## Snyder, Amanda

**From:** ACOR-II Committee <ACOR-II@lists.psu.edu> on behalf of Rodgers, Jodi <jer30@psu.edu>
**Sent:** Thursday, December 22, 2016 11:13 AM
**To:** acor-ii
**Subject:** Limited Submission - Announcing Cybersecurity Innovation for Cyberinfrastructure (CICI) - Due 1/18/2017

We are pleased to announce the launch of the Cybersecurity Innovation for Cyberinfrastructure (CICI) competition. Click on the link below to view more information. Thank you!

- **Internal Submission Deadline:** Wednesday, January 18, 2017
- **Funding Organization's Deadline:** Wednesday, March 1, 2017
- **Award Cycle:** 2016-2017
- **Discipline/Subject Area:** Cybersecurity
- **Funding Available:** 1,000,000.00
- **Description:**

  Program Title: Cybersecurity Innovation for Cyberinfrastructure (CICI)

  Synopsis of Program: Advancements in data-driven scientific research depend on trustworthy and reliable cyberinfrastructure. Researchers rely on a variety of networked technologies and software tools to achieve their scientific goals. These may include local or remote instruments, wireless sensors, software programs, operating systems, database servers, high-performance computing, large-scale storage, and other critical infrastructure connected by high-speed networking. This complex, distributed, interconnected global cyberinfrastructure ecosystem presents unique cybersecurity challenges. NSF-funded scientific instruments, sensors and equipment are specialized, highly-visible assets that present attractive targets for both unintentional errors and malicious activity; untrustworthy software or a loss of integrity of the data collected by a scientific instrument may mean corrupt, skewed or incomplete results. Furthermore, often data-driven research, e.g., in the medical field or in the social sciences, requires access to private information, and exposure of such data may cause financial, reputational and/or other damage.

Therefore, an increasing area of focus for NSF is the development and deployment of hardware and software technologies and techniques to protect research cyberinfrastructure across every stage of the scientific workflow.

CICI comprises two Program Areas outlined below:

1. Resilient Security Architecture for Research Cyberinfrastructure

Research Cyberinfrastructure environments have become increasingly complex as campuses and other research institutions adapt their existing research cyberinfrastructure to include a range of new technologies and modalities including private and commercially-available cloud computing resources, new forms of shared data and computing infrastructure, identity management which spans institutions, and distributed shared computing, storage and network resources. As a result, it has become difficult to monitor and control the end-to-end scientific environment. Deliberate or unintentional incidents that affect systems are often difficult to detect. Identifying unauthorized users, system anomalies and the loss or corruption of data remain formidable challenges.

Collaborative scientific experiments are complex and may include participants from multiple institutions, national labs or organizations physically distributed across campuses, sites or countries. Legitimate users often arrive at scientific experiments and collaborations from a multitude of institutions and with complex access relationships. Complex technical relationships may exist between experiments, This program area seeks to address this complexity by encouraging novel and trustworthy architectural and design approaches, models and frameworks for the creation of a holistic, integrated security environment that spans the entire scientific CI ecosystem. Projects must demonstrate strong security architecture and systems security engineering generalizable across a diverse scientific workflow. Technical solutions must be driven by at least one scientific community, facility or project.

NSF recognizes the inherent diversity that exists in an organization's operational security practices and policies as well as the range of underlying security architectures. However, understanding and mitigating threats to the environment based on empirical data is critical to enhancing the security and resilience of scientific cyberinfrastructure. Approaches that address the collection of quantitative security-related metrics are encouraged, as these metrics can be used to define a risk

management posture for the open science being conducted by an institution, experiment or collaboration.

Proposals are encouraged to include a technical proof-of-concept implementation or operational prototype, including the participation of end users, for the proposed approach. Collaborations with other government agencies or industry partners are welcome.

Some areas of interest include, but are not limited to:

New approaches that demonstrate substantive improvements to secure and protect operational cyberinfrastructure. Key infrastructure services include, but are not limited to, naming/Domain Name System (DNS), secure routing, and network time synchronization. For all these areas, security standards such as Domain Name System Security (DNSSEC) and Resource Public Key Infrastructure (RPKI) are available, but few organizations have chosen to adopt and implement these in their environments. As a result, communication may be misdirected to the wrong data location, a man-in-the-middle attack may modify data in transit, or key data aspects such as timestamps may be invalid.

Techniques and tools to detect behavioral anomalies across cyberinfrastructure systems, including detecting the tools and techniques of an attack and methods to mitigate security threats.

More robust, efficient and secure transfer of data while retaining the integrity of the data sets. With the growing amount of remote instruments and the increasing amount of data being collected from multiple, often remote, wireless and mobile sensors, science is increasingly distributed and virtual. Solutions such as the introduction of blockchain technology are needed to ensure the integrity and confidentiality of data as it traverses multiple environments such as mobile, cloud, campus, and Internet networks.

Security metrics, including the implementation of data analytics and trend analysis methodologies and tools in order to both provide incident tracking and measurement of the effectiveness and impact of security tools, processes and architectures. This can include the creation of meaningful visualizations or metrics that are tightly integrated with other information technology (IT) functions. Quantitative and actionable security metrics are critical to performing consistent long-term trending of the cyberinfrastructure and making iterative improvements to the security posture.

2. Cybersecurity Enhancement

Cyberinfrastructure projects often proceed without considerations of the security, integrity and privacy implications of the system or effort. This program area addresses the critical need to focus attention and resources on the security attributes of scientific cyberinfrastructure. Systems and network discovery is a precursor to understanding the attack surface and lays the foundation for development and implementation of a strong security architecture.

Proposals submitted to this area should address scientific research and education needs for secure connectivity on campus and/or externally. Proposals may address the need to assess and redesign their campus security architecture to better support scientific and research data flows.

Some areas of interest include, but are not limited to:

Activities such as security assessments and security design reviews that lead to a better understanding of the protocols utilized by the science workflows within a campus or site, between campuses and/or sites, within a region and between regional and national resources. For example, in preparation for re-architecting a network to support large science data flows by designing and building a Science DMZ, an understanding of the underlying communication protocols is essential. This understanding can serve to define a risk management posture for the scientific collaboration. It also provides an understanding of the state of the environment prior to and after deployment of a Science DMZ or secure architecture or system. It can also lead to the quicker identification of a compromised host or system. Such activities should lead to a baseline of what is accepted as "normal" traffic traversing the cyberinfrastructure, so that anomalies can be more easily identified by security monitoring systems. Activities may include remediation efforts to ensure the cyberinfrastructure is more secure.

Novel means by which to operationally integrate and deploy commercial and open source security tools such as protocol analyzers, intrusion detection systems, event monitoring tools, logging devices and firewalls to protect all aspects of the scientific workflow.

Efforts to add open source federated identity management to existing cyberinfrastructure-related applications in order to streamline user access to resources hosted within an organization or by another federation partner.

View competition

InfoReady Review is a convenient online workspace that helps Administrators, Applicants, and Reviewers streamline their submission, routing, and review processes. No more paper trails, email threads, or missing data. Now you can get your work done faster, smarter, and better than ever before.