A HISTORICAL PERSPECTIVE ON ADDRESSING CYBER-SECURITY AT NSF SUPPORTED COMMUNITIES

Clifford A. Jacobs

(NSF Retired)

Clifford A. Jacobs Consulting, LLC

CAVEAT AUDITOR

The opinions and recollections expressed in this talk
are those of
the speaker, not the National Science Foundation

TOPICAL OUTLINE

- Cybersecurity in Context
- Focal Points for NSF
- Implementations
- A work in progress

CYBERSECURITY IN CONTEXT

Our National Agenda and NSF's role with its awardees

“

CYBERSECURITY IS NOW A MAJOR NATIONAL SECURITY PROBLEM FOR THE UNITED STATES.

”

- Securing Cyberspace for the 44th Presidency:
A Report of the Center for Strategic and International Studies
Washington, DC - December 2008

The statement remains as relevant today as it was seven years ago

“

…CYBER THREAT IS ONE OF THE MOST SERIOUS ECONOMIC AND NATIONAL SECURITY CHALLENGES WE FACE AS A NATION AND … AMERICA'S ECONOMIC PROSPERITY IN THE 21ST CENTURY WILL DEPEND ON CYBERSECURITY.

”

- President Barack Obama

Washington, DC - May 29, 2009

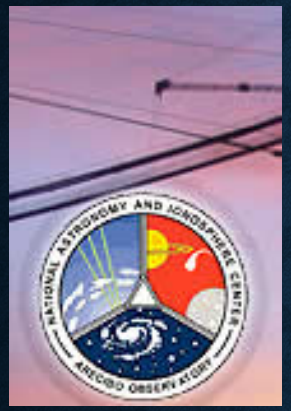
NSF must exercise good stewardship of the US scientific enterprises under its purview

“TODAY’S CYBERSPACE—THE POWERFUL, VIRTUAL ENVIRONMENT ENABLED BY DIGITAL INFRASTRUCTURE—PROVIDES A BRIGHT LANDSCAPE FOR COMMERCE, SCIENCE, EDUCATION, COMMUNICATION, AN OPEN AND EFFICIENT GOVERNMENT, AND MUCH MORE. IT ALSO HARBORS THREATS TO SECURITY AND PRIVACY THAT CAN LIMIT ITS USES AND POTENTIAL.”

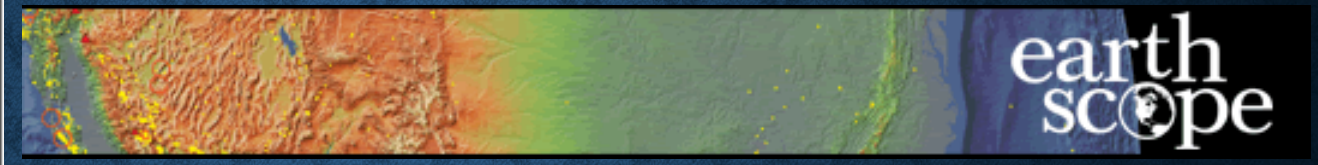
John P. Holdren
Assistant to the President for Science and Technology Director,
Office of Science and Technology Policy

From cover letter convenying the National Science and Technology Council report
TRUSTWORTHY CYBERSPACE: STRATEGIC PLAN FOR THE FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAM
December 2011

CYBERSECURITY IN AN NSF LARGE FACILITY



Expanded Very Large Array



LIGO

NCAR

XSEDE
Extreme Science and Engineering Discovery Environment

GEMINI OBSERVATORY

TeraGrid

NEES

Open Science Science Grid

IODP
INTEGRATED OCEAN DRILLING PROGRAM

WATERS NETWORK

NRAO

NNIN

NCSA

University-National Oceanographic Laboratory System

neon
NATIONAL ECOLOGICAL OBSERVATORY NETWORK

BLUE WATERS
SUSTAINED PETASCALE COMPUTING

incorporated research institutions for seismology
IRIS

FOCAL POINTS FOR NSF

How should NSF respond to cyber-security concerns at the large facilities supported by the agency?

THREE AREAS OF ACTION

- **Responsibility**
  - Define responsibilities of NSF and Awardee
- **Communication**
  - Facilitate dialog within NSF and among stakeholders
  - Articulate NSF's expectations
- **Demonstration**
  - Proactively exhibit that the agency takes cyber-security seriously

ESTABLISH AN NSF INTERNAL WORKING GROUP (FACSEC)

An informal group of program officers and administrators with responsibilities for large facilitates

CONTEXT OF FACSEC

- **History**: established about 10 year ago
- **Impetus**: Originally formed as an ad hoc committee in 2003-2004 after the "Stakkato" incident affected many facilities including the TeraGrid, NCAR, other NSF supercomputers, and DoE, DoD and other facilities
- **Stewardship**: Proactively demonstrates NSF's awareness of, and attention to, cybersecurity issues large research facilities face
- **Organization**: Originally was subcommittee of the Security and Privacy Working Group (which no longer meets) and now is convened under the auspicious of Division of Advanced Cyberinfrastructure (ACI)

FACSEC'S GUIDING PRINCIPLES AND GOALS

- **Tenet:** the awardee is responsible for establishing and maintaining good cybersecurity practices for NSF awards
- **Goal:** For large facilities projects using cyberinfrastructure, encourage cyber-security best practices be employed in all cyber-components of facility
- **Activities:**
  - Facilitate communication about cyber-security within the large facility research community
  - Inform large facilities program officers for about cyber-security issues and highlight challenges and opportunities experienced by the community and coordinate outreach efforts
  - Keep NSF management informed about the every-changing security landscape
  - Demonstrate that NSF is actively addressing security concerns with its

MEMBERSHIP TODAY

- Chaired by Anita Nikolich (Division of Advanced Cyberinfrastructure)
- Representation drawn from
  - Directorates and POs with large facilities, operating or under construction
  - The Division of Acquisition and Cooperative Support and Large Facilities Office
  - Office of General Counsel (when appropriate)

FACILITATED BY FACSEC

- **Communication**: Enabled communication after TeraGrid (Stakkato) incident
  - Inside NSF
  - With the community
  - Facilitated communication within the community
  - Offered guidance on "Best Practices in Cybersecurity that Might Be Useful for NSF's Large Facilities"
- **Responsibilities**: Developed language that is now included in the Special Terms and Conditions of the Cooperative Agreements for FFRDCs and Large Facilities
- **Demonstration**: Supported Cybersecurity Summit Meetings
  - Evolving topics, maturing over time
  - Building communication and self-sufficiency in the community

SUMMIT MEETING

- Purpose:
  - Engage the community in dialog about cyber-security
  - Inform NSF about the opportunities and challenges in maintaining a secure research environment
  - Provide training
- Summit Meetings --- 8 to date
  - 2004 – 2009
  - 2013 – 2015
- Tutorials added as part of meeting venue

NSF COOPERATIVE AGREEMENTS INFORMATION SECURITY REQUIREMENT

- Incorporated in NSF's Supplemental Financial and Administrative Terms and Conditions (next slide)

- Purpose is to help ensure that NSF large facilities and FFRDCs have policies, procedures and practices to protect research and education activities in support of the award
  - Reference: See CA-FATC LF Article 52 or CA-FATC FFRDC Article 55
- Influenced by recommendations from awardees at previous NSF-sponsored Cybersecurity Summits

INFORMATION SECURITY RESPONSIBILITIES AS LISTED IN THE COOPERATIVE AGREEMENT

- **Premise**: The facility itself is best able to assess cybersecurity appropriate for its operations
- **Responsibility**: Security for all IT systems is the Awardee's responsibility.
  - Includes equipment, data and information
  - All subawardees, subcontractors, researchers and others with access to the awardee's systems and facilities shall have appropriate security measures in place.
- **Reporting**: Awardee is required to provide a summary of its IT Security program, including:
  - Roles and responsibilities, risk assessment, technical safeguards, administrative safeguards; physical safeguards; policies and procedures; awareness and training; notification procedures.
  - Evaluation criteria employed to assess the success of the program
- **Sharing**: Awardee will participate in ongoing dialog with NSF and others to promote awareness and sharing of best practices.

OTHER SUPPORTING ACTIVITIES
(IN ADDITION TO SUMMIT MEETINGS)

- **Technical Help**:
  - Center for Trustworthy Scientific Cyberinfrastructure
    - To improve the cybersecurity of NSF science and engineering projects, while allowing those projects to focus on their science endeavors
    - A technical/social experiment
- **Campus Level**:
  - Campus Cyberinfrastructure - Data, Networking, and Innovation Program (CC*DNI) (NSF 15-534)
  - Review criteria include *"how resource access control, federated identity management, and other cybersecurity related issues and community best practices are addressed"*

A WORK IN PROGRESS
(EXAMPLE QUESTIONS)

- **Within NSF (FACSEC)**
  - How do we convey the message that cybersecurity is not an entity unto itself but integral to complex enterprises?
  - How best to evaluate summary cyber-security plans submitted by facilities
  - How best to keep abreast of the changing security landscape: policies, procedures and best practices?
- **From the Community**
  - What is a cyber-security plan and how do you develop one?
  - Why don't you just tell us what to do?
  - Under what circumstances should be notify you of security problems at the facility?
  - What part of the science do you want us to cut so we have develop and implement cyber-security measures?

QUESTIONS AND/OR COMMENTS