CTSC

CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

The NSF Cybersecurity Center of Excellence

Welcome to the CCoE Webinar Series. Our speakers today are from the Regional CICI Cybersecurity Collaboration Projects. Our host is Amy Starzynski Coddens.

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.

Cybersecurity Innovation for Cyberinfrastructure (CICI)

Anita Nikolich
Program Director, Advanced Cyberinfrastructure
Dec 12, 2016

Cybersecurity Innovation for Cyberinfrastructure (CICI) NSF 16-533

Activities that impact the security of science, engineering and education environments – the scientific workflow

Target community is operational cyberinfrastructure

- Program Areas:
  - Secure and Resilient Architecture ($1M awards/3 year)
  - Regional Cybersecurity Collaboration ($500K awards/2 year)
- Awards:
  - 4 Regional
  - 8 Secure and Resilient Architecture

Cybersecurity Innovation for Cyberinfrastructure (CICI) NSF 17-528

- Due March 1, 2017
- Program Areas:
  - Secure and Resilient Architecture ($1M awards/3 year)
    - Proofs of concept/prototypes encouraged
  - Cybersecurity Enhancement ($1M awards/2 year)
    - Partnership with CISO and/or campus IT

How can NSF help?

- Tell us CICI areas that have been overlooked
- Tell us your cybersecurity challenge or success story!
- Can we help connect you with good work or research that's been done?

anikolic@nsf.gov

Xinwen Fu

New England Cybersecurity Operation and Research Center (CORE)

CICI: Regional: New England Cybersecurity Operation and Research Center (CORE)

Xinwen Fu (PI), UMass Lowell
Benyuan Liu (Co-PI) , UMass Lowell
Yan Luo (Co-PI) , UMass Lowell
Lawrence Wilson (Co-PI), UMass President Office
Keith Moran (Consultant), UMass President Office

About CORE

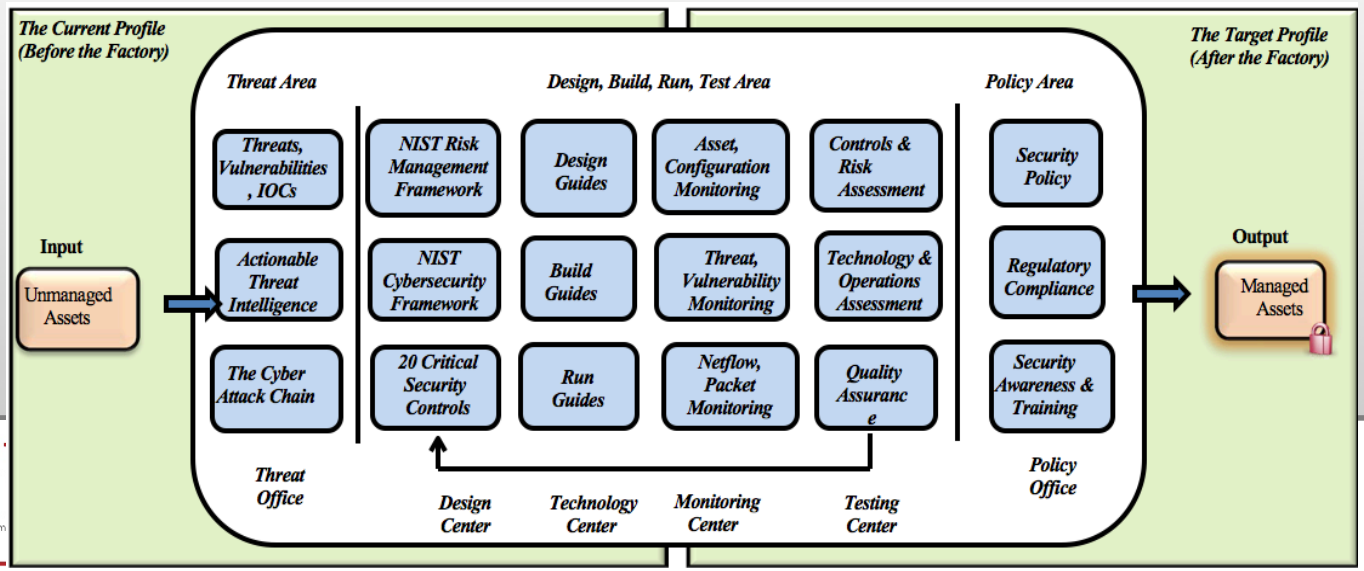
- A Regional New England Cybersecurity Operation and REsearch Center (CORE)
  - University of Massachusetts Lowell (UMass Lowell) and the Office of the President of University of Massachusetts
  - Hosted in the UMass Data Center in Shrewsbury, MA
  - A satellite site at the Center of Internet Security and Forensics Education and Research (iSAFER) of UMass Lowell, a member of National Centers of Academic Excellence in Cyber Defense Research (CAE-R) designated by NSA and DHS
  - A collaboration among regional institutions and industrial partners

Services of CORE

- The focus on under-resourced colleges and universities & collaboration with government and industry partners
  - Cybersecurity education/certification, security consulting/design reviews and assessments, cybersecurity implementation/professional services, cybersecurity operations/managed security services and cybersecurity research on emerging threats, trends and defense.
- A long list of partnerships with local IT and cybersecurity related organizations and consortia
  - Advanced Cyber Security Center (ACSC), Boston Consortium for Higher Education, Information Systems Audit and Control Association (ISACA)

Open Cybersecurity Program for Regional Support

- Based on the NIST Cybersecurity Framework
- An organization first discovers their current security framework profile and subsequently determine their target profile.
- Security controls are then applied to corresponding assets to implement the target profile.
- The controls program factory: the input = unmanaged asset with weak controls or without controls; the output:= is a managed asset with strong controls.



No.	Cybersecurity Service	Service Description
1	Threat and Vulnerability Management Practice	Provide our partners with the latest threat and vulnerability intelligence information through collaboration and sharing with our service partners.
2	Cybersecurity Program Design and Build Service	Help our customers design, implement and maintain their cybersecurity program based on the NIST Cybersecurity Framework [NIST14] and 20 Critical Security Controls (CSC).
3	Cybersecurity Operations and Incident Response Service	Provide 24×7 continuous security monitoring, alerting and escalation; ensuring incidents are detected, investigated, communicated, remediated and reported.
4	Cybersecurity Risk Management Practice	Help our customers identify, understand and address risks to their assets [DHS11].
5	Cybersecurity Education, Training, Awareness	Include CAE-CDE (National Centers of Academic Excellence in Cyber Defense Education), CAE-2Y (National Centers of Academic Excellence in Cyber Defense 2-Year Education), CAE-R (National Centers of Academic Excellence in Cyber Defense Research), Industry Certification training with ISACA (Information Systems Audit and Control Association) and ISC2 (IT Certification and Security Experts), Designing and Building a Cybersecurity Program based on the NIST Framework, Cybersecurity Awareness and Skills Training.
6	Sponsored Projects, Testing, Student Internships	Sponsor projects from ACSC (Advanced Cyber Security Center) members and other industry partners defined and delivered through a Statement of Work (SOW). Provide University security lab services, delivered and managed by students internships under supervision of the University President's Office and campus IT departments.

Research, Education and Outreach

- Research
  - Derive baseline truth of cyber attacks and trends
  - Scaling firewall performance with Apache Spark
  - Behavior based methodology to analyze malware and attacks to IoT
- Education
  - Help developing cybersecurity workforce
  - Internships, co-ops in security operation and research center
- Outreach
  - Direct support to under-resourced institutions
  - Workshops, tutorials, seminars to regional organizations

James Joshi & Brian Stengel

SAC-PA: Security Assured Cyberinfrastructure in Pennsylvania

NSF CICI Regional: SAC-PA: Towards Security Assured Cyberinfrastructure in Pennsylvania

DEC 12, 2016

JAMES JOSHI (PI)
PROFESSOR & DIRECTOR, LERSAIS
UNIVERSITY OF PITTSBURGH

People Involved

- James Joshi (PI), Professor, SIS, University of Pittsburgh
- Brian Stengel (Co-PI), University of Pittsburgh
- Balaji Palanisamy (Co-PI), Assistant Professor, SIS
- Michael B. Spring (Co-PI), Associate Professor, SIS
- Prashant Krishnamurthy (Co-PI), Associate Professor, SIS
- David Tipper (Co-PI), Professor, SIS

Project Page: http://www.sis.pitt.edu/lersais/research/sac-pa/

LERSAIS Page: http://www.sis.pitt.edu/lersais/

Motivation

- Data-driven scientific research & discovery
  - An unprecedented opportunity
- Cybersecurity is growing concern
  - Can be huge setback for scientific research/education if cyberinfrastructures are not protected
  - A significant national security issue
- Challenges:
  - Public-privated cyberinfrastructure resources need to be interlinked/shared and protected
    - Need to help resource-constrained institutions
  - Cybersecurity needs and risks vary – requiring better ways to manage resources and institutional risk
  - Security best practices, better collaboration among stakeholders - sharing resources, expertise and information
- Regional collaboration and partnership among cyberinfrastructure providers and users critical !!
  - Such concerted collaborative effort is also very critical in addressing the National Cyberecurity concerns

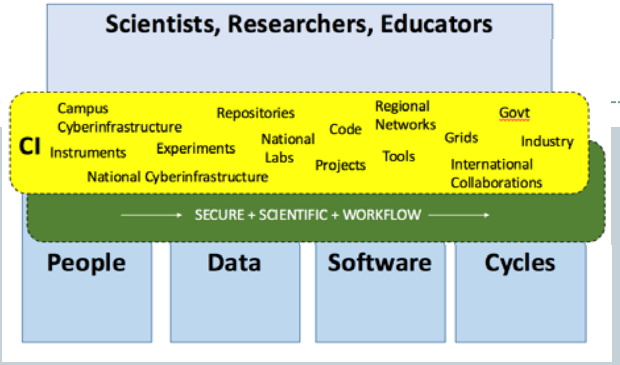


Figure 1. Cyberinfrastructure

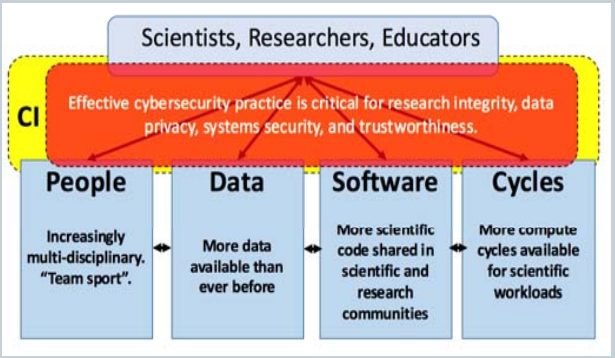


Figure 2. Effective Cybersecurity Practice

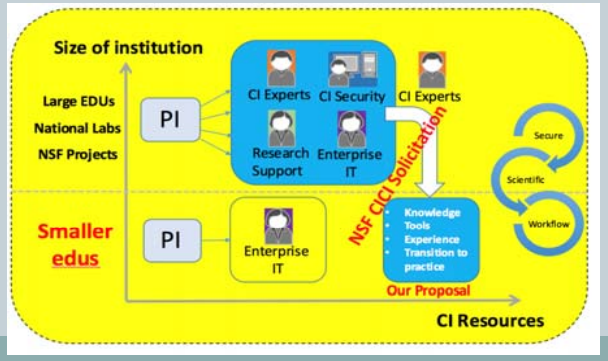


Figure 3. Project Landscape

SAC-PA Project Objectives

- Establish a regional collaboration and partnership framework, SAC-PA, within the state of Pennsylvania
  - Provide critical support to smaller academic institutions (schools and colleges, etc.), including resource constrained regional institutions that serve under-represented groups, females and high school teachers and students.
  - Enable concerted activities to promote the use of effective cybersecurity techniques and practice of security-assured cyberinfrastructure.

SAC-PA will provide a regional cybersecurity collaboration and partnership model that can be adopted by other regions, or be extended for national level collaborations.

Key Tasks

- Task 1: Develop and Deliver Regional Workshops for Cybersecurity
  - 3 workshops in Pittsburgh area
  - Identify challenges, exploring partnership/collaboration models
- Task 2: Collaboratively Develop Training/Awareness Materials
  - Develop and share cybersecurity training and awareness materials based on the needs and capabilities identified in the workshops
- Task 3: Establish Regional Partnerships and a Shared Repository of Cybersecurity Resources/Capabilities.
  - Establish SAC-PA framework
  - Creation & sharing of innovative solutions, best practices & know-how, expertise and resources

Initial Partners for Collaboration

- Keystone Initiative for Network Based Education and Research (KINBER)
  - Primary Contact: Wendy Huntoon
- University of Pittsburgh's CSSD's Information Security Team
  - Primary Contact: Sean Sweeney – CISO
- Open Science Grid
  - Primary Contact: Rob Gardner
- Center of Trustworthy Scientific Computing (CTSC)
  - Primary Contact: Von Welch, Jim Marsteller
- Internet2
  - Primary Contact: Florence Hudson, Paul Howell
- Energy Sciences Network (ESnet)
  - Primary Contact: Jason Zurawski
- Pittsburgh Supercomputing Center
  - Primary Contact: Jim Marsteller
- REN-ISAC
  - Primary Contact: Kim Milford
- National Cyber-Forensics & Training Alliance (NCFTA)
  - Primary Contact: Matt LaVigna
- Federal Bureau of Investigation (FBI, Pittsburgh)
  - Primary Contact: Christopher A. Geary
- University of Pittsburgh Medical Center (UPMC) – IT Security
  - Primary Contact: TBD
- SEI-CERT
  - Primary Contact: TBD

Evaluation

Metrics for Evaluation of Success

Workshops and Participation:

- Number of workshops (3 proposed)
- Number of attendees and breakdown of positions and responsibilities
- Number of attendees from smaller colleges, universities, and other similar organizations
- Number of student attendees
- Number of faculty participating in the workshops
- Diversity of attendee pool with regards to demographics
- Attendees map to locations in the region, state, multi-state
- List of partners providing content and participation in the workshops
- Number of campus research groups attending the workshops
- Web repository for collaboration site for presentations, papers, etc.
- Attendee survey to be used for subsequent workshop planning

Engagements and Outcomes:

- Number of follow-thru "engagements" resulting from attending the workshops. These could include professional engagements, formal engagements, or informal engagements
- Demonstrable examples of benefits reported/realized from attendees
- Number/Examples of tools, materials, information provided to the engaged communities
- Number/Examples of campus IT to campus scientist engagements resulting from the workshop activities
- Number/Examples of NSF projects including knowledge, tools, techniques learned in the workshops
- Number of talks/presentations on the workshops given by PI team at other events, conferences, meetings, etc.
- Feedback from collaborators and attendees on the training materials – with regards to deliver quality, suitability to attendees' cyber environment, etc.

Others

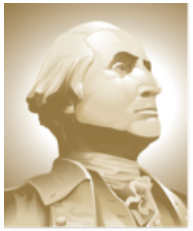
Project Timeline

August 2016	Anticipated Notice of award
October 2016	Engage collaborators. SME lists. Begin planning for first workshop
November 2016	Begin regular project team meetings. To be held monthly or as needed
December 2016	Conduct marketing, promotion, registration for first workshop
January 2017	Begin assembling training materials for first workshop
March 2017	**Conduct first workshop (SAC-PA 1)**
April 2017	Execute attendee surveys, and refine; Begin development of collaboration site
May 2017	Engage collaborators. SME lists. Begin planning for second workshop
July 2017	Conduct marketing promotion, registration for second workshop
August 2017	Begin assembling training materials for second workshop
October 2017	**Conduct second workshop (SAC-PA 2)**
November 2017	Execute attendee surveys and make adjustments based on results
December 2017	Engage collaborators. SME lists. Develop collaboration framework; Plan SAC-PA 3
December 2017	Bring collaboration site online and available to all participants
January 2018	Conduct marketing promotion, registration for third workshop
February 2018	Begin assembling training materials for third workshop
May 2018	**Conduct third Workshop (SAC-PA 3)**
June 2018	Follow up on activities and opportunities focused on regional collaborations – sustainability activities; Refinements, and finalize SAC-PA framework
August 2018	Complete final report and close of project

Thanks a lot!

Jaroslav Flidr

Substrate for Cybersecurity Education; a Platform for Training, Research, and Experimentation (SCEPTRE)



THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

CAAREN
Capital Area Advanced Research and Education Network | Powered by GW

CICI: Regional: Substrate for Cybersecurity Education; a Platform for Training, Research and Experimentation (SCEPTRE)

Jaroslav Flidr (PI), The George Washington University
Donald DuRousseau (Co-PI) , The George Washington University
Frederic Lemieux (Co-PI) , The George Washington University

SCEPTRE

Local Education, **Regional** Engagement, and **National** Environment

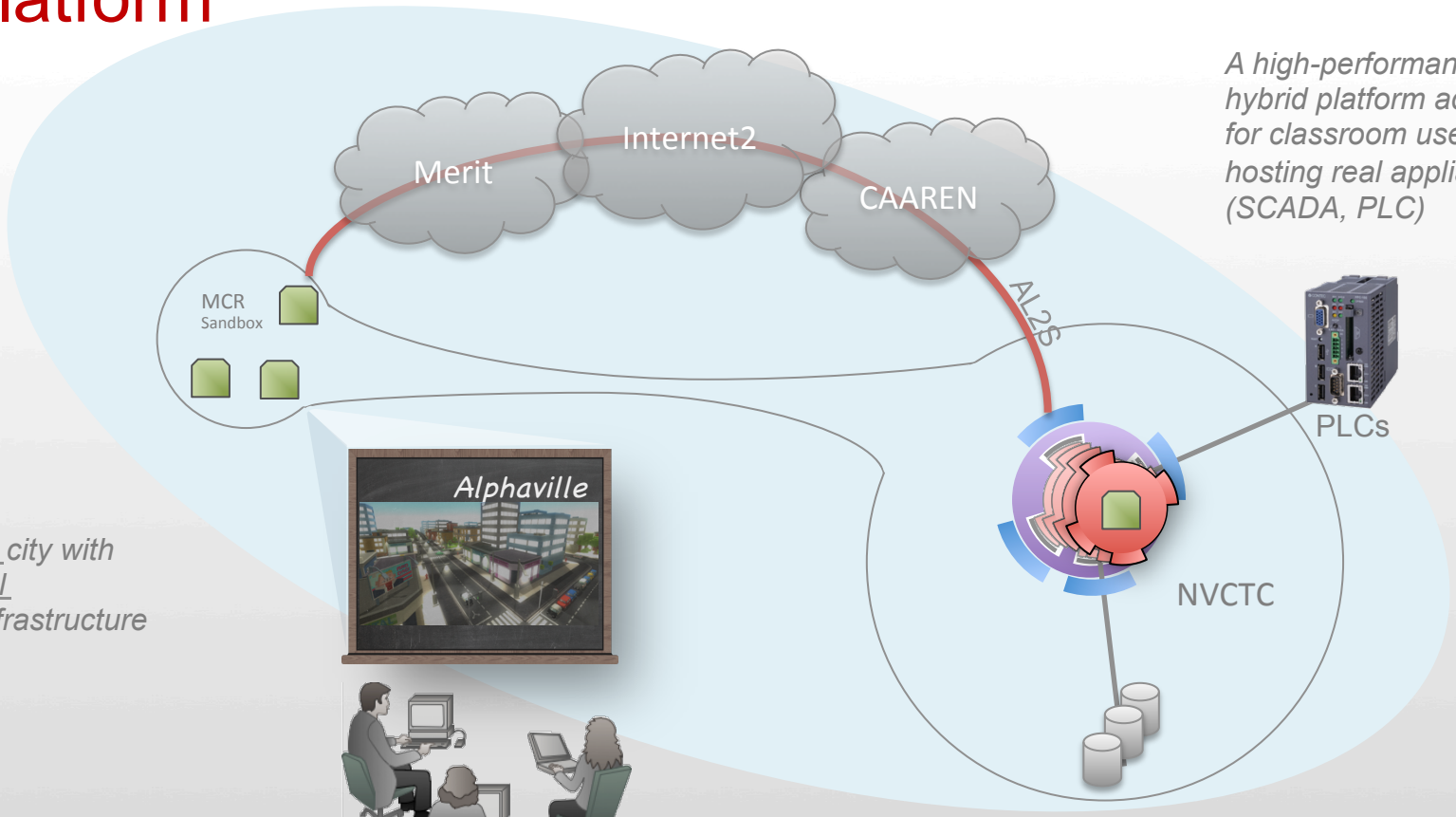
Substrate for Cybersecurity Education:

- Platform
  - Advance, expand and integrate the underlying technologies
- Training
  - Provide credit bearing courses, practicums, certifications
- Research
  - Investigate aspects of applied Cybersecurity,
  - Transition To Practice
- Experimentation
  - *e.g.* Industrial Control Systems (SCADA, PLCs)

Substrate

- Motivation
  - Workforce shortage: 100,000's
  - Lack of training resources: Cyber Ranges
  - Insufficiently satisfying career paths:
- Collaboration within Region (VA)
  - Academia: GW's College of Professional Studies
  - Industry: Northern Virginia technology sector
  - Government: Incubators, Accelerators and the Military
- Collaboration across Regions (VA – MI)
  - Merit: interconnectivity and impressive Cyber Range resources: Michigan Cyber Range (MCR)
  - CAAREN: interconnectivity and a high-performance, hybrid platform
  - GW: accredited education component

Platform



A high-performance, hybrid platform adapted for classroom use hosting real appliances (SCADA, PLC)

A virtual city with very real Cyberinfrastructure

Training

Reasonably safe and secure cyberinfrastructures cannot be built and operated without adequately trained human beings. This new workforce cannot be trained outside of realistic and adaptable environments and outside the context of existing policies and politics. Furthermore, due to the complexity of the problem, it is imperative that the trained individuals are well versed in a broad spectrum of related subjects, i.e. trained at an academic institution where they can find instruction in any area of study.

- Goals
  - Educate traditional and nontraditional students (students with associate degrees, students expanding their majors, undergraduates' transition to their postgraduate studies)
  - Make it an integral component of GW Cyber Academy
  - Encourage continuing education
  - Provide rewarding, life-long careers

Research and Experimentation

- heterogeneous environment of:
  - students
  - instructors
  - researchers
  - engineers
  - multiple organizations
  - concepts
  - devices
- facilitates experimentation with and research of:
  - policies
  - implications
  - techniques
  - technologies
  - behavioral patterns

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

CAAREN
Capital Area Advanced Research and Education Network | Powered by GW

Jill Gemmill

SouthEast SciEntific Cybersecurity for University REsearch (SouthEast SECURE)

CICI Regional: SouthEast SciEntific Cybersecurity for University Research (SouthEast SECURE)

- **Clemson University:** Jill Gemmill
- **Auburn University:** Tony Skjellum
- **University of Alabama at Huntsville**: Sara Graves
- **Voorhees College:** Barbara Nimmons
- **Jackson State University:** Richard Alo





Target Audience & Goal

- **Target Audience** -- NSF Funded Investigators in the SouthEastern US
- **Goal** – provide education, training, and select cybersecurity services to NSF-funded researchers across the Southeast.

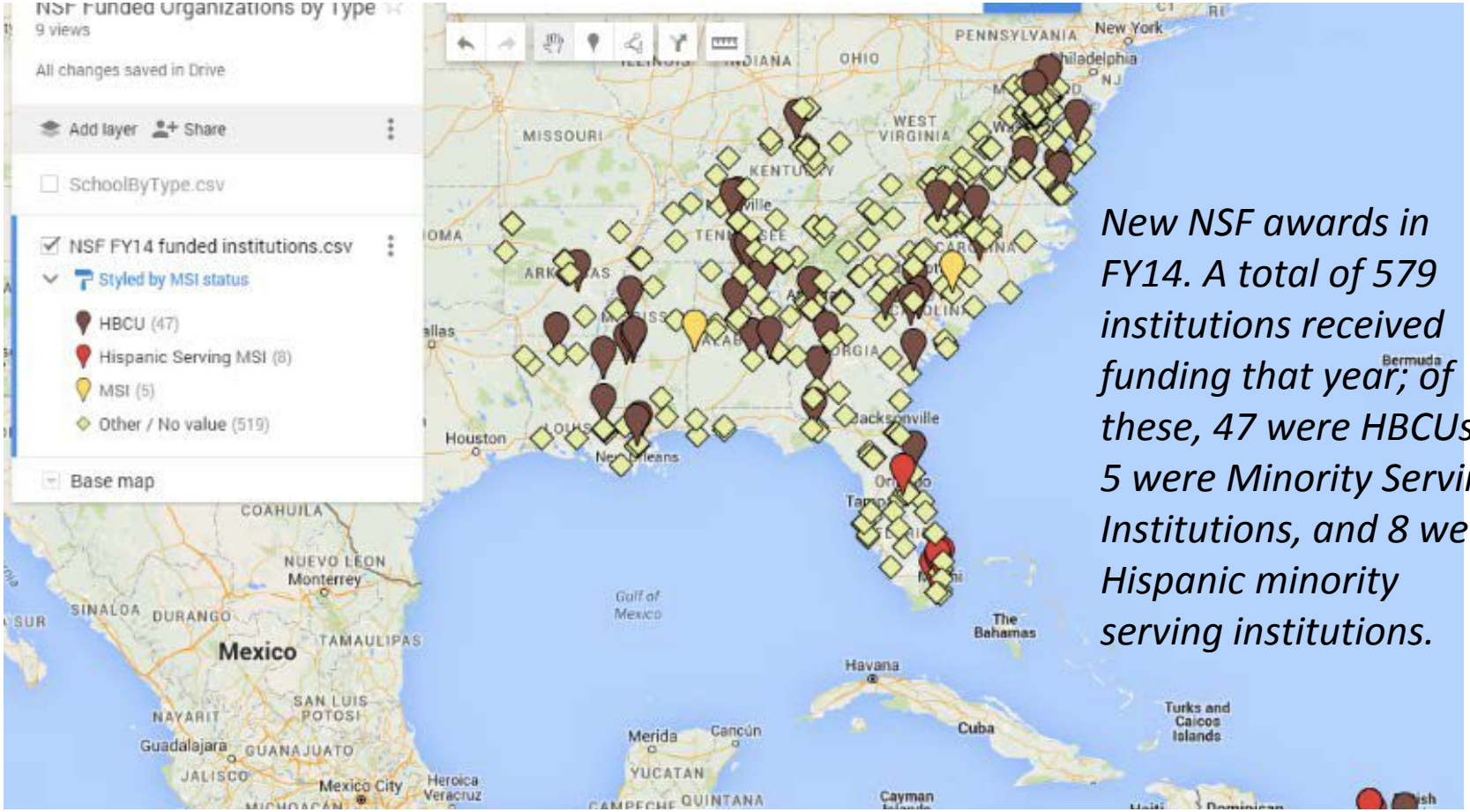
To hope to get the attention of busy faculty, a cybersecurity service must be perceived as

1. **USEFUL**
2. **Trustworthy**
3. **Concise**
4. **Under PI's control**

Desired Outcomes

- PIs should:
  - Understand their role & responsibilities in the cyber ecosystem
  - Have an inventory & plan for protecting their assets (data, systems, instruments)
  - Know what resources are available (locally, regionally, nationally)
- Campus IT / Administration should:
  - Understand cybersecurity needs of investigators
  - Know where to get help with campus network/wireless design for security

Some features of the SouthEast



New NSF awards in FY14. A total of 579 institutions received funding that year; of these, 47 were HBCUs, 5 were Minority Serving Institutions, and 8 were Hispanic minority serving institutions.

The Program

1. **Survey** NSF funded investigators in the SouthEast to learn their current level of knowledge, concerns & interests
   - Use our 5 own institutions for Phase 0
   - Organize follow-up and training w. our 5 campuses
   - Identify FAQs
   - Repeat for SouthEastern region
2. **Concrete and practical assistance** in how to do right-sized risk analysis/mitigation
   - Downsize great CTSC materials
   - Use words familiar to domain scientists

3. Provide a **ToolKit** to test and validate local cybersecurity
   - Leverage DoE cybersecurity pipeline program at HBCUs
   - Student-built devices
   - Auburn measures of university web site SSL/TLS security & patch speed over time
4. **Facilitate communication** between research faculty and university IT/Data Security staff.
5. Create short, informative A/V materials
6. **Build communities of people** with common interests in cybersecurity and in helping others; build these connections between regions and with national centers and programs

Metrics

1. Numbers of faculty, students and staff reached & trained
2. Web site vulnerability & time to patch
3. Voluntary reporting from ToolKit scans
4. Number of follow up contacts
5. Compare final survey to initial survey results

How to reach people?

COMMUNICATION CONDUITS

- **ACI-REF**
- **CISO/CIO**
- **SURA**
- **EARTHCUBE**
- **Campus leaders**
- **Direct Survey**
- **EPSCoR**
- **SE EDUCAUSE**
- **Higher Education Security RoundTable**

WHAT?

- **Detection Tool Kit**
- **>=5 minute videos**
- **Survey**
- **Follow up Conversations**
- **Workflow Templates (GEO & BIO focus)**

POTENTIAL SERVICES

- **Consulting/advice**
- **Point to right resources**
- **Training in open-source tools**
- **On-line office hours**
- **Share best practices**

Help Us !

-- Suggest people we can help

-- Offer us material we can use

-- Suggest ways to make the program bigger, better, broader

-- Partner with us on extending

Thank You!

Questions?

Please take our survey.

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 January 23rd at 11am Eastern

Topic: Open Science Cyber Risk Profile

Speakers: Von Welch and Sean Peisert

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.

CTSC

CTSC

CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE

The NSF Cybersecurity Center of Excellence

Thank You

trustedci.org

@TrustedCI

We thank the National Science Foundation (grant 1547272) for supporting our work.