecurity challenges.

...builds the NSF cybersecurity community.

...leads the community in advancing the state of practice.

...undertakes applied research in community engagement.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Trusted CI: Impacts

Updated impact as of June 2021:

Trusted CI has positively impacted over 490 NSF projects since inception in 2012.

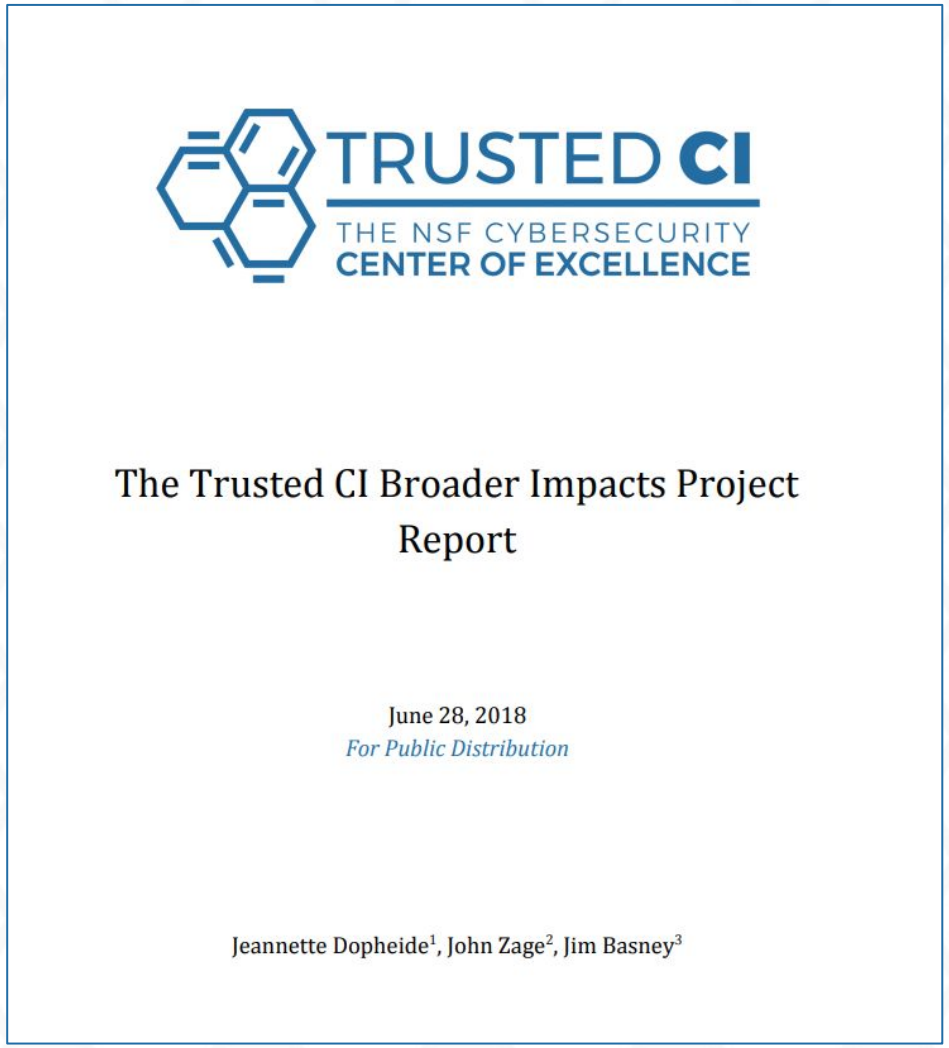
Members of more than 330 NSF projects have attended our NSF Cybersecurity Summit.

Members of more than 160 NSF projects have attended our monthly webinars.

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

We've had 57 engagements with NSF funded projects, including ten NSF Large Facilities.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE



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/

Identity Management Best Practices

https://trustedci.org/iam

Science Gateways

https://trustedci.org/sgci/

Software Assurance

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

Software Engineering Guide

https://sweguide.trustedci.org/

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Engagements: One-on-one Collaborations

Accept applications every six months:

https://trustedci.org/application/

Engagement topics include:

- 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: US ARF
https://www.unols.org/

Engagement addressed:

- Compliance with the upcoming International Maritime Organization 2021 cybersecurity regulations.
- Standardizing policies across the fleet.
- Improving asset management.
- Developing a cybersecurity program for the fleet.

Trusted CI and ARF on the R/V Robert Gordon Sproul

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Example: Globus Auth

https://www.globus.org/

Engagement addressed:

- In-depth vulnerability assessment of the Globus Auth code.
- Applied the First Principles Vulnerability Assessment methodology.
- Checked their implementation of the OAuth2 specification.
- Produced architectural and resource diagrams, and performing an in-depth component analysis.
- No vulnerabilities were found but made recommendations for improving the security of the code.

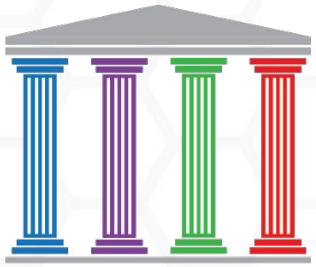
Other Trusted CI Activities

- Webinars
- Annual NSF Cybersecurity Summit
- Consultations
- Annual Challenge (deep dives into a topic)
- Training
- Large Facilities Security Team
- Cyberinfrastructure Vulnerabilities
- Transition to Practice

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

The Trusted CI Framework

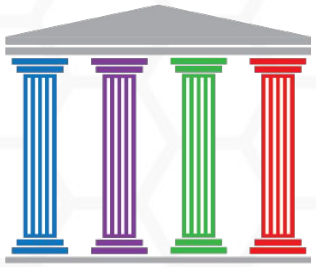
4 Pillars, 16 Musts



Developed to help science project leadership establish effective, efficient cybersecurity programs (not just a list of controls).

Its straightforward structure focuses on foundational decisions about organizational **mission alignment**, **governance**, **resources**, and **controls**.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE



Why Another Cybersecurity Framework?

Organizations need a **reasonable** minimum standard for cybersecurity **programs**.

Our assessments routinely find that the biggest problems lie upstream of technology, namely inadequate funding, personnel, and governance.

Many existing frameworks:

a. Focus on technology/controls;

b. Assume an effective cybersecurity program is in place and it just needs to be told what to do;

c. Are one-size fits all, devolve into checklist exercises, and discourage mission-oriented (*i.e.*, science) trade-offs; ***and/or***

d. Don't speak to senior leaders and decision makers.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

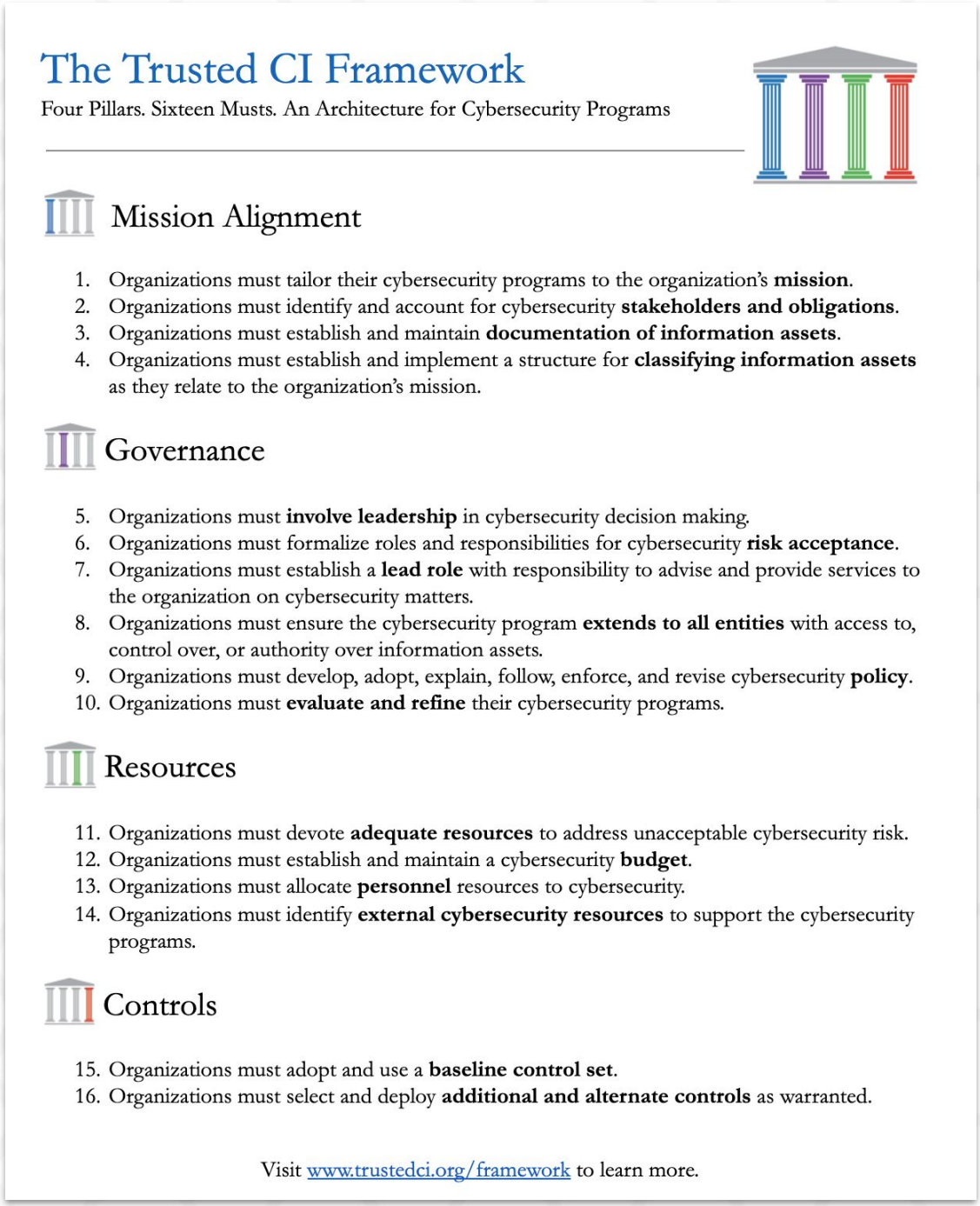
Getting Started

trustedci.org/framework/core

This briefly explains the **16 Musts**. For each, ask yourself, "Have we addressed this? If not, why not? If so, how's it working out?"

Hit the green button to grab the guide, and share with your teams.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE



The Trusted CI Framework

Four Pillars. Sixteen Musts. An Architecture for Cybersecurity Programs

Mission Alignment

1. Organizations must tailor their cybersecurity programs to the organization's **mission**.
2. Organizations must identify and account for cybersecurity **stakeholders and obligations**.
3. Organizations must establish and maintain **documentation of information assets**.
4. Organizations must establish and implement a structure for **classifying information assets** as they relate to the organization's mission.

Governance

5. Organizations must **involve leadership** in cybersecurity decision making.
6. Organizations must formalize roles and responsibilities for cybersecurity **risk acceptance**.
7. Organizations must establish a **lead role** with responsibility to advise and provide services to the organization on cybersecurity matters.
8. Organizations must ensure the cybersecurity program **extends to all entities** with access to, control over, or authority over information assets.
9. Organizations must develop, adopt, explain, follow, enforce, and revise cybersecurity **policy**.
10. Organizations must **evaluate and refine** their cybersecurity programs.

Resources

11. Organizations must devote **adequate resources** to address unacceptable cybersecurity risk.
12. Organizations must establish and maintain a cybersecurity **budget**.
13. Organizations must allocate **personnel** resources to cybersecurity.
14. Organizations must identify **external cybersecurity resources** to support the cybersecurity programs.

Controls

15. Organizations must adopt and use a **baseline control set**.
16. Organizations must select and deploy **additional and alternate controls** as warranted.

Visit www.trustedci.org/framework to learn more.

Some Lessons from Trusted CI's First 10 Years

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Most Cybersecurity problems aren't Technology

Budgeting
Governance
Lack of science mission alignment

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Scientists care about cybersecurity if you talk their language

Examples of what works:

- Trustworthiness of scientific results
- Data integrity
- Enabling collaboration
- Productivity (e.g. availability of instruments)
- Reproducibility

Service and Leadership

Providing services is helpful to build trust and community

- Consultations, best practices, webinars, etc.

Providing leadership is needed to push to make progress.

- Framework, ransomware, etc.

NSF Helpful Getting Cybersecurity into the Budget

NSF-funded project providing operational services for NSF CI

- IDS, virtual CISO/ISO, Ransomware consulting, training

Model: NSF funding first year for first year out of OAC, then project pays ongoing costs

https://researchsoc.iu.edu/

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

@TrustedCI

Monthly Office Hours

Announced on discuss email list

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

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/

Acknowledgments

Trusted CI is supported by the National Science Foundation under Grants 1234408, 1547272, and 1920430.
The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Trusted CI activities are made possible thanks to the contributions of a multi-institutional team:

https://trustedci.org/who-we-are/

Trusted CI License Statement

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Thanks!

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.