



CENTER FOR TRUSTWORTHY  
SCIENTIFIC CYBERINFRASTRUCTURE  
The NSF Cybersecurity Center of Excellence

# The NSF Cybersecurity Center of Excellence

---

James A. Marsteller  
CTSC Co-PI

Towards Security Assured Cyberinfrastructure in Pennsylvania (SAC-PA)  
CI Cybersecurity Workshop  
June 22nd 2017

---

*trustedci.org*

# NSF Cybersecurity Center of Excellence (CCoE)

CTSC began with a 3-year NSF grant in 2012.

NSF 2015 Cybersecurity Innovation for Cyberinfrastructure (CICI) solicitation called for an NSF CCoE.

CTSC submitted a proposal to continue its funding as a CCoE and was awarded this honor.

### 3. Cybersecurity Center of Excellence

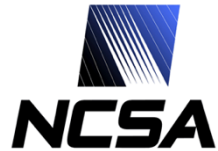
NSF-funded cyberinfrastructure presents unique challenges for operational security personnel. The research environment is purposefully built as an "open" one, in which data is freely accessed among collaborators. As such, sites, centers, campuses and institutions that host cyberinfrastructure must find the right balance of security, privacy and usability while maintaining an environment in which data are openly shared. Many research organizations lack expertise in technical and policy security and could benefit from an independent, shared security resource pool.

A Cybersecurity Center of Excellence must:

- Provide leadership to the NSF research community in the continuous building and distribution of a body of knowledge on the topic of trustworthy cyberinfrastructure;
- Conduct security audits and security architecture design reviews for projects at multiple scales, from large Major Research Equipment and Facilities Construction (MREFC) projects to small CI developments;
- Ensure adoption of security best practices in the NSF research community;
- Provide situational awareness of the current cyber threats to the research and education environment, including those that impact scientific instruments;
- Develop a threat model (or multiple threat models if appropriate), identifying the vulnerabilities in NSF-funded cyberinfrastructure and scientific data associated with that cyberinfrastructure and recommending countermeasures to protect the systems; and
- Host an annual workshop in addition to meetings, seminars, training and other events in order to interact with members of the NSF community, industry, government and academia who wish to collaborate on projects and other initiatives.

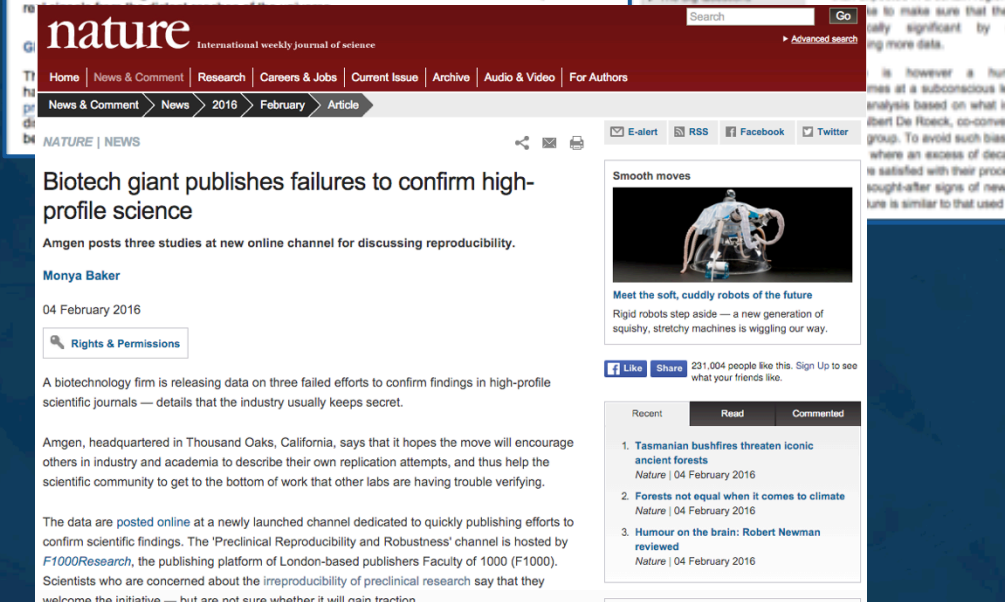
<http://www.nsf.gov/pubs/2015/nsf15549/nsf15549.htm>

<http://trustedci.org/who-we-are/>



# What Really Matters? Trusted and Reproducible Science






# Center for Trustworthy Cyberinfrastructure

## The NSF Cybersecurity Center of Excellence

---

### Mission

Provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.

# Vision for the NSF Science Community

---

1. For the NSF science community to **understand fully the role of cybersecurity in producing trustworthy science.**
2. For all NSF projects and facilities to **have the information and resources they need to build and maintain effective cybersecurity programs** appropriate for their science missions, and responsive to evolving risks and requirements.
3. For **all NSF Large Facilities to have highly effective cybersecurity programs.**

# CCoE Thrusts

---

## **Building Community**

NSF Cybersecurity Summit, Monthly Webinars, Blog, Email Lists, Partnerships, Benchmarking Survey

## **Sharing Knowledge**

Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects, Identity Management Best Practices, Situational Awareness, Training, OSCTP

## **Collaboration to Tackle Challenges: Engagements**

LIGO, SciGaP, IceCube, Pegasus, CC-NIE peer review, DKIST, LTERNO, DataONE, SEAD, CyberGIS, HUBzero, Globus, LSST, NEON, U. Utah, PSU, OOI, Gemini, Array of Things, IBEIS, SciGaP, US Antarctic Program...

# New CCoE Activities

## Building Community

NSF Cybersecurity Summit, **Monthly Webinars**, Blog, Email Lists, **Partnerships**, **Benchmarking Survey**

## Sharing Knowledge

Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects, Identity Management Best Practices, **Situational Awareness**, Training, **OSCTP**

## Collaboration to Tackle Challenges: Engagements

LIGO, SciGaP, IceCube, Pegasus, CC-NIE peer review, DKIST, LTERNO, DataONE, SEAD, CyberGIS, HUBzero, Globus, LSST, NEON, U. Utah, PSU, OOI, Gemini, **Array of Things**, **IBEIS**, **SciGaP**, **US Antarctic Program...**



# Collaboration to Tackle Challenges: Engagements

---

# Engagements

---

Focused collaborations with one (or small group) of NSF projects to tackle a project's cybersecurity or identity and access management challenge.

CCoE's time is covered by our NSF grant.

## Examples:

Developing a cybersecurity program

Assessing an existing program

Software assurance/evaluation

Custom training

IAM design

*Your challenge here...*

# Any challenge is in scope!

## More examples...

Drafting a Privacy Policy (AoT)

Security Officer search (LIGO)

Identity and Access

Management:

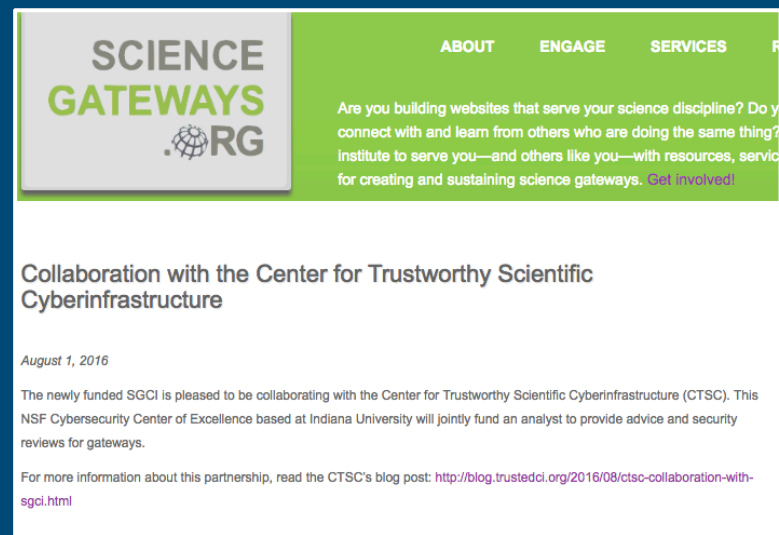
<http://trustedci.org/iam/>

Software Assurance:

<http://trustedci.org/software-assurance/>

## Science Gateways w/SGCI SI2 Institute:

<http://sciencegateways.org/news/collaboration-ctsc/>



The screenshot shows a webpage header for Science Gateways with a logo and navigation links (ABOUT, ENGAGE, SERVICES). Below the header is a green banner with a call to action: "Are you building websites that serve your science discipline? Do you connect with and learn from others who are doing the same thing? The SGCI SI2 Institute to serve you—and others like you—with resources, services, and support for creating and sustaining science gateways. [Get involved!](#)"

The main content area features the title "Collaboration with the Center for Trustworthy Scientific Cyberinfrastructure" and a date "August 1, 2016". The text reads: "The newly funded SGCI is pleased to be collaborating with the Center for Trustworthy Scientific Cyberinfrastructure (CTSC). This NSF Cybersecurity Center of Excellence based at Indiana University will jointly fund an analyst to provide advice and security reviews for gateways." A link is provided for more information: "For more information about this partnership, read the CTSC's blog post: <http://blog.trustedci.org/2016/08/ctsc-collaboration-with-sgci.html>"



CENTER FOR TRUSTWORTHY  
SCIENTIFIC CYBERINFRASTRUCTURE  
The NSF Cybersecurity Center of Excellence

Home

About CTSC +

Getting Help From CTSC

Engaged Communities -

Engagements Home

Engagement Application

AARC

AOT

## Apply for a One-on-One Engagement with CTSC

One of CTSC's core activities is conducting one-on-one engagements with NSF projects and facilities. To manage scheduling and learn about prospective engagees, we have instituted an engagement application process. When you are ready to apply, click the link below and complete the online form.

>> [Click here to complete the CTSC Engagement Application Form.](#)

### Our Application Review Cycle & Current Status

We review applications and plan engagements on a six-month cycle, unless an expedited process is undertaken for a particular application. Most of our engagements are executed over a 1 to 6 month period. If you are seeking a letter of support for a proposal, please contact [info@trustedci.org](mailto:info@trustedci.org).

Currently, we are accepting applications for Jan-Jun 2017 engagements and Jul-Dec 2017 engagements. We encourage early application (before the deadline) to help us process applications efficiently and thoroughly.

### Important Dates:

- Sep 16, 2016: Applications due for engagements to be executed Jan-Jun 2017
- Nov 4, 2016: Applicants notified
- Jan 2016: Kickoff new engagements for Jan-Jun 2017
- Mar 17, 2017: Applications due for engagement to be executed Jul-Dec 2017
- May 5, 2017: Applicants notified

Application Review Processing & Phases

<http://trustedci.org/application>

Demand outpacing Supply, **online application process.**  
Summer 2017: Begin accepting applications for consideration for execution in the first half of CY 2018.

# Sharing Knowledge

## Guides, Best Practices, Situational Awareness, Training

---

# Situational Awareness

---

Advise NSF CI community about **relevant software vulnerabilities** and provide guidance on mitigation. Leverage NIST, US-CERT, XSEDE, REN-ISAC, and other sources of vulnerability information. **Please subscribe** to the email list(s) to receive situational awareness notifications of relevance to you.

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

# Cybersecurity Guides and Tools

Addressing concerns **unique to science**

Policy templates:

Acceptable Use, Access Control,  
Asset Management, Disaster  
Recovery, Incident Response,  
Inventory, Awareness, Physical  
Security, ...

Risk assessment table

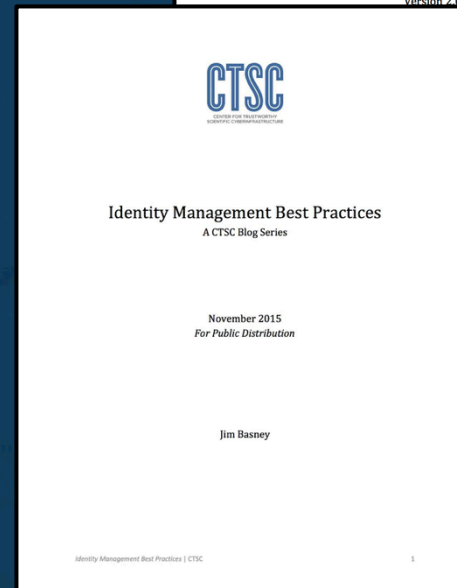
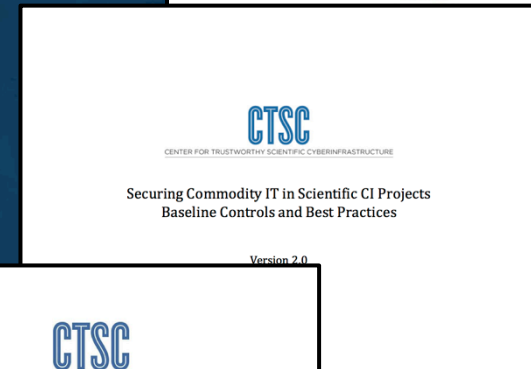
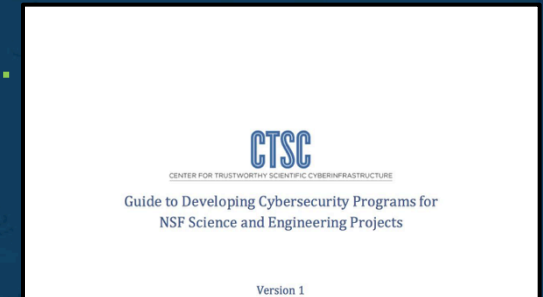
Securing commodity IT

Self-assessment Tool

Identity Management Best Practices

<http://trustedci.org/guide>

<http://trustedci.org/iam>





CENTER FOR TRUSTWORTHY  
SCIENTIFIC CYBERINFRASTRUCTURE  
The NSF Cybersecurity Center of Excellence

Home

About CTSC +

Getting Help From CTSC

Engaged Communities +

Community Resources +

Training -

Online Training

Training Materials

## Training materials

2016 Spring Practical Cybersecurity for Open Science Projects

2015 NSF Cybersecurity Summit Training Materials (August 17, 2015)

- Bro Platform Training Workshop - Johanna Amann (ICSI), Justin Azoff (NCSA) & Adam Slagell (NCSA)
- Developing Cybersecurity Programs for NSF Projects - Bob Cowles, Craig Jackson, Jim Marsteller & Susan Sons (CTSC)
- Vulnerabilities, Threats, and Secure Coding Practices - Barton P. Miller & Elisa Heymann
- Industrial Control Systems, Networking, and Cybersecurity - Phil Salkie (Jenarlah Industrial Automation)
- Aligning your Research Cyberinfrastructure with HIPAA and FISMA - Anurag Shankar (Indiana University)
- Incident Response Training - Randy Butler (NCSA)

2014 NSF Cybersecurity Summit Training Materials (August 26, 2014)

- Developing Cybersecurity Programs for NSF Projects (PDF) - Jim Marsteller, Susan Sons, Craig Jackson, Jared Allar (CTSC)
  - Also available as a series of online videos
- Vulnerabilities, Threats, and Secure Coding Practices (PDF) - Barton P. Miller, James A. Kupsch, Elisa Heymann (University of Wisconsin)
- HPC, HIPAA, and FISMA: Meeting the Regulatory Challenge through Effective Risk Management (PowerPoint) - Bill Barnett & Anurag Shankar (Indiana University)
- Incident Response Training (Powerpoint part 1, Powerpoint part 2) - Randy Butler, Warren Raquel, Patrick Duda (NCSA)

NSF Cybersecurity Summit, XSEDE, SuperComputing, **other locations by request.**

Topics: Cybersecurity Program Development, Incident Response, Secure Coding, Software Engineering...

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



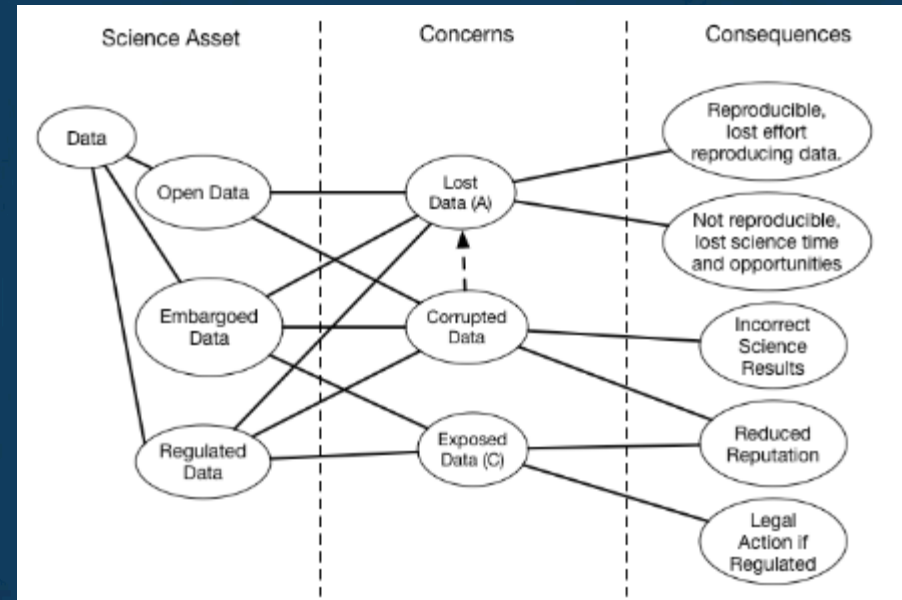
# The Open Science Cyberthreat Profile: Understanding the Cybersecurity of Science

Scientists and cybersecurity professionals need to communicate to understand the risks related to science assets to the science mission.

OSCTP working group is **developing a profile of open science assets and their common risks** to aid risk management for open science.

Presentations from ATLAS, IBEIS, LSST, and OOI (& DataONE in Sep.)

Published in late 2016. <https://trustedci.org/oscrp/>



Members: **Altintas** (SDSC), **Bevier** (Caltech), **Cuff** (Harvard), **LeDuc** (Northwestern), **Meunier** (Purdue/HUBzero), **Moore** (iRods), **Schwab** (ISI), **Stocks** (UCSD)  
Organizers: **Adams** (CTSC), **Dopheide** (ESnet), **Peisert** (ESnet), **Welch** (CTSC).

# Building Community

NSF Cybersecurity Summit, Webinars, Blog, Email  
Lists, Partnerships

---

# NSF Cybersecurity Summit

---

- Inaugural summit in 2004 in response to cyber attack affecting many NSF funded projects
- CTSC Relaunched Summit in 2013 after 4 year hiatus
- **Growing!** 90 registrants in 2015, **100** in 2016.
- Opportunity for LFs, CI projects, MREFCs to collaborate: build **connections**, identify and solve **common challenges**, develop **best practices**, share **experiences**, receive **training**.
- **Address** the changing threat landscape for NSF CI.

More info at <http://trustedci.org/summit/>

# Summit Recommendations **turn into Actions**

## *2015 Summit Recommendations*

- *Recommendation 1: The NSF CI and Large Facility community should **develop** a broadly applicable strategy for information security budgets, including how, why, and where it does what it does in terms of spending*
- *Recommendation 2: The NSF CI and Large Facility community should **support research on metrics that indicate** whether spending on information security is sufficient and appropriately balanced with a project's science mission*
- *Recommendation 3: The NSF CI and Large Facility community should develop a **common understanding** among all stakeholders of how accountability, risk responsibility, and risk acceptance practices are most efficiently and appropriately distributed among project leadership, project personnel, and other stakeholders*
- *Recommendation 4: The NSF CI and Large Facility community should determine its **software assurance, quality, and supply chain requirements***

Reflected in this year's **Call for Participation** and the **activities of the CCoE**.

Recommendations from 2016 will similarly **carry over** into action.

# Building Consensus: **Software Assurance**

*Recommendation 4: The NSF CI and Large Facility community should determine its **software assurance, quality, and supply chain requirements***

Our plan:

Work with Large Facilities and other NSF large projects to determine software expectations.

Disseminate expectations, with implementation guidance and help, to software developers (e.g. NSF SI2 community).

Leverage community resources e.g. Software Assurance Marketplace.



# CTSC Webinar Series

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

---

## *Upcoming Webinars:*

- *July 24th: **Internet2 Cyberinfrastructure** by Paul Howell (Registration coming soon)*
- *August 28th: **Improving the Security and Usability of Two-Factor Authentication for Cyberinfrastructure** with Nitesh Saxena & Stanislaw Jarecki*
- *September 25th: **Threat Intelligence Sharing** with Romain Wartel*

Contact [info@trustedci.org](mailto:info@trustedci.org) if have a suggestion for a presentation or would like to present.

Suggestion: **CICI projects and RCNs, CC\*, etc.**

# Partnerships

---

**Interoperability with** and **best practices** from our global collaborators.

**ESnet**: Open Science Cyberthreat Profile

**AARC**: Identity Management with the EU

**SGCI SI2 Institute**: Science Gateway cybersecurity

**Bro CoE**: Training, network security

**REN-ISAC**: Situational Awareness

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

# Community Benchmarking Survey

---

**Goal:** To produce a report on the aggregated state of cybersecurity across the community and track the improvement of that state over time.

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



## Staying in contact with the CCoE

---

Join our email lists for discussions and updates:

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

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

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





CENTER FOR TRUSTWORTHY  
SCIENTIFIC CYBERINFRASTRUCTURE  
The NSF Cybersecurity Center of Excellence

Thank You

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

---

We thank the National Science Foundation (grant 1547272) 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.