CTSC

CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE

The NSF Cybersecurity Center of Excellence

CTSC and the Guide to Developing Cybersecurity Programs for Science and Engineering Projects

Bob Cowles

EUGridPMA, Bratislava
19 January 2016

NSF Grant Announcement

IU leads $5 million collaborative grant for NSF-funded Cybersecurity Center of Excellence

Jan. 15, 2016
FOR IMMEDIATE RELEASE

BLOOMINGTON, Ind. -- The security of the more than $7 billion in research funded by the National Science Foundation will be significantly bolstered, thanks to a $5 million grant to Indiana University and partner institutions to create the NSF Cybersecurity Center of Excellence.

The funding will designate the IU-led Center for Trustworthy Scientific Cyberinfrastructure as a Cybersecurity Center of Excellence.

The center, a three-year-old collaboration between IU, the National Center for Supercomputing Applications, the Pittsburgh Supercomputing Center and the University of Wisconsin-Madison, works to address cybersecurity challenges of NSF science.

Ensuring scientific computing remains trustworthy and uncorrupted is essential in protecting the nation's science. In its role as a Cybersecurity Center of Excellence, the CTSC will provide readily available cybersecurity services tailored to the NSF science community.

These resources will include leadership and coordination across organizations, and education and training to expand the pool of available cybersecurity expertise.

CTSC Grant Announcement

CTSC funded as the NSF Cybersecurity Center of Excellence

We're pleased to announce that CTSC has been funded for the next three years as the NSF Cybersecurity Center of Excellence. Ensuring scientific computing remains trustworthy and uncorrupted is essential in protecting the nation's science. In its role as a Cybersecurity Center of Excellence, the CTSC will provide readily available cybersecurity services tailored to the NSF science community.

These resources will include leadership and coordination across organizations, and education and training to expand the pool of available cybersecurity expertise.

"NSF-funded cyberinfrastructure presents unique challenges for operational security personnel and impacts other important areas of research affecting society, including ocean sciences, natural hazards, engineering, biology and physics," said Anita Nikolich, cybersecurity program director at the NSF's advanced cyberinfrastructure division. "Organizations 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."

The CTSC will collaborate directly with NSF-funded research organizations to address their cybersecurity challenges and provide forums for cybersecurity collaboration across organizations.

Additionally, the CTSC will collaborate with the U.S. Department of Energy's Energy Science Network, or ESnet, to develop a threat profile for open science.

CTSC Mission

Improve the cybersecurity of NSF science and engineering projects, while allowing those projects to focus on their science endeavors


Training for CI Professionals
One-on-One Engagements
Leadership

Training for CI Professionals

Audiences:

- PIs and managers
- Technical staff

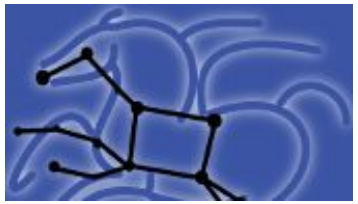
We present at existing conferences (XSEDE, SC, NSF Cybersecurity Summit, etc.) or can come to you.

Can contribute cybersecurity to an existing curriculum.

Topics:

- Secure coding
- Identity Management and Federation
- Developing a cybersecurity plan.
- Incident Response

One-on-One Engagements



(DKIST)

One-on-One Engagements

Collaboratively addressing a cybersecurity issue:

- Building or reviewing a cybersecurity plan
- Software assessment
- Design review
- Advanced challenges (federated IdM, delegation, etc.)
- Topics as needed by the community.

No cost outside of time and effort.

Can be answering a question,
a phone call to advise,
a day-long review,
or week-to-months of collaboration.

One-on-One: CyberCheckup

Week-long review of an existing cybersecurity plan.

Project provides documents, we return a quick evaluation for missing/weak components.

Can lead to a full collaboration. Quicker to schedule.

One-on-One: CyberCheckup

Friday, August 14, 2015

Gemini and CTSC Collaborate on Intensive Cybercheckup

In June 2015, as a precursor to a forthcoming full engagement, Gemini Observatory and CTSC undertook a brief, but very intensive "cybercheckup"-style engagement. Using Indiana University's REDCap service (https://redcap.uits.iu.edu/), CTSC has developed a questionnaire designed to gather key pieces of information regarding the information security program at large-scale NSF projects and facilities. Gemini personnel completed this questionnaire, and met with the CTSC engagement team on two occasions, to discuss the cybercheckup process and provide more detailed information. In early July, CTSC delivered a report to Gemini with recommendations for the Gemini information security program, prioritized by CTSC's estimated cost and impact in implementing the recommendations. Following the NSF Cybersecurity Summit, we will sit down in person in Arlington to review the report. Gemini and CTSC will use these results to structure and make the most of our Fall 2015 full engagement.

Leadership

Leadership: NSF Cybersecurity Summit

Leadership: Operational Best Practices

Leadership: Threat Intelligence

Leadership: Enable Collaboration

Monday, June 8, 2015

AARC and CTSC Collaborate on Interfederation

CTSC is starting a collaboration with the European Authentication and Authorisation for Research and Collaboration (AARC) project on use of federated identities for international science. AARC is a two year project that started May 2015. Jim Basney from CTSC joined the June 3-4 AARC kick-off meeting to begin the collaboration.

As the infrastructures for international scientific collaborations migrate from X.509 to SAML for identity management, there is a strong need for interoperability across national SAML federation boundaries. In 2014, the US InCommon federation joined eduGAIN, which connects SAML federations around the world, and now InCommon is engaging with science projects on international interfederation pilots. At the same time, the AARC project in Europe is addressing international adoption of SAML federations by research projects. This represents an opportunity to achieve critical mass around EU-US interfederation activities for science, with CTSC providing needed coordination on the US side.

Leadership: Risk-based Cybersecurity Process for NSF Community

Friday, December 4, 2015

CTSC Risk Assessment of NEON

The National Ecological Observatory Network (NEON) is a nationwide network of ecological sensors and observation facilities sponsored by the National Science Foundation (NSF) to gather and synthesize data on the impacts of climate change, land use change, and invasive species on natural resources and biodiversity. NEON collects data from over 80 land and water based sites across the United States and standardizes this data for use by scientists.

CTSC, in collaboration with the NEON team, performed a cybersecurity risk assessment on the NEON network of sensors and data servers. The results of this assessment will be used to develop a cybersecurity plan for the NEON project. The engagement commenced in March 2015 and was completed in August 2015. CTSC personnel conducted this review using CTSC assessment methodologies designed to fit the scope and objectives of the review. CTSC personnel interacted closely with NEON personnel to perform this engagement.

The goals for the collaboration with NEON were to:

- generate a list of threats, vulnerabilities, estimates for likelihood, and impacts;
- review and prioritize these lists into risks; and
- generate a high level cybersecurity plan for NEON's Airborne Observation Platform (AOP) and CyberInfrastruture (CI).

CTSC Guide

Program formalization is a key step in virtually all maturity models for distinguishing relatively immature programs from relatively mature. Policy development and implementation is necessary for formalization.

Results in:

- Reproducible, communicable, and enforceable processes.
- Artifacts that can be critiqued and evolved.

Background: Getting Started

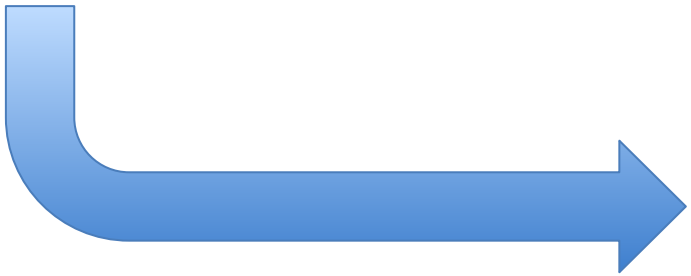
56. Information Security

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.

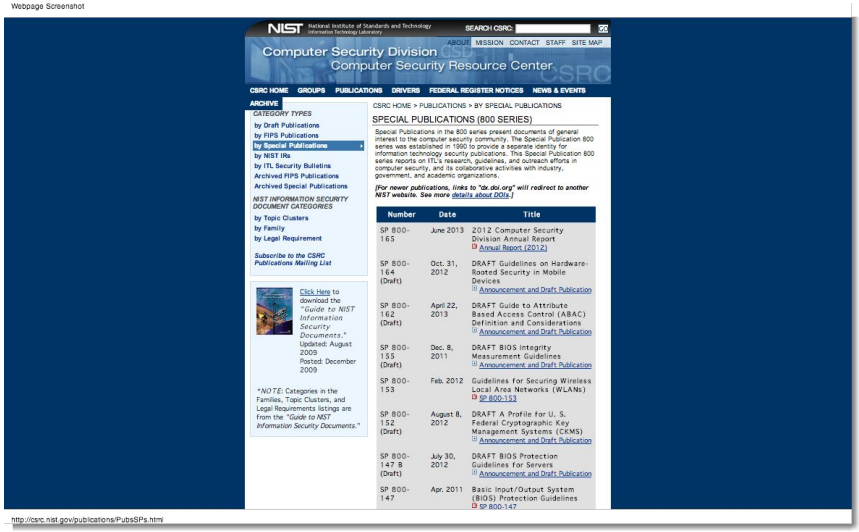
The Summary shall describe the information security program appropriate for the project including, but not limited to: roles and responsibilities, risk assessment, technical safeguards, administrative safeguards, physical safeguards, policies and procedures, awareness and training, and notification procedures 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 Cooperative Agreement T&C
234 words



Webpage Screenshot



NIST SP800
Cybersecurity documents
~150 documents

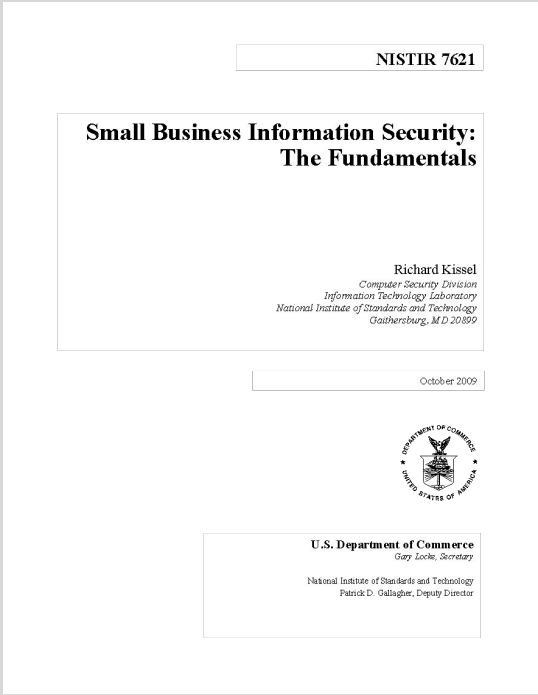
CTSC

To be fair, there is some good work out there for the small organization…

Cybersecurity 2011…
and beyond
What Makes a Good Security Plan?

Ardoth Hassler
Senior IT Advisor
National Science Foundation

Associate VP University Information Services
Georgetown University


NISTIR 7621

Small Business Information Security:
The Fundamentals

Richard Kissel
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

October 2009

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Deputy Director

…but it's the exception and not the rule.

CTSC

Background: Environment

The landscape is a churn of mostly short-lived (~3-5 year) projects, organizations and personnel.

Underlying technologies are constantly changing.

Knowledge base is, at best, hard to capture from a wide range of papers. (Mistakes often not captured.)

Background: Heterogenous NSF Projects

Small (single PI) to large (multi-org teams).

Discipline-specific, interdisciplinary, and general-purpose.

Varying maturity: Development, integration, deployment, and operations.

Compute, network, data, storage, 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.

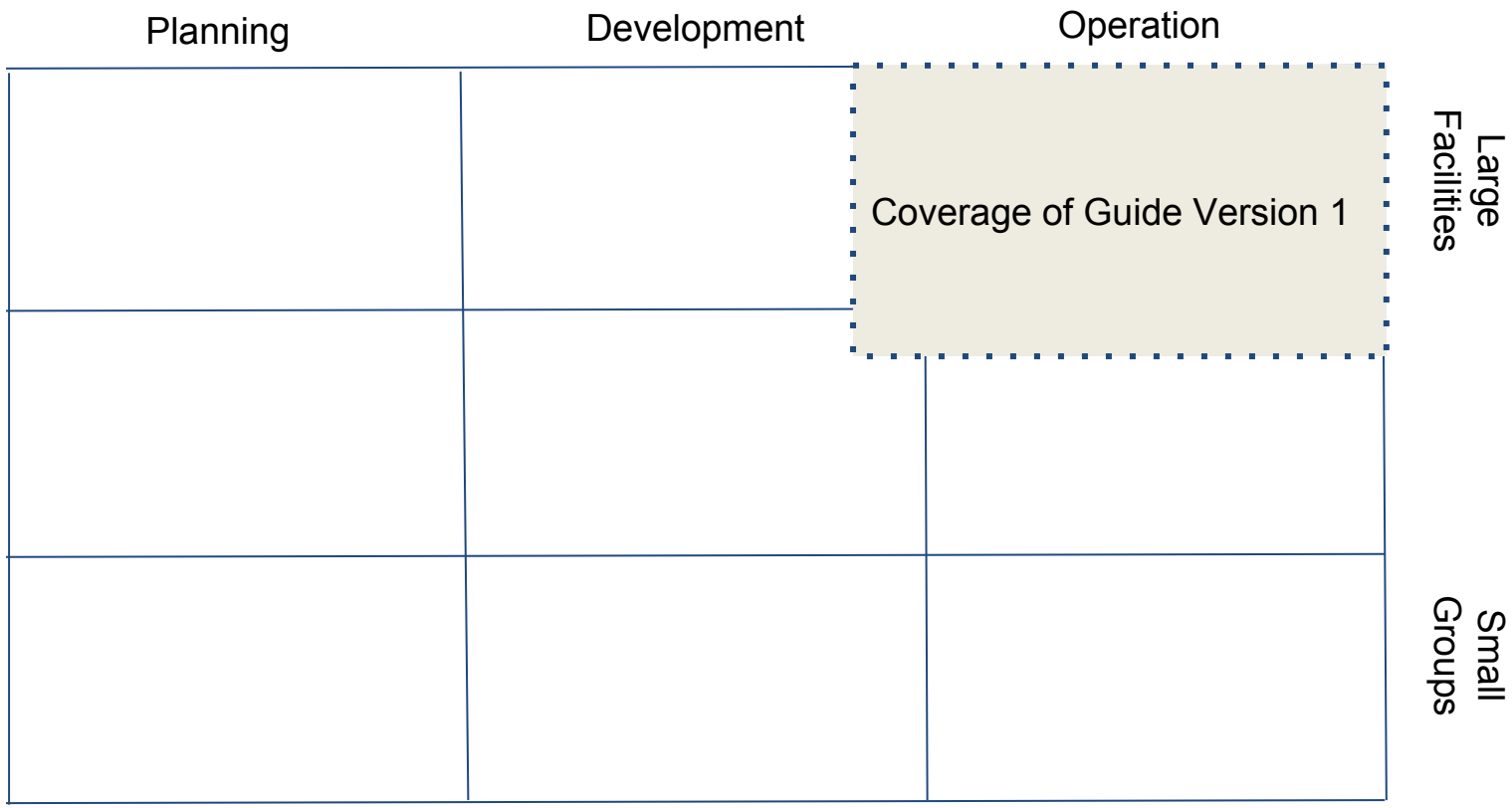
Guide: Provide Framework & Templates

The 40+ page Guide is located at:
http://trustedci.org/guide
(link near top of page under “Read the Guide”)

The templates are found at:
http://trustedci.org/guide

Cautionary Note told to engagees:
Make these your own

Guide: Coverage of NSF Projects



Guide: Highlighted Policies

- Master Information Security Policy and Procedures (MISPP)
- Acceptable Use Policy (AUP)
- Incident Response Policies & Procedures
- Access Control Policy
- Note about Privacy Policies

(But… Physical security, disaster recovery, asset management, HR-specific, "specials" specific… other policies can be critically important for your project.)

-

Master Information Security Policy & Procedures

Purpose: Core, general policies + guide for navigating the full corpus of policies and procedures.

- Roles & Responsibilities (... CISO, Leadership)
- Developing, Implementing, and Maintaining Our Cybersecurity Program (... core processes)
- Resources & Key Contacts (... we're here to help)
- Other Policy and Procedure Documents (a gateway of sorts)
- Enforcement provisions
- Terms & Acronyms
- … plus anything else so central to the program that it warrants stating here

Acceptable Use Policy

Purpose: Establish a code-of-conduct for all users on the usage of a resource/information system.

- Define rights and responsibilities of all users
- Establishes authority
- Consequences of infractions to policy (suspension, legal, criminal)
- Reduce Liability: disclaimers, no warranties
- Other Policy and Procedure Documents (Privacy, Password, management, Academic Citation)
- Contact Information (General support, Emergency/Security)

Incident Response Policy

Purpose: Decide and document what to do in the event of a security incident BEFORE on happens, so that the response can be both rapid and well thought out.

- Define priorities for IR (e.g. relative importance of gathering forensic data vs. minimizing downtime)
- Define who is responsible for which decisions
- Lay out response procedures for grey pigeon and black swan events
- Specify when and how response procedures will be tested

Access Control Policy

Purpose: Define how access to various information assets (both systems and data) will be mediated, as well as who will be allowed access to what.

- Know what your assets are
- Least privilege principle
- Authentication vs. authorization
- Impacts every control

Note About Privacy Policies …

There is not a template, on purpose

- Might not be required
- Might not not want to have one
- Legal implications … talk to general counsel
- International collaboration can complicate things in a hurry!!!!

Policy Development: Tips and Gotchas …

- Do:
  - Involve stakeholders (yes, even the relevant lawyers)
  - Prioritize
  - Use templates, examples from others
  - Ask for help
  - Share the resulting policies and train your personnel
- Please don't:
  - Allow policies to be developed without a formal approval process
  - Work in a vacuum
  - Assume you need one of each
  - Be afraid to take this seriously
  - Underestimate the power of v2

Guide V2: Starting Work

- Revisions
  - Incorporate feedback from projects
  - Incorporate text and ideas developed in CTSC's draft contribution to the cyber security section of the NSF Large Facilities Manual
  - Incorporate other suggestions / revisions / corrections
- Ideas (not vetted with Guide team)
  - Improve coverage (applicability) of Guide
  - Break up Guide into separate chapters
    - Provide overview - what pieces to select / implement
    - Allow selection based on timeframe and project size
    - Easier update process

Thank You!

bob.cowles@gmail.com

Resources

www.trustedci.org

www.trustedci.org/guide

blog.trustedci.org

@TrustedCI

The Center for Trustworthy Scientific Cyberinfrastructure is the Cybersecrutity Center of Excellence supported by the National Science Foundation under award ACI-1547272.