



CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

Cybersecurity for NSF Science: What does that mean?

Von Welch, PI CTSC

*NSF Cybersecurity Summit
August 27, 2014*

trustedci.org

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



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.

What we have learned about cybersecurity for NSF science?

Cybersecurity Historically: Technology

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

Cybersecurity Contemporarily

Cybersecurity supports an organization by managing risks to information assets from a range of threats.

(Manage == reduce, mitigate, and accept.)

Translating to NSF projects...

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

Risky Thinking in the Context of Science

What are the threats?

What are our assets?

Data, infrastructure, reputation, etc.

What risks to the assets are intolerable to the science?

How do we manage those risks?

Challenges to NSF Cybersecurity

Where to start? NIST SP800 is over 150 documents!

What are our threats?

Complexity: open, multi-organizational projects.

Short-lived projects, changing technology - building principles and body of knowledge?

Heterogeneity - from disk drives to earthquake tables, satellites, telescopes, etc. - we've got it.

Learn, Collaborate and Sharing

Understand what we are trying to accomplish and how we (imperfectly!) measure effectiveness.

Get over the cultural factors and be willing to share, teach, and learn.

Transfer knowledge from project to project - directly or imbue into persistent community.

Principles that Survive Over Time

Constant change in threats, technology, science collaborations, etc. makes practices ephemeral.

Need to determine not just what we do today, but principles on how we figure out what to do tomorrow!

Progress by CTSC

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

Securing Commodity IT in Scientific CI Projects
Baseline Controls and Best Practices

Training

NSF Cybersecurity Summits for LF and CI
Good CFP Response!



CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

Thank You

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.

Extra slides

Challenges

Getting started...

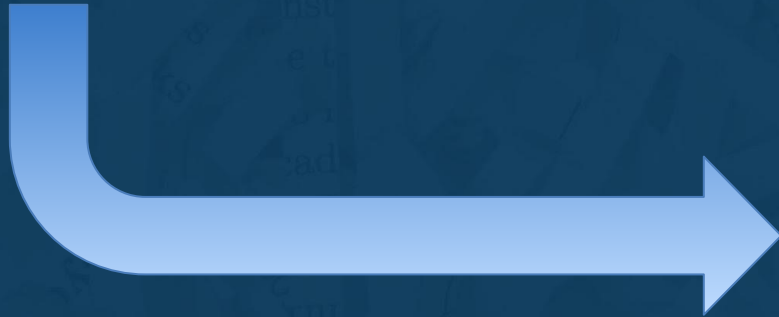
56. Information Security

Security for all information technology (IT) systems employed in the performance of this award, including equipment and information, is the awardee's responsibility. Within a time mutually agreed upon by the awardee and the cognizant NSF Program Officer, the awardee shall provide a written Summary of the policies, procedures, and practices employed by the awardee's organization as part of the organization's IT security program, in place or planned, to protect research and education activities in support of the award.

The Summary shall describe the information security program appropriate for the project including, but not limited to: roles and responsibilities, risk assessment, technical safeguards, administrative safeguards, physical safeguards, policies and procedures, awareness and training, and notification procedures in the event of a cyber-security breach. The Summary shall include the institution's evaluation criteria that will measure the successful implementation of the IT Security Program. In addition, the Summary shall address appropriate security measures required of all subawardees, subcontractors, researchers and others who will have access to the systems employed in support of this award.

The Summary will be the basis of a dialogue which NSF will have with the awardee, directly or through community meetings. Discussions will address a number of topics, such as, but not limited to, evolving security concerns and concomitant cyber-security policy and procedures within the government and at awardees' institutions, available education and training activities in cyber-security, and coordination activities among NSF awardees.

NSF CA T&C
Item 59
234 words



NIST SP800
Cybersecurity documents
~150 documents

The screenshot shows the NIST Computer Security Division website. The main content area is titled "SPECIAL PUBLICATIONS (800 SERIES)". Below the title is a table with columns for "Number", "Date", and "Title". The table lists several publications, including "2012 Computer Security Division Annual Report", "DRAFT Guidelines on Hardware-Rooted Security in Mobile Devices", "DRAFT Guide to Attribute Based Access Control (ABAC) Definition and Considerations", "DRAFT BIOS Integrity Measurement Guidelines", "Guidelines for Securing Wireless Local Area Networks (WLANs)", "DRAFT A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS)", "DRAFT BIOS Protection Guidelines for Servers", and "Basic Input/Output System (BIOS) Protection Guidelines".

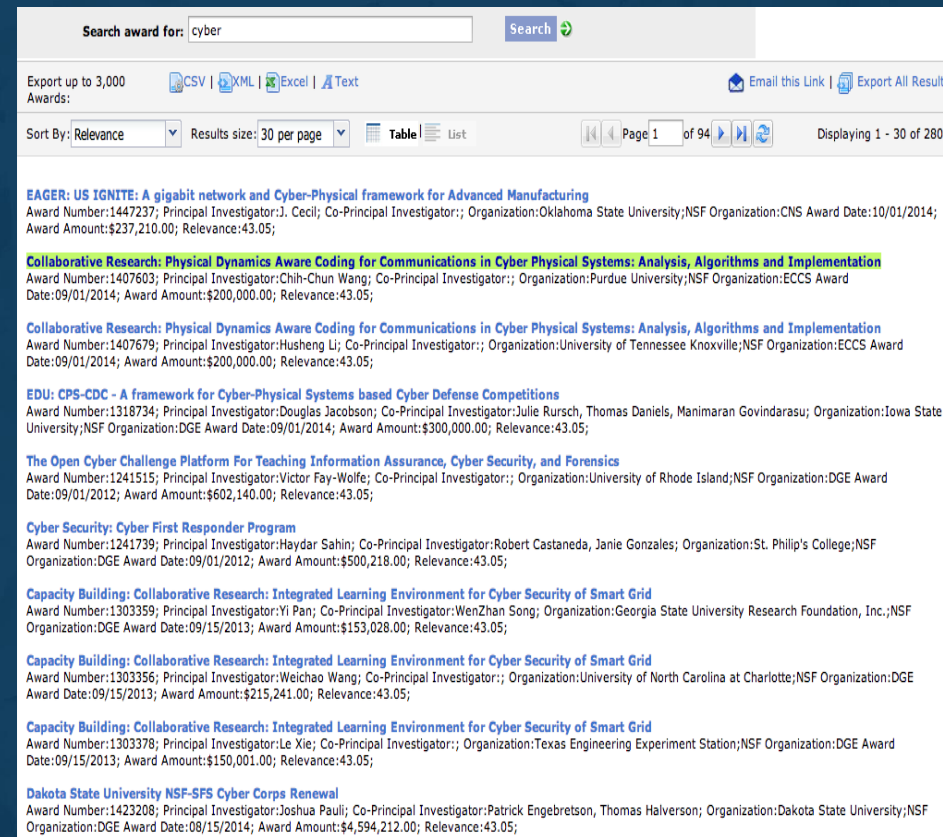
Number	Date	Title
SP 800-163	June 2013	2012 Computer Security Division Annual Report Annual Report (2012)
SP 800-164	Oct. 31, 2012 (Draft)	DRAFT Guidelines on Hardware-Rooted Security in Mobile Devices Announcement and Draft Publication
SP 800-162	April 22, 2013 (Draft)	DRAFT Guide to Attribute Based Access Control (ABAC) Definition and Considerations Announcement and Draft Publication
SP 800-155	Dec. 8, 2011 (Draft)	DRAFT BIOS Integrity Measurement Guidelines Announcement and Draft Publication
SP 800-153	Feb. 2012	Guidelines for Securing Wireless Local Area Networks (WLANs) SP 800-153
SP 800-152	August 8, 2012 (Draft)	DRAFT A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS) Announcement and Draft Publication
SP 800-147 B	July 30, 2012 (Draft)	DRAFT BIOS Protection Guidelines for Servers Announcement and Draft Publication
SP 800-147	Apr. 2011	Basic Input/Output System (BIOS) Protection Guidelines SP 800-147

Maintaining the Wheel

Short-lived (~3-5 year) projects.

Underlying technologies are constantly changing.

Corpus of knowledge is a smattering of papers (with no mistakes!)



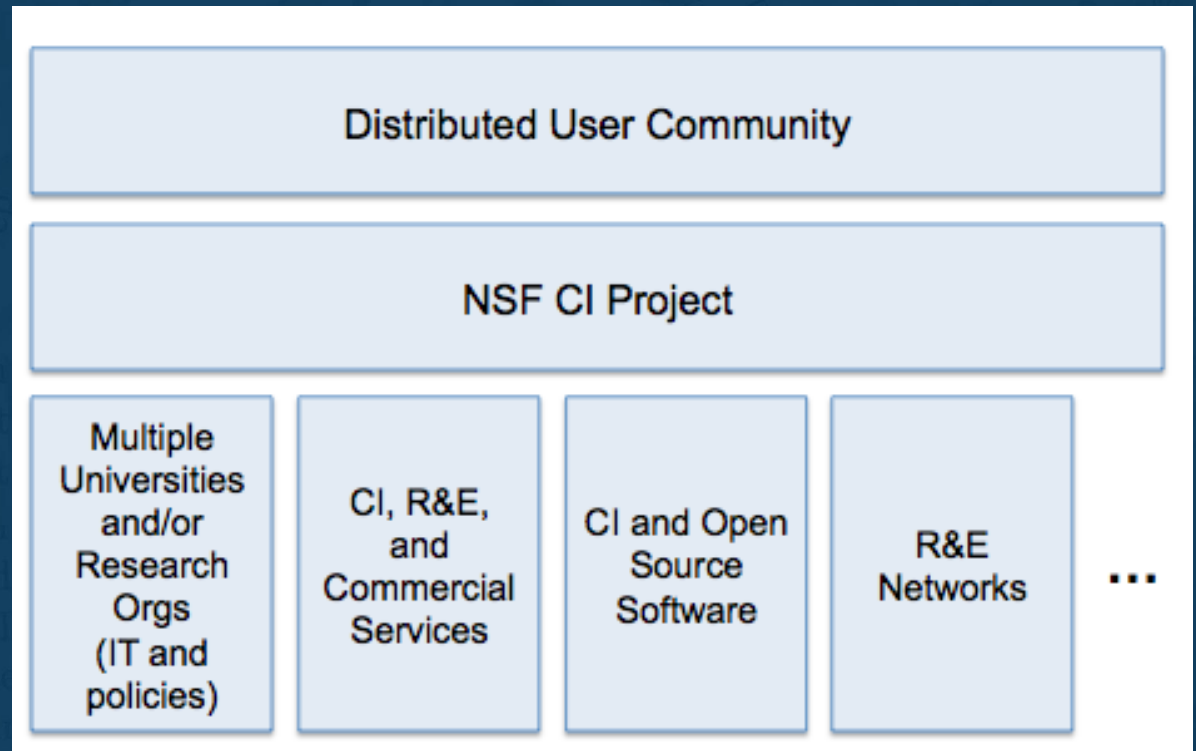
The screenshot shows a search results page for the keyword 'cyber'. The search bar at the top contains 'cyber' and a search button. Below the search bar, there are options to export up to 3,000 awards in CSV, XML, Excel, or Text format. The results are sorted by Relevance, with 30 items per page. The first few results are:

- EAGER: US IGNITE: A gigabit network and Cyber-Physical framework for Advanced Manufacturing**
Award Number:1447237; Principal Investigator:J. Cecil; Co-Principal Investigator;; Organization:Oklahoma State University;NSF Organization:CNS Award Date:10/01/2014; Award Amount:\$237,210.00; Relevance:43.05;
- Collaborative Research: Physical Dynamics Aware Coding for Communications in Cyber Physical Systems: Analysis, Algorithms and Implementation**
Award Number:1407603; Principal Investigator:Chih-Chun Wang; Co-Principal Investigator;; Organization:Purdue University;NSF Organization:ECCS Award Date:09/01/2014; Award Amount:\$200,000.00; Relevance:43.05;
- Collaborative Research: Physical Dynamics Aware Coding for Communications in Cyber Physical Systems: Analysis, Algorithms and Implementation**
Award Number:1407679; Principal Investigator:Husheng Li; Co-Principal Investigator;; Organization:University of Tennessee Knoxville;NSF Organization:ECCS Award Date:09/01/2014; Award Amount:\$200,000.00; Relevance:43.05;
- EDU: CPS-CDC - A framework for Cyber-Physical Systems based Cyber Defense Competitions**
Award Number:1318734; Principal Investigator:Douglas Jacobson; Co-Principal Investigator:Julie Rursch, Thomas Daniels, Manimaran Govindarasu; Organization:Iowa State University;NSF Organization:DGE Award Date:09/01/2014; Award Amount:\$300,000.00; Relevance:43.05;
- The Open Cyber Challenge Platform For Teaching Information Assurance, Cyber Security, and Forensics**
Award Number:1241515; Principal Investigator:Victor Fay-Wolfe; Co-Principal Investigator;; Organization:University of Rhode Island;NSF Organization:DGE Award Date:09/01/2012; Award Amount:\$602,140.00; Relevance:43.05;
- Cyber Security: Cyber First Responder Program**
Award Number:1241739; Principal Investigator:Haydar Sahin; Co-Principal Investigator:Robert Castaneda, Janie Gonzales; Organization:St. Philip's College;NSF Organization:DGE Award Date:09/01/2012; Award Amount:\$500,218.00; Relevance:43.05;
- Capacity Building: Collaborative Research: Integrated Learning Environment for Cyber Security of Smart Grid**
Award Number:1303359; Principal Investigator:Yi Pan; Co-Principal Investigator:WenZhan Song; Organization:Georgia State University Research Foundation, Inc.;NSF Organization:DGE Award Date:09/15/2013; Award Amount:\$153,028.00; Relevance:43.05;
- Capacity Building: Collaborative Research: Integrated Learning Environment for Cyber Security of Smart Grid**
Award Number:1303356; Principal Investigator:WeiChao Wang; Co-Principal Investigator;; Organization:University of North Carolina at Charlotte;NSF Organization:DGE Award Date:09/15/2013; Award Amount:\$215,241.00; Relevance:43.05;
- Capacity Building: Collaborative Research: Integrated Learning Environment for Cyber Security of Smart Grid**
Award Number:1303378; Principal Investigator:Le Xie; Co-Principal Investigator;; Organization:Texas Engineering Experiment Station;NSF Organization:DGE Award Date:09/15/2013; Award Amount:\$150,001.00; Relevance:43.05;
- Dakota State University NSF-SFS Cyber Corps Renewal**
Award Number:1423208; Principal Investigator:Joshua Pauli; Co-Principal Investigator:Patrick Engebretson, Thomas Halverson; Organization:Dakota State University;NSF Organization:DGE Award Date:08/15/2014; Award Amount:\$4,594,212.00; Relevance:43.05;

Complexity

How do we manage risk on a finite budget and with many trust relationships?

Need appropriate abstractions for sites, whole classes of users, commercial services, etc.



Heterogeneity of Computational Science

Single PI to multi-org teams.

Discipline-specific, interdisciplinary,
and general-purpose.

Varying maturity.

Development, integration,
deployment, and operations.

Compute, network, data, storage,
unique science instruments,
software, web portals, services,
etc.

Cybersecurity and trust are a combination of technical and social issues: the right solutions applied in the right way – there is no “one size fits all.”

Understanding and adapting to the community’s needs and desires is critical.