The NSF Cybersecurity Center of Excellence

Craig Jackson
Chief Policy Analyst, Indiana University Center for Applied Cybersecurity Research
Co-PI, NSF Cybersecurity Center of Excellence

GPN ENCITE Webinar
24 Feb 2017

trustedci.org
NSF Cybersecurity Center of Excellence (CCoE)

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

Re-funded in 2015 for 3 years via ACI/OAC’s Cybersecurity Innovation for Cyberinfrastructure (CICI) solicitation.

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.

What does cybersecurity mean for NSF Science? Is it relevant?
Our Information Environment is Stormy
Science Happens in a Complex Ecosystem

Science!

Distributed Scientific Community

NSF Cyberinfrastructure (IT++)

- Multiple Universities and/or Research Orgs (IT and policies)
- CI, R&E, and Commercial Services
- CI and Open Source Software
- R&E Networks

Requirements, Risks

Services, Risks, Policies
What Really Matters? Trustworthy and Reproducible Science

A biotechnology firm is releasing data on three failed efforts to confirm findings in high-profile scientific journals — details that the industry usually keeps secret.

Amgen, headquartered in Thousand Oaks, California, says that it hopes the move will encourage others in industry and academia to describe their own replication attempts, and thus help the scientific community get to the bottom of work that other labs are having trouble verifying.

The data are posted online at a newly launched channel dedicated to quickly publishing efforts to confirm scientific findings. The Precritical Reproducibility and Robustness channel is hosted by PLoS (Public Library of Science). Faculty of 1000 (F1000).

Scientists who are concerned about the irreproducibility of preclinical research say that they welcome the initiative — but are not sure whether it will catch traction.
“I’m doing open science… I don’t need cybersecurity.”

- Information has always been central to science.
- And, the Internet’s severe weather conditions impact everyone who is connected.
- Cybersecurity is about confidentiality, availability, and integrity of information and information systems.
  - Availability of instruments and systems.
  - Trust in and availability of the data.
- Reputation, trust, and other “intangibles” matter.
We know science projects and facilities are experiencing a range of adverse information security events.
Some of it is Internet weather.
Some of it is targeted.
“My data isn’t valuable to anyone…”

“...except you!”
How does open science navigate all of this?
Our Philosophy, Mission, Vision, and Activities
If the highest aim of a captain were to preserve his ship, he would keep it in port forever.

- Thomas Aquinas
Zero Risk --> Zero Science
Balance is Key: **Mission and Risk**

Minimize Three Things:

- Cost of breaches/incidents
- Cost of cybersecurity program
- Negative impact on science productivity

Text paraphrased from: “The Defender’s Dilemma. Charting a Course Toward Cybersecurity”
[http://www.rand.org/pubs/research_reports/RR1024.html](http://www.rand.org/pubs/research_reports/RR1024.html)
CTSC’s mission is to 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 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

More information at trustedci.org
Collaboration to Tackle Challenges:
Engagements
Engagements
trustedci.org/application

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

Our effort 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...

Demand outpaces supply; apply by March 17 for late 2017 engagements.
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/
Sharing Knowledge
Guides, Best Practices, Situational Awareness, Training
Cybersecurity Guides and Tools
trustedci.org/guide
trustedci.org/iam

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
The Open Science Cyberthreat Profile
trustedci.org/oscrp

OSCTP working group has developed a profile of **common open science assets and associated cyber risks**.

Facilitates communication among scientists and cybersecurity practitioners.

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

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).
Advise NSF CI community about **relevant software vulnerabilities** and provide guidance on mitigation.


**Please subscribe** to the email list(s) to receive situational awareness notifications of relevance to you.
Training
trustedci.org/trainingmaterials/

NSF Cybersecurity Summit, XSEDE, SuperComputing,...
other venues by request or as engagement deliverables.

Topics:
● Cybersecurity Program Development
● Incident Response
● Secure Coding
● Software Engineering
Building Community

NSF Cybersecurity Summit, Webinars, Blog, Email Lists, Partnerships
NSF Cybersecurity Summit
trustedci.org/summit

- Started in 2004 in response to cyber attack affecting many NSF funded projects
- CTSC relaunched Summit in 2013 after 4 year hiatus
- Growing! 90 registrants last year, >120 this year.
- More sharing! CFP. Opportunities to build connections, identify and solve common challenges, develop best practices, share experiences, receive training.
- Reports inform agendas and CCoE activities on a continuous basis: Identifying and solving problems.

Past Reports at http://trustedci.org/useful-links/
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

Recordings of past webinars are available online.

Upcoming:

- February 27th (11am ET): Practical Cybersecurity Program for (Smaller) Science Projects with Susan Sons, Craig Jackson, & Bob Cowles
- March 27th (11am ET): SDN and IAM Integration at Duke
- April 24th (11am ET): Compliance panel with Susan Ramsey & Anurag Shankar
- May 22nd (11am ET): Cybersecurity Research: Transition to Practice with Emily Nichols and Alec Yasinsac

Contact info@trustedci.org if have a suggestion for a presentation or would like to present. Suggestion: CICI projects and RCNs, CC*, etc.
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

**NSF CICI Regional Cybersecurity Collaboration projects**: CORE, SAC-PA, SCEPTRE, and SouthEast SECURE
Connecting with us...

Join our email lists for discussions and updates:
[trustedci.org/ctsc-email-lists](trustedci.org/ctsc-email-lists)

Blog: [blog.trustedci.org](blog.trustedci.org)

Twitter: @TrustedCI

scjackso@iu.edu
Thank You! Questions?

trustedci.org
@TrustedCI

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.