



CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

# Cybersecurity for Cyberinfrastructure... and Science!

---

*Von Welch (PI)*

*Susan Sons (HUBzero Engagement Lead)*

*Hubbub 2014*

*30 September 2014*

*[trustedci.org](http://trustedci.org)*

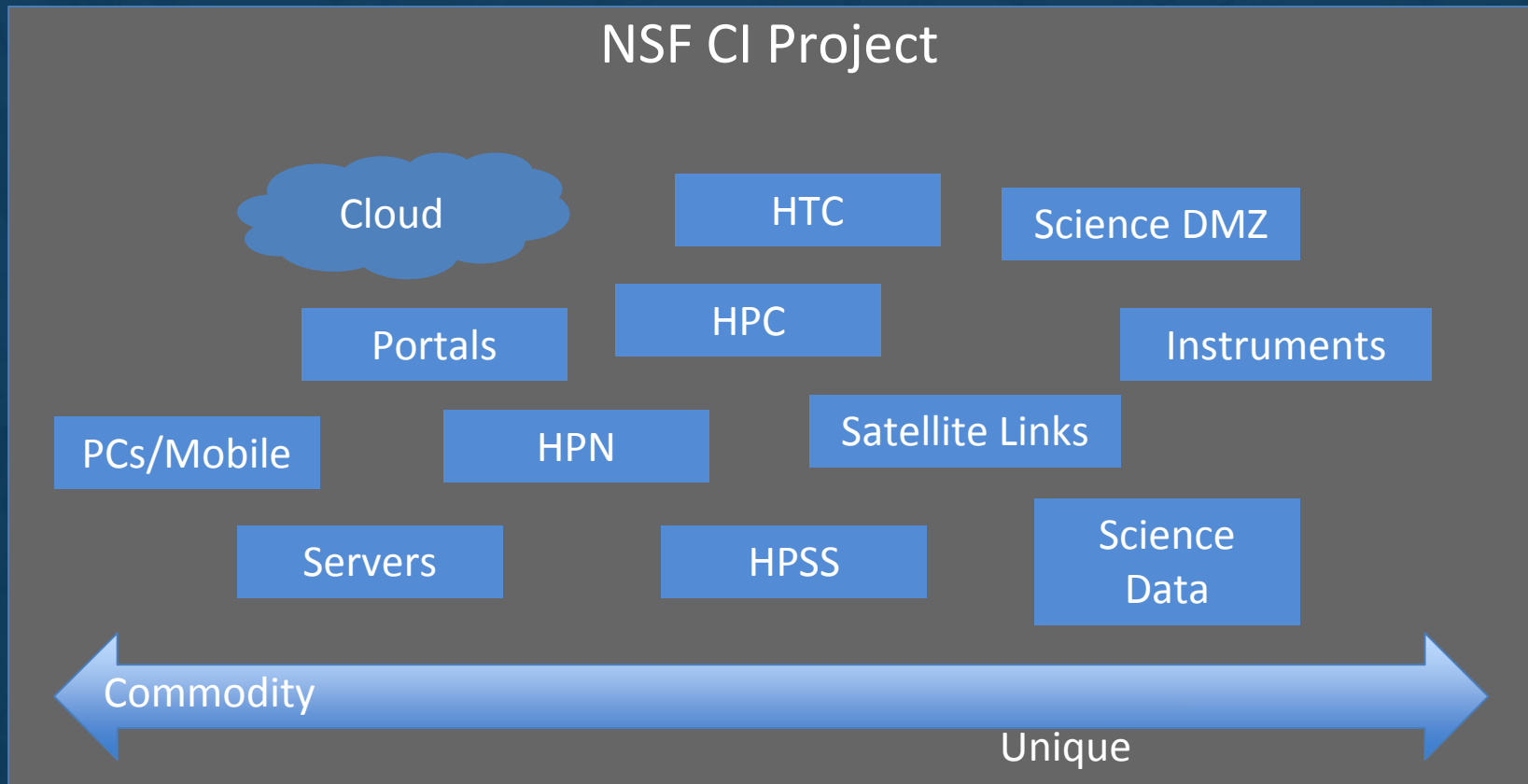
---

# Cyberinfrastructure Ecosystem

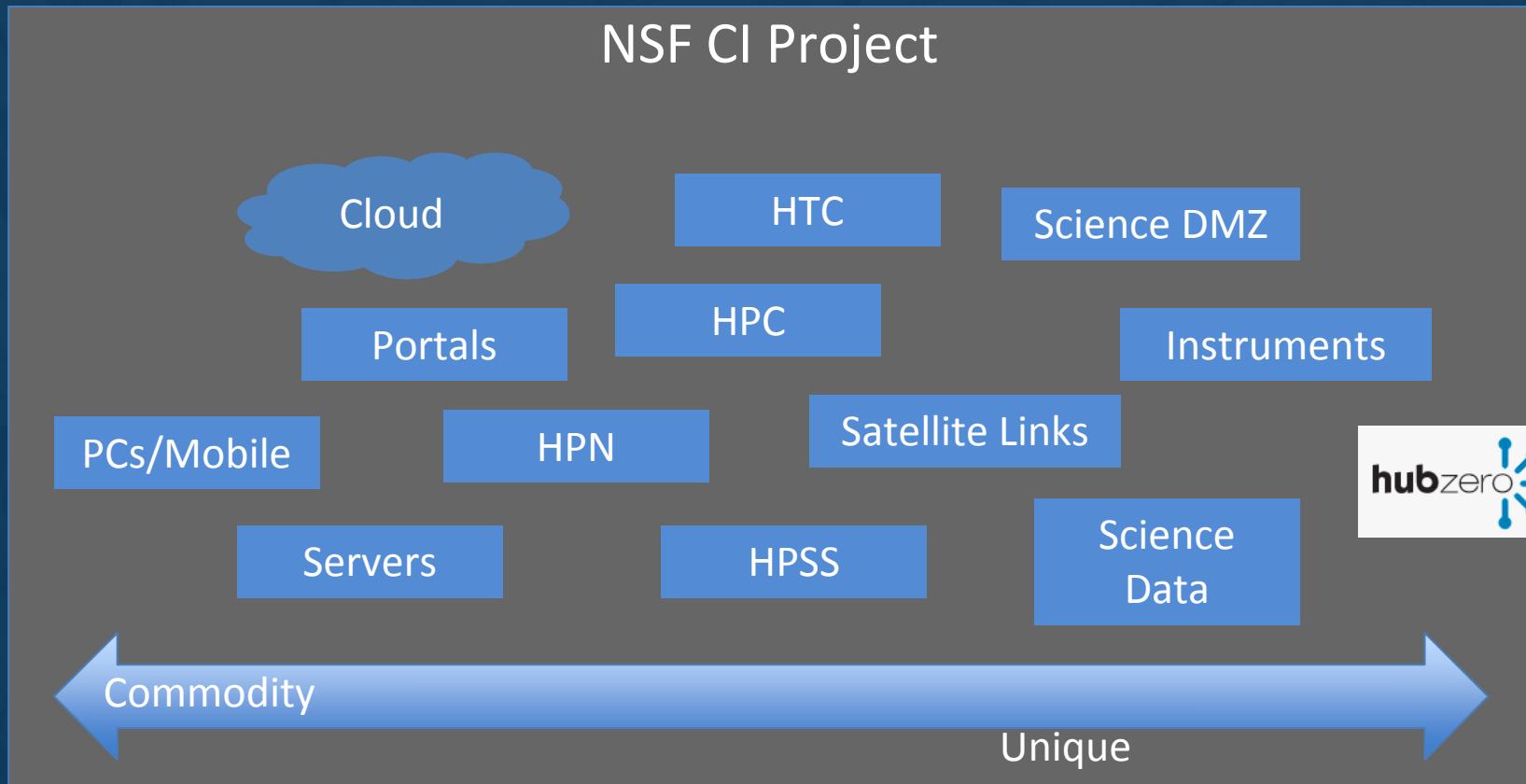


**Maintainability, sustainability, and extensibility**

# NSF Cyberinfrastructure



# NSF Cyberinfrastructure



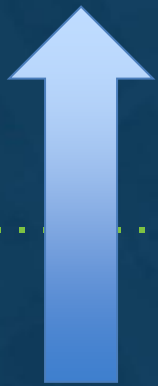
# CTSC

Science!

URE  
Requirements,  
Risks

Distributed Scientific Community

NSF CI Project



Services,  
Risks,  
Policies



Multiple  
Universities  
and/or  
Research  
Orgs  
(IT and  
policies)

CI, R&E, and  
Commercial  
Services

CI and Open  
Source  
Software

R&E  
Networks

...

So, what is cybersecurity for NSF science?

---

# Cybersecurity Historically: Technology

---

Firewalls, IDS, encryption, logs, passwords, etc.

# Cybersecurity Contemporarily

---

Cybersecurity supports an organization's mission by managing risks to information assets.



# Translating to NSF projects...

---

Cybersecurity manages risks to the performance and integrity of computational science.

June 9, 2014

## US Researcher Caught Mining for Bitcoins on NSF Iron

Tiffany Trader



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

Risks  
CYBERINFRASTRUCTURE

### Postdoc and Mentor Perpetuate Data Falsification and Fabrication In a Series of Published Articles

A former postdoctoral researcher and his mentor at a Colorado university perpetuated the apparent validity of research data after the postdoc had intentionally falsified and fabricated the original study. After coauthors on the original study were unable to replicate the postdoc's research results, the mentor's college—without informing university-level administration—conducted an informal inquiry and recommended that the issue be worked out in the literature rather than through a formal investigation. Although the mentor's lab members had been able to repeat the results when the postdoc was there, after he left they could not do so.

The screenshot shows the ISGTW (International Science Grid This Week) website. The main article is titled "Federated trust expands internationally with eduGAIN Declaration" and is dated May 28, 2014. The article text describes an ongoing collaboration between the Laser Interferometer Gravitational-Wave Observatory (LIGO) project and the Center for Trustworthy Scientific Cyberinfrastructure (CTSC). It mentions that CTSC bore fruit recently as InCommon signed the eduGAIN Declaration, marking the first formal step in connecting the main identity federation in the US with 30 peer identity federations worldwide, including those in Australia, Brazil, Canada, Chile, Japan, and New Zealand, as well as in Europe. Below the text is a video player with a play button and a progress bar showing 0:00 / 4:06. The video title is "How to benefit from interfederating through eduGAIN". To the right of the article is a sidebar with "Latest", "Top Rated", and "Editor's Picks" sections. The "Latest" section includes a link to "Advancing excellent science at the EGI Community Forum". The "Top Rated" section includes a link to "Biomedical data and supercomputing analysis reveal links between Alzheimer's and cancer". The "Editor's Picks" section includes a link to "Federated trust expands internationally with eduGAIN Declaration". At the bottom right of the page is the logo for the International Supercomputing Conference (ISC) 2014, The HPC Event.

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

<http://www.nsf.gov/pubs/2014/oig14002/oig14002.pdf>

<http://www.isgtw.org/spotlight/federated-trust-expands-internationally-edugain-declaration>

# Center for Trustworthy Cyberinfrastructure

The goal of CTSC is to provide the NSF community with a coherent understanding of cybersecurity, its importance to computational science, and the resources to achieve and maintain an appropriate cybersecurity program.



CENTER FOR APPLIED  
CYBERSECURITY RESEARCH

INDIANA UNIVERSITY  
Pervasive Technology Institute



THE UNIVERSITY  
of  
**WISCONSIN**  
MADISON



# CTSC Activities

---

## **Engagements**

LIGO, SciGAP, IceCube, Pegasus, CC-NIE peer review, DKIST, LTERNO, DataONE, SEAD, CyberGIS, HUBzero, Globus....

## **Education, Outreach and Training**

Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects, Securing Commodity IT in Scientific CI Projects Baseline Controls and Best Practices, Training for CI professionals.

## **Leadership**

Organized 2013, 2014 & 2015 Cybersecurity Summits for Large Facilities and CI, Incident response, IdM Best Practices.

# CTSC and HUBzero Engagement

---

# HUBzero and cybersecurity

---

Used by 60+ communities, some with 10s or 100s of thousands of users.

Export control (ITAR) and HIPAA compliance requirements.

HUBzero approached CTSC to assess and improve their cybersecurity.

# HUBzero/CTSC “Cybercheckup”

---

Initial week-long “cybercheckup” of existing HUBzero cybersecurity program.

Finding was a mature, robust cybersecurity program.

Identified places for improvement and further review: better documented physical security, use of two-factor authentication, access control, disaster/incident response plan, and vulnerability scan handling.

# In-depth Review

---

- **Web Server Security Model**

*Covers security measures--both technological and procedural--implemented by the HUBzero operations team.*

- **Disaster Recovery Plan**

*Covers operational safeguards that ensure resiliency in case of a major failure, such as a hub hardware failure, and procedures for doing recovery operations.*



# New Initiatives: Formalizing Procedures

---

- **CMS Security Model**

*Codifies the design of access control and other security features of HUBzero's CMS software for program longevity and so that they can be reviewed and improved upon.*

- **Vulnerability Management**

*Formalizing the procedures for managing vulnerabilities discovered both in the CMS software and in HUBzero's operations environment.*

# Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects

---

<http://trustedci.org/guide>

Basis for CTSC evaluation.

Will be extended with vulnerability management as part of HUBzero engagement.



CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

# Thank You

[trustedci.org](https://trustedci.org)

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

---

We thank the National Science Foundation (grant 1234408) for supporting our work.

The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.