Welcome to the CCoE Webinar Series kickoff presentation. Our speakers today are Von Welch, Jim Basney, James Marsteller, and Barton Miller. Our host is Jeannette Dopheide.

The meeting will begin shortly. Participants are muted. You may type questions into the chat box during the presentation.

This meeting is being recorded.

The CTSC Webinar Series is supported by National Science Foundation grant #1547272.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.
The Cybersecurity Challenge to NSF Science
Science Must be **Trusted and Reproducible**

**Biotech giant publishes failures to confirm high-profile science**

Amgen posts three studies at new online channel for discussing reproducibility.

Monya Baker
04 February 2016

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 to 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 *Preclinical Reproducibility and Robustness* channel is hosted by PLoS Research, the publishing platform of London-based publisher 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 do the trick.
Science Happens in a Complicated 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

Services, Risks, Policies

Requirements, Risks
Our IT World is Stormy

Hackers Remotely Kill a Jeep on the Highway—With Me in It

Hacking America

FBI: Computer expert briefly made plane fly sideways

Nasa hack: AnonSec attempts to crash $222m drone, releases secret flight videos and employee data

Symantec Security

Digital Extortion: Rise
“My science and data is open, hence I don’t need cybersecurity…”

No need for confidentiality is not a “Get of of Jail Free” card!

Reputation, trust, and other “intangibles” matter.

Integrity and availability of data

Illicit use of systems

Availability of instruments

Before “going public” with big news.

Hacktivism

Etc.
“My data isn’t valuable to anyone…”

“...except me!”
Zero Risk == Zero Science
Balance is Key: Mission and Risk

Minimize:
Cost of breaches/incidents
+ 
Cost of cybersecurity program 
+ 
Impact on science productivity

One Million Cybersecurity Job Openings In 2016

Steve Morgan, CONTRIBUTOR
I write about the business of cybersecurity.

Discover our three approaches to help bring cyber security risk to a manageable level.

> Read the POV

How does science navigate all of this?
Center for Trustworthy Cyberinfrastructure
The NSF Cybersecurity Center of Excellence

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.
NSF Cybersecurity Center of Excellence (CCoE)

CTSC began with a 3-year NSF grant in 2013.

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

CTSC submitted a proposal 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.

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.
CTSC Activities
More information at trustedci.org

Tailored Public Resources
Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects; Identity Management Best Practices; Email Lists, Vulnerability Announcements

Outreach
Blog; Participation in LF Workshop; Int’l relationships

Community Events
Annual NSF Cybersecurity Summit, Monthly Webinars

Training
Developing Programs, Secure Coding, Incident Response

Engagements
New CTSC Activities as CCoE

- Expanded situational awareness service

- Annual community benchmarking survey

- Threat model for open science

- Tailoring resources for smaller / newer projects

- Software assurance
  [http://trustedci.org/software-assurance/](http://trustedci.org/software-assurance/)

- Identity and access management (IAM)
  [http://trustedci.org/iam/](http://trustedci.org/iam/)
Focused Discussions

Identity and Access Management

Situational Awareness

Software Assurance

NSF Cybersecurity Summit
Identity and Access Management (IAM)

IAM is an important part of the cybersecurity program. Enabling access to NSF CI while managing risks. Supporting distributed scientific collaborations. Leveraging shared IAM services like InCommon. Topics: identity federation, password management, multi-factor authentication, access control policies, ...

http://trustedci.org/iam
CTSC IAM Engagements To-Date

**AARC:** US-EU coordination

**DataONE:** IAM system review

**IBEIS:** SSO and RBAC system design and prototyping

**LIGO:** international interfederation

**SciGaP:** science gateway authentication/authorization

http://trustedci.org/engagements
InCommon went international in February!

CTSC & LIGO engagement launched InCommon’s interfederation working group in 2013.

blog.trustedci.org/2013/01/interfed.html

http://incommon.org/edugain/
Providing 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/
Software Assurance

Software assurance is the natural progression from developing security programs and assessing risk to improving software development security practices.

- Training
- Engagements
- Situational Awareness
- Best Practices

http://trustedci.org/software-assurance/
Software Assurance

- **Software Engineering Best Practices:** How to develop secure code, be ready for vulnerabilities, distribute code securely.
- Working with NSF Large Facilities, Software Institutes & other projects to drive **consensus on software security requirements**.
- More **training**, including software assurance tools (and SWAMP), mobile, executive briefs, software development best practices.
- **New delivery methods:** videos, MOOC
- **Situational Awareness** - alerts about vulnerabilities in software CI relies on and advice on addressing.
Software Assurance

Leverage freely available resources, including the DHS-funded Software Assurance Marketplac (SWAMP)

https://www.mir-swamp.org

Help projects to transition to a continuous software assurance model, leveraging an open, simple-to-use source of code analysis tools for a wide variety of languages and environments.
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
- Opportunity for CI, MREFCs to collaborate: solve common challenges, develop best practices, share experiences/knowledge, training sessions
- Help to address the changing threat landscape for NSF CI
2015 Summit Highlights

“Understanding the Information Assets that Enable Science”

- 90 Participants
- **Significant** growth in Call For Participation (17 submissions) had more proposals than available time
- Attendee evaluations and feedback were overwhelmingly positive - 95% rating summit as “good” or “excellent”
- Expanded training program to full day
2016 Call For Participation (CFP)

Now accepting community proposals:
- Plenary Presentations
- Training Sessions
- Table Top Sessions
- Student Program
- CFP Deadline June 3rd

More information: http://trustedci.org/summit

CFP topics addressing 2015 findings are encouraged
Suggested CFP Topics

2015 Findings:

- **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.
Suggested CFP Topics

2015 Findings (con’t):

- **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*
2016 NSF Cybersecurity Summit:
August 16-18, 2016 - Arlington, Virginia

http://trustedci.org/summit
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.
About the CTSC Webinar Series

To view presentations, join the discuss mailing list, or submit requests to present, visit:

http://trustedci.org/webinars

The next webinar is June 27th at 11am EDT
Speaker: Terry Fleury
Topic: Risk Self-Evaluation

The CTSC Webinar Series is supported by National Science Foundation grant #1547272.

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