This document has been archived and replaced by NSF 19-514.

Cybersecurity Innovation for Cyberinfrastructure (CICI)

PROGRAM SOLICITATION
NSF 18-547

REPLACES DOCUMENT(S):
NSF 17-528

National Science Foundation

Directorate for Computer & Information Science & Engineering
Office of Advanced Cyberinfrastructure

Full Proposal Deadline(s) (due by 5 p.m. submitter's local time):

June 04, 2018

IMPORTANT INFORMATION AND REVISION NOTES

This solicitation updates the Cybersecurity Innovation for Cyberinfrastructure (CICI) solicitation NSF 17-528. The CICI program continues to support the goal of a secure scientific workflow. The current solicitation:

- Adds two new program areas, Collaborative Security Response Center and Research Data Protection;
- Removes the Cybersecurity Enhancement Area; and
- Renames the Resilient Security Architecture for Research Cyberinfrastructure program area to Secure Scientific Cyberinfrastructure.

Any proposal submitted in response to this solicitation should be submitted in accordance with the revised *NSF Proposal & Award Policies & Procedures Guide* (PAPPG) (NSF 18-1), which is effective for proposals submitted, or due, on or after January 29, 2018.

SUMMARY OF PROGRAM REQUIREMENTS

General Information

Program Title:

Cybersecurity Innovation for Cyberinfrastructure (CICI)

Synopsis of Program:

The objective of the Cybersecurity Innovation for Cyberinfrastructure (CICI) program is to develop, deploy and integrate security solutions that benefit the scientific community by ensuring the integrity, resilience and reliability of the end-to-end scientific workflow. CICI seeks three categories of projects:

1. **Secure Scientific Cyberinfrastructure:** These awards seek to secure the scientific workflow 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;
2. **Collaborative Security Response Center**: This single award targets the development of a community resource to provide security monitoring, analysis, expertise, and resources Research & Education (R&E) cyberinfrastructure staff, regardless of physical location or organization; and
3. **Research Data Protection:** These awards provide solutions that both ensure the provenance of research data and reduce the complexity of protecting research data sets regardless of funding source.

Cognizant Program Officer(s):

Please note that the following information is current at the time of publishing. See program website for any updates to the points of contact.

- Kevin Thompson, Program Director, CISE/OAC, telephone: (703) 292-4220, email: kthompso@nsf.gov

Applicable Catalog of Federal Domestic Assistance (CFDA) Number(s):

- 47.070 --- Computer and Information Science and Engineering

Award Information

Anticipated Type of Award: Standard Grant or Continuing Grant or Cooperative Agreement

Estimated Number of Awards: 6 to 12

Anticipated Funding Amount: $10,000,000 to $12,000,000

Total funding for the CICI program is $10,000,000 to $12,000,000, subject to the availability of funds. Secure Scientific Cyberinfrastructure awards will be supported at up to $1,000,000 total per award for up to three years. Research Data Protection awards will be supported at up to $1,000,000 total per award for up to three years. A single Collaborative Security Response Center award will be supported at up to $5,000,000 for up to three years.

Eligibility Information

Who May Submit Proposals:

Proposals may only be submitted by the following:

- Institutions of Higher Education (IHEs) - Two- and four-year IHEs (including community colleges) accredited in, and having a campus located in the US, acting on behalf of their faculty members. Special Instructions for International Branch Campuses of US IHEs: If the proposal includes funding to be provided to an international branch campus of a US institution of higher education (including through use of subawards and consultant arrangements), the proposer must explain the benefit(s) to the project of performance at the international branch campus, and justify why the project activities cannot be performed at the US campus.
- Non-profit, non-academic organizations: Independent museums, observatories, research labs, professional societies and similar organizations in the U.S. associated with educational or research activities.

Who May Serve as PI:

There are no restrictions or limits.

Limit on Number of Proposals per Organization:

Organizations are limited to 2 CICI proposals. These eligibility constraints will be strictly enforced in order to treat everyone fairly and consistently. In the event that an organization exceeds this limit, proposals received within the limit will be accepted based on earliest date and time of proposal submission (i.e., the first two proposals received will be accepted and the remainder will be returned without review). No exceptions will be made.

Limit on Number of Proposals per PI or Co-PI:

An individual can participate as PI, co-PI or senior personnel on no more than two CICI proposals. Note that any individual whose biographical sketch is provided as part of the proposal will be considered as Senior Personnel in the proposed activity, irrespective of whether that individual will receive financial support from the project.

Proposal Preparation and Submission Instructions

A. Proposal Preparation Instructions

- **Letters of Intent:** Not required
- **Preliminary Proposal Submission:** Not required
- **Full Proposals:**
  - Full Proposals submitted via FastLane: *NSF Proposal and Award Policies and Procedures Guide* (PAPPG) guidelines apply. The complete text of the PAPPG is available electronically on the NSF website at: https://www.nsf.gov/publications/pub_summ.jsp?ods_key=pappg.
  - Full Proposals submitted via Grants.gov: *NSF Grants.gov Application Guide: A Guide for the Preparation and Submission of NSF Applications via Grants.gov* guidelines apply (Note: The *NSF Grants.gov Application Guide* is available on the Grants.gov website and on the NSF website at: https://www.nsf.gov/publications/pub_summ.jsp?ods_key=grantsgovguide).

B. Budgetary Information

- **Cost Sharing Requirements:**

  Inclusion of voluntary committed cost sharing is prohibited.

- **Indirect Cost (F&A) Limitations:**

Not Applicable

- **Other Budgetary Limitations:**

  Not Applicable

C. Due Dates

- **Full Proposal Deadline(s)** (due by 5 p.m. submitter's local time):

  June 04, 2018

Proposal Review Information Criteria

Merit Review Criteria:

National Science Board approved criteria. Additional merit review considerations apply. Please see the full text of this solicitation for further information.

Award Administration Information

Award Conditions:

Standard NSF award conditions apply.

Reporting Requirements:

Standard NSF reporting requirements apply.

TABLE OF CONTENTS

I. INTRODUCTION

The integrity of the scientific workflow and associated data is essential to scientific credibility. Network-connected remote or local scientific instruments such as telescopes, microscopes, external data repositories, research computers, and sensing devices collect and analyze large amounts of raw information, yet remain vulnerable. The research environment may be much more complex, yet often receives less attention than business systems. Unprotected research cyberinfrastructure (CI) and scientific data may be valuable or subject to confidentiality requirements, and potentially vulnerable to theft or corruption, presenting an attractive target of opportunity for

attack and compromise. As national and international collaborations become commonplace and broader access to research data occurs, protection of systems, processes, data, software and the network from deliberate misuse is essential. This solicitation addresses the protection, integrity and reliability of research processes and the resulting information.

II. PROGRAM DESCRIPTION

Science is increasingly being conducted by distributed international collaborations and virtual organizations using shared cyberinfrastructure resources. Given the challenges with deploying and operating cyberinfrastructure at a large scale, security and resilience for the environment are both paramount. The objective of the Cybersecurity Innovation for Cyberinfrastructure (CICI) program is to develop, deploy and integrate security solutions that benefit the scientific community by ensuring the integrity, resilience and reliability of the end-to-end scientific workflow. This solicitation seeks unique ways to protect scientific instruments, resources, cyberinfrastructure and data that extend beyond building better perimeters and point solutions.

The scope of the scientific workflow encompasses instruments, mobile and traditional networks, processing software, analysis tools, computing and storage resources as well as information repositories and data archives. In order to produce accurate results, each data source must be identifiable and trustworthy. Systems must guarantee that data sets cannot be altered, which could potentially modify the analytic outcomes.

Funded activities under CICI should identify opportunities for community and student engagement as well as cybersecurity education and training. Proposals that demonstrate opportunities to engage undergraduate or graduate students directly in the deployment, operation, and advancement of the CICI-funded activities are welcome.

The CICI program is not the appropriate mechanism to provide support for fundamental cybersecurity or privacy research. Such projects would be better served as submissions to the Secure and Trustworthy Cyberspace (SaTC) program.

CICI comprises three Program Areas outlined below:

1. **Secure Scientific Cyberinfrastructure**

   Scientific cyberinfrastructure has become increasingly complex as campuses, research institutions and scientific facilities 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 spanning institutions and countries, 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.

   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 one or more scientific communities, facilities or projects.

   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 include 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. Setting up an isolated lab experiment is not considered an operational prototype. 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 scientific cyberinfrastructure;
   - New deployment of key secure networking infrastructure services in R&E environments such as secure routing (Border Gateway Protocol Security/Resource Public Key Infrastructure) and Domain Name System Security (DNSSEC);
   - Re-design of the campus or facility border security and current approaches such as the "Science DMZ" (see http://fasterdata.es.net/fasterdata/science-dmz/ for more information); Science DMZ's are rapidly scaling to accommodate increasing amounts of scientific data transfers and becoming more complex as Science DMZs are now stretching between sites and traversing multiple organizations; designs to improve the authentication and usability for the Science DMZ and the data transfer systems within it are encouraged; and
   - Techniques and tools that provide improved granularity in the correlation and analysis of behavioral anomalies across scientific cyberinfrastructure as well as improved detection of actionable security events. Security management systems and infrastructure monitoring tools, both proprietary and open source, provide a large and potentially overwhelming amount of information through which to sort. Tools that mine the data, detect, and identify the tools and techniques of an attack and lead to a greater understanding of what constitutes both normal and anomalous behavior are encouraged.

   Proposers are encouraged to consider how to measure effectiveness in project activities.

   A proposal in this area must demonstrate that the proposed architecture responds to the needs of the science and engineering

communities and serve to advance scientific discoveries, collaborations, and innovations. Proposers must document explicit partnerships or collaborations with one or more domain scientists, research groups, or information technology (IT) support organizations. Partnership documentation from personnel not included in the proposal as PI, co-PI, or senior personnel should be in the form of a letter of collaboration located in the Supplementary Documents section of the proposal.

Proposers are encouraged to explain the threat model upon which the proposed solution is predicated. For reference on a threat model for Open Science, please refer to the Open Science Cyber Risk Profile (OSCRP), co-authored by the NSF-funded Cybersecurity Center of Excellence and the Department of Energy's Energy Sciences Network (ESnet): http://trustedci.github.io/OSCRP/OSCRP.html

A sustainability plan describing how the proposed system will be supported beyond the project time period must be included.

In the Supplementary Documents section, a proposal responsive to this program area must include Systems Architecture diagram(s) of the proposed implementation or framework. Proposers should use the diagram(s) to document both the logical and physical architecture(s) of the proposed implementation and describe the system components and interrelationships.

Each proposal must also include as a Supplementary Document a Project Plan of up to 5 pages addressing the goals and milestones for development of the resulting system or framework.

Any software development under proposed activities must be made available under an open source license. Proposals must state which software license will be used for any released software, and why this license has been chosen.

2. **Collaborative Security Response Center**

Research cyberinfrastructure is often the unwitting target of malicious activity. For example, Distributed Denial of Service (DDoS) attacks can affect a single campus or group of campuses by interfering with normal network operations and disrupting connectivity to systems for extended periods of time. Scientific facilities have also been the victims of such attacks, in addition to infection by computer worms and malware. The Internet address space in R&E networks is constantly being scanned by potentially malicious actors; scanning can often be a precursor to more nefarious activities. As scientific collaborations traverse multiple campuses, infrastructures, networks, and systems, the various cyberinfrastructure elements are monitored by a myriad of groups using disparate frameworks, tools, and approaches with varying levels of cybersecurity expertise.

This program seeks to establish a collaborative approach towards improving the mechanisms for identifying, analyzing and disseminating critically important security information to R&E cyberinfrastructure staff, regardless of physical location or organization. Shared analytical information on common threats and trends also serves to apprise scientific researchers of serious security events or incidents that could impact their research and the trustworthiness of their data.

NSF recognizes the limited cybersecurity resources available at sites, individual campuses and institutions. Security personnel remain in high demand, and scientific facilities or projects often do not have dedicated security engineers. Scientific cyberinfrastructure also often presents unique design, implementation and configuration scenarios compared to enterprise scenarios. Since the R&E community bears a collective responsibility towards ensuring the security of scientific cyberinfrastructure, economies of scale can be achieved by leveraging common security solutions, resources, and analytical methods among cyberinfrastructure providers.

This program area seeks to build a Collaborative Security Response Center (CSRC) through a consortium of physical and/or virtual entities whose expertise and resources can be leveraged by the entire R&E community to improve the cybersecurity posture of scientific cyberinfrastructure and raise awareness of security threats facing the community.

The CSRC should comprise a collection of technology, techniques, people, and processes. Proposals in this area should define the exact scope of the CSRC, which can be physical or virtual, and describe the anticipated impact of the CSRC upon scientific discovery. Proposals in this area should also specifically describe the: approach to providing resources for support for the operational security of scientific cyberinfrastructure at local, regional, and national levels; participants' and organizational expertise in security; planned outreach and engagement activities, especially to under-resourced colleges, universities, and scientific collaborations; mechanisms for monitoring and detecting security incidents, trends, or data breaches, and the responses to such incidents; collaborations with national entities such as Internet2, ESnet, and Regional Optical Networks (RON), as well as interactions with virtual organizations such as the Open Science Grid (OSG), NSF Extreme Science and Engineering Discovery Environment (XSEDE), and other large scientific experiments and their institutional partners.

Critical to the success of the CSCR is its ability to access operational systems' data such as site data flows, telemetry, packet captures, systems logs (syslogs), and other types of information relevant to comprehensive security analyses. Given the inherent policy and technical obstacles involved in sharing such data, the CSCR is expected to demonstrate progress towards solving these challenges in a privacy-preserving manner. Proposers should describe the data protection plan for the data that the CSCR obtains.

The CSRC's activities may include, but are not limited to:

- Assessing and analyzing emerging security threats and trends that affect the R&E cyberinfrastructure environment and disseminating this information to the community;
- Coordinating with local, national, and International complementary resources and centers such as the Research & Education Networking Information Sharing & Analysis Center (REN-ISAC), Community Emergency Response Team (CERT), NSF Cybersecurity Center of Excellence (CCoE), and Global R&E Network Operations Centers (GRNOC), and aggregating and analyzing threat intelligence information from these and other public and private sources to understand the imminent and long term security threats to the scientific and R&E environments;
- Providing real-time threat detection, incident response, and situational analysis specific to the R&E environment;
- Detecting behavioral anomalies across systems including the detection of the tools and techniques of an attack;
- Selectively investigating security incidents that affect multiple sites or campuses;
- Providing analysis and objective recommendations on tools, technologies, and integrated systems related to cybersecurity operations;

Producing security metrics at an aggregated level across campuses, regions, scientific collaborations, or other logical groupings; and
- Sharing and aggregating syslogs and monitoring data in order to quickly find compromised hosts and identify security trends throughout the R&E community; solving the tools and policy aspects of this task will be critical to its success.

Cybersecurity remains a socio-technical challenge, with personnel forming a crucial part of a comprehensive security approach. A trained human eye, for example, may pick up patterns a machine cannot necessarily recognize; human analysts can contextualize alerts in a broader scheme. A successful approach includes a combination of both technical and human skills to assess alerts and information from multiple, disparate systems and sources and provide thoughtful analysis. Proposers are encouraged to think about the human aspect and also incorporate training and educational activities in order to grow the current and future community of cybersecurity experts.

Proposers are encouraged to consider how to measure effectiveness in project activities.

Proposals should demonstrate the team's understanding of the threats to open science and research cyberinfrastructure. The focus should be less on the development of new tools or the purchase of vendor solutions than on the means by which open source, widely deployed community tools and techniques such as existing honeypots, Security Incident and Event Management (SIEM) systems, the Bro Intrusion Detection System, and Real Time Black Hole Routing can be leveraged at scale and across entities. Collaborations with industry are encouraged in order to facilitate novel approaches. Solutions should be easily leveraged by the community at the conclusion of the grant.

Any software development under proposed activities must be made available under an open source license. Proposals must state which software license will be used for any released software, and why this license has been chosen.

A proposal in this area must demonstrate that proposed solutions and services respond to the cybersecurity needs of the science and engineering community and serves to advance scientific discoveries, collaborations, and innovations. NSF requires a team-based, distributed approach to the CSRC and therefore requires collaborative proposals. All proposals in this area must document explicit partnerships with other institutions, scientific collaborations, facilities, entities, or industrial partners. All proposals in this area must also document explicit partnerships or collaborations with the IT support organization, including security leaders such as the Chief Information Security Officer (CISO), Chief Privacy Officer (CPO), or similar functional positions within an institution, collaboration, or facility. Letters of collaboration with research cyberinfrastructure leadership are encouraged. Partnership documentation from personnel not included in a proposal as PI, co-PI, or senior personnel should be in the form of a letter of collaboration located in the Supplementary Documents section of the proposal.

An initial community of adopters of the CSRC's services for year 1 must be detailed in a Supplementary Document.

Proposals must include as a Supplementary Document a Project Plan of up to 10 pages addressing the goals and milestones for activities in this area.

3. **Research Data Protection**

Science has become highly interdisciplinary, and the most ground-breaking discoveries occur when researchers cross traditional boundaries of individual scientific domains. Such breakthroughs are enabled by the ability to conduct analyses across combinations of open and protected data sets that may have been funded by numerous sources with different constraints and policies on data. Maliciously or unintentionally altered data impact scientific research and can affect conclusions. Ultimately, the data upon which scientific discovery rests must be trustworthy and retain its veracity at every point in the scientific workflow regardless of origin.

In order to enhance scientific analysis, interdisciplinary research, and cross-agency collaboration on science that is conducted on data sets that result from multiple funding sources, this program area seeks to fund solutions that reduce the complexity of protecting research data sets.

A major challenge for these scientific environments in hosting and protecting data remains navigating and translating into tangible IT implementations the variety of laws, controls, and best practices that are either required by, or suggested through, common frameworks by funding agencies. As an example, the NIST Framework for Improving Critical Infrastructure Cybersecurity and NIST Special Publication 800-53 delineate security controls associated with the requirements in the Federal Information Processing Standard (FIPS).

Activities in this area may include, but are not limited to:

- Technical proof-of-concept implementations demonstrating assurance that unauthorized parties are prevented from modifying data at any point in the scientific workflow in order to ensure integrity and/or provenance for scientific data;
- Frameworks that align the security policies of institutions, facilities, and scientific collaborations with the grant-required controls and requirements, and that combine both into implementable cyberinfrastructure tools; tools should be developed for use across multiple institutions and collaborations while taking into account combinations of data on site locally, in the cloud, and accessed across a network and virtualized resources; and
- Methods of providing outreach and assistance to the scientific communities on topics in this area.

Proposers should first apply the Open Science Risk Profile (OSRP) to assess the threat and risk to the environment and then interpret the security and compliance requirements that must be applied.

All proposals in this area must document explicit partnerships or collaborations with one or more domain scientists, research groups, or IT support organizations. Partnership documentation from personnel not included in the proposal as PI, co-PI, or senior personnel should be in the form of a letter of collaboration located in the Supplementary Documents section of the proposal.

Any software development under proposed activities must be made available under an open source license. Proposals must state which software license will be used for any released software, and why this license has been chosen.

A Systems Architecture Diagram(s) and a Project Plan of up to 5 pages in length must be included as Supplementary

Documents.

III. AWARD INFORMATION

Anticipated Type of Award: Continuing Grant or Cooperative Agreement or Standard Grant

Estimated Number of Awards: 6-12

Anticipated Funding Amount: $10,000,000 - $12,000,000

Total funding for the CICI program is subject to the availability of funds. Secure Scientific Cyberinfrastructure awards will be supported at up to $1,000,000 total per award for up to three years. Research Data Protection awards will be supported at up to $1,000,000 total per award for up to three years. A single Collaborative Security Response Center award will be supported at up to $5,000,000 for up to three years.

Estimated program budget, number of awards and average award size/duration are subject to the availability of funds.

IV. ELIGIBILITY INFORMATION

Who May Submit Proposals:

Proposals may only be submitted by the following:

- Institutions of Higher Education (IHEs) - Two- and four-year IHEs (including community colleges) accredited in, and having a campus located in the US, acting on behalf of their faculty members. Special Instructions for International Branch Campuses of US IHEs: If the proposal includes funding to be provided to an international branch campus of a US institution of higher education (including through use of subawards and consultant arrangements), the proposer must explain the benefit(s) to the project of performance at the international branch campus, and justify why the project activities cannot be performed at the US campus.
- Non-profit, non-academic organizations: Independent museums, observatories, research labs, professional societies and similar organizations in the U.S. associated with educational or research activities.

Who May Serve as PI:

There are no restrictions or limits.

Limit on Number of Proposals per Organization:

Organizations are limited to 2 CICI proposals. These eligibility constraints will be strictly enforced in order to treat everyone fairly and consistently. In the event that an organization exceeds this limit, proposals received within the limit will be accepted based on earliest date and time of proposal submission (i.e., the first two proposals received will be accepted and the remainder will be returned without review). No exceptions will be made.

Limit on Number of Proposals per PI or Co-PI:

An individual can participate as PI, co-PI or senior personnel on no more than two CICI proposals. Note that any individual whose biographical sketch is provided as part of the proposal will be considered as Senior Personnel in the proposed activity, irrespective of whether that individual will receive financial support from the project.

Additional Eligibility Info:

Collaborative proposals submitted as simultaneous submissions of proposals from different organizations, with each organization requesting a separate award, are not allowed. Instead, proposals involving multiple institutions must be submitted as a single proposal, in which a single award is being requested (with subawards administered by the lead organization).

V. PROPOSAL PREPARATION AND SUBMISSION INSTRUCTIONS

A. Proposal Preparation Instructions

Full Proposal Preparation Instructions: Proposers may opt to submit proposals in response to this Program Solicitation via Grants.gov or via the NSF FastLane system.

- Full proposals submitted via FastLane: Proposals submitted in response to this program solicitation should be prepared and submitted in accordance with the general guidelines contained in the *NSF Proposal & Award Policies & Procedures Guide*

(PAPPG). The complete text of the PAPPG is available electronically on the NSF website at: https://www.nsf.gov/publications/pub_summ.jsp?ods_key=pappg. Paper copies of the PAPPG may be obtained from the NSF Publications Clearinghouse, telephone (703) 292-7827 or by e-mail from nsfpubs@nsf.gov. Proposers are reminded to identify this program solicitation number in the program solicitation block on the NSF Cover Sheet For Proposal to the National Science Foundation. Compliance with this requirement is critical to determining the relevant proposal processing guidelines. Failure to submit this information may delay processing.

- Full proposals submitted via Grants.gov: Proposals submitted in response to this program solicitation via Grants.gov should be prepared and submitted in accordance with the *NSF Grants.gov Application Guide: A Guide for the Preparation and Submission of NSF Applications via Grants.gov*. The complete text of the *NSF Grants.gov Application Guide* is available on the Grants.gov website and on the NSF website at: (https://www.nsf.gov/publications/pub_summ.jsp?ods_key=grantsgovguide). To obtain copies of the Application Guide and Application Forms Package, click on the Apply tab on the Grants.gov site, then click on the Apply Step 1: Download a Grant Application Package and Application Instructions link and enter the funding opportunity number, (the program solicitation number without the NSF prefix) and press the Download Package button. Paper copies of the Grants.gov Application Guide also may be obtained from the NSF Publications Clearinghouse, telephone (703) 292-7827 or by e-mail from nsfpubs@nsf.gov.

See PAPPG Chapter II.C.2 for guidance on the required sections of a full research proposal submitted to NSF. Please note that the proposal preparation instructions provided in this program solicitation may deviate from the PAPPG instructions.

The following information supplements the guidelines and requirements in the NSF PAPPG and NSF Grants.gov Application Guide:

Proposal Titles: Proposal titles should begin with **CICI** followed by a colon, then the program area acronym followed by a colon, then the title of the project. Select the program area acronym below:

- Secure Scientific Cyberinfrastructure: **SSC;**
- Collaborative Security Response Center: **CSRC;** or
- Research Data Protection: **RDP.**

For example, if you are submitting a Secure Scientific Cyberinfrastructure proposal, then your title would be: **CICI: SSC: title.**

Project Description: Refer to Section II. Program Description, for additional information about requirements for each of the three program areas.

Supplementary Documents:

Supplementary documents are limited to the specific types of documentation listed in the PAPPG, with exceptions specified below.

1. *List of Project Personnel and Partner Institutions (Note - In proposals with subawardee institutions, only the institution submitting the proposal should provide this information):* Provide current, accurate information for **all personnel and institutions involved in the project.** NSF staff will use this information to manage reviewer selection. The list should include all PIs, Co-PIs, Senior Personnel, paid/unpaid Consultants or Collaborators, Sub awardees, Postdocs, and project-level advisory committee members. This list should be numbered, in alphabetical order by last name, and include for each entry (in this order) Full name, Organization(s), and Role in the project, with each item separated by a semi-colon. Each person listed should start a new numbered line. For example:
    1. Mary Adams; XYZ University; PI
    2. John Brown; University of PQR; Senior Personnel
    3. Jane Green; XYZ University; Postdoc
    4. Bob Jones; ABC Inc.; Paid Consultant
    5. Tim White; ZZZ University; Subawardee
2. *Letters of Collaboration:* Refer to Section II. Program Description, for additional information about requirements for each of the three program areas.
3. *Project Plan:* Each proposal should include a Project plan. Up to 5 pages are allowed for **SSC** and **RDP** proposals and up to 10 pages are allowed for **CSRC** proposals.

Refer to Section II. Program Description, for additional Supplementary Document requirements for each of the three program areas.

Single Copy Documents:

Collaborators and Other Affiliations Information:

Proposers should follow the guidance specified in Chapter II.C.1.e of the NSF PAPPG. Submitters using Grants.gov may upload this document as a PDF.

B. Budgetary Information

Cost Sharing:

Inclusion of voluntary committed cost sharing is prohibited.

Budget Preparation Instructions:

Budgets should include travel funds for the project principal investigators and other team members, as appropriate, from all collaborating institutions to attend one annual Principal Investigators' meeting.

C. Due Dates

- **Full Proposal Deadline(s)** (due by 5 p.m. submitter's local time):

  June 04, 2018

D. FastLane / Grants.gov Requirements

For Proposals Submitted Via FastLane:

To prepare and submit a proposal via FastLane, see detailed technical instructions available at: https://www.fastlane.nsf.gov/a1/newstan.htm. For FastLane user support, call the FastLane Help Desk at 1-800-673-6188 or e-mail fastlane@nsf.gov. The FastLane Help Desk answers general technical questions related to the use of the FastLane system. Specific questions related to this program solicitation should be referred to the NSF program staff contact(s) listed in Section VIII of this funding opportunity.

For Proposals Submitted Via Grants.gov:

Before using Grants.gov for the first time, each organization must register to create an institutional profile. Once registered, the applicant's organization can then apply for any federal grant on the Grants.gov website. Comprehensive information about using Grants.gov is available on the Grants.gov Applicant Resources webpage: http://www.grants.gov/web/grants/applicants.html. In addition, the NSF Grants.gov Application Guide (see link in Section V.A) provides instructions regarding the technical preparation of proposals via Grants.gov. For Grants.gov user support, contact the Grants.gov Contact Center at 1-800-518-4726 or by email: support@grants.gov. The Grants.gov Contact Center answers general technical questions related to the use of Grants.gov. Specific questions related to this program solicitation should be referred to the NSF program staff contact(s) listed in Section VIII of this solicitation.

Submitting the Proposal: Once all documents have been completed, the Authorized Organizational Representative (AOR) must submit the application to Grants.gov and verify the desired funding opportunity and agency to which the application is submitted. The AOR must then sign and submit the application to Grants.gov. The completed application will be transferred to the NSF FastLane system for further processing.

Proposers that submitted via FastLane are strongly encouraged to use FastLane to verify the status of their submission to NSF. For proposers that submitted via Grants.gov, until an application has been received and validated by NSF, the Authorized Organizational Representative may check the status of an application on Grants.gov. After proposers have received an e-mail notification from NSF, Research.gov should be used to check the status of an application.

VI. NSF PROPOSAL PROCESSING AND REVIEW PROCEDURES

Proposals received by NSF are assigned to the appropriate NSF program for acknowledgement and, if they meet NSF requirements, for review. All proposals are carefully reviewed by a scientist, engineer, or educator serving as an NSF Program Officer, and usually by three to ten other persons outside NSF either as *ad hoc* reviewers, panelists, or both, who are experts in the particular fields represented by the proposal. These reviewers are selected by Program Officers charged with oversight of the review process. Proposers are invited to suggest names of persons they believe are especially well qualified to review the proposal and/or persons they would prefer not review the proposal. These suggestions may serve as one source in the reviewer selection process at the Program Officer's discretion. Submission of such names, however, is optional. Care is taken to ensure that reviewers have no conflicts of interest with the proposal. In addition, Program Officers may obtain comments from site visits before recommending final action on proposals. Senior NSF staff further review recommendations for awards. A flowchart that depicts the entire NSF proposal and award process (and associated timeline) is included in PAPPG Exhibit III-1.

A comprehensive description of the Foundation's merit review process is available on the NSF website at: https://www.nsf.gov/bfa/dias/policy/merit_review/.

Proposers should also be aware of core strategies that are essential to the fulfillment of NSF's mission, as articulated in *Investing in Science, Engineering, and Education for the Nation's Future: NSF Strategic Plan for 2014-2018*. These strategies are integrated in the program planning and implementation process, of which proposal review is one part. NSF's mission is particularly well-implemented through the integration of research and education and broadening participation in NSF programs, projects, and activities.

One of the strategic objectives in support of NSF's mission is to foster integration of research and education through the programs, projects, and activities it supports at academic and research institutions. These institutions must recruit, train, and prepare a diverse STEM workforce to advance the frontiers of science and participate in the U.S. technology-based economy. NSF's contribution to the national innovation ecosystem is to provide cutting-edge research under the guidance of the Nation's most creative scientists and engineers. NSF also supports development of a strong science, technology, engineering, and mathematics (STEM) workforce by investing in building the knowledge that informs improvements in STEM teaching and learning.

NSF's mission calls for the broadening of opportunities and expanding participation of groups, institutions, and geographic regions that are underrepresented in STEM disciplines, which is essential to the health and vitality of science and engineering. NSF is committed to this principle of diversity and deems it central to the programs, projects, and activities it considers and supports.

A. Merit Review Principles and Criteria

The National Science Foundation strives to invest in a robust and diverse portfolio of projects that creates new knowledge and enables breakthroughs in understanding across all areas of science and engineering research and education. To identify which projects to support, NSF relies on a merit review process that incorporates consideration of both the technical aspects of a proposed project and its potential to contribute more broadly to advancing NSF's mission "to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense; and for other purposes." NSF makes every effort to conduct a fair, competitive, transparent merit review process for the selection of projects.

1. Merit Review Principles

These principles are to be given due diligence by PIs and organizations when preparing proposals and managing projects, by reviewers when reading and evaluating proposals, and by NSF program staff when determining whether or not to recommend proposals for funding and while overseeing awards. Given that NSF is the primary federal agency charged with nurturing and supporting excellence in basic research and education, the following three principles apply:

- All NSF projects should be of the highest quality and have the potential to advance, if not transform, the frontiers of knowledge.
- NSF projects, in the aggregate, should contribute more broadly to achieving societal goals. These "Broader Impacts" may be accomplished through the research itself, through activities that are directly related to specific research projects, or through activities that are supported by, but are complementary to, the project. The project activities may be based on previously established and/or innovative methods and approaches, but in either case must be well justified.
- Meaningful assessment and evaluation of NSF funded projects should be based on appropriate metrics, keeping in mind the likely correlation between the effect of broader impacts and the resources provided to implement projects. If the size of the activity is limited, evaluation of that activity in isolation is not likely to be meaningful. Thus, assessing the effectiveness of these activities may best be done at a higher, more aggregated, level than the individual project.

With respect to the third principle, even if assessment of Broader Impacts outcomes for particular projects is done at an aggregated level, PIs are expected to be accountable for carrying out the activities described in the funded project. Thus, individual projects should include clearly stated goals, specific descriptions of the activities that the PI intends to do, and a plan in place to document the outputs of those activities.

These three merit review principles provide the basis for the merit review criteria, as well as a context within which the users of the criteria can better understand their intent.

2. Merit Review Criteria

All NSF proposals are evaluated through use of the two National Science Board approved merit review criteria. In some instances, however, NSF will employ additional criteria as required to highlight the specific objectives of certain programs and activities.

The two merit review criteria are listed below. **Both** criteria are to be given **full consideration** during the review and decision-making processes; each criterion is necessary but neither, by itself, is sufficient. Therefore, proposers must fully address both criteria. (PAPPG Chapter II.C.2.d(i). contains additional information for use by proposers in development of the Project Description section of the proposal). Reviewers are strongly encouraged to review the criteria, including PAPPG Chapter II.C.2.d(i), prior to the review of a proposal.

When evaluating NSF proposals, reviewers will be asked to consider what the proposers want to do, why they want to do it, how they plan to do it, how they will know if they succeed, and what benefits could accrue if the project is successful. These issues apply both to the technical aspects of the proposal and the way in which the project may make broader contributions. To that end, reviewers will be asked to evaluate all proposals against two criteria:

- **Intellectual Merit:** The Intellectual Merit criterion encompasses the potential to advance knowledge; and
- **Broader Impacts:** The Broader Impacts criterion encompasses the potential to benefit society and contribute to the achievement of specific, desired societal outcomes.

The following elements should be considered in the review for both criteria:

1. What is the potential for the proposed activity to
    a. Advance knowledge and understanding within its own field or across different fields (Intellectual Merit); and
    b. Benefit society or advance desired societal outcomes (Broader Impacts)?
2. To what extent do the proposed activities suggest and explore creative, original, or potentially transformative concepts?
3. Is the plan for carrying out the proposed activities well-reasoned, well-organized, and based on a sound rationale? Does the plan incorporate a mechanism to assess success?
4. How well qualified is the individual, team, or organization to conduct the proposed activities?
5. Are there adequate resources available to the PI (either at the home organization or through collaborations) to carry out the proposed activities?

Broader impacts may be accomplished through the research itself, through the activities that are directly related to specific research projects, or through activities that are supported by, but are complementary to, the project. NSF values the advancement of scientific knowledge and activities that contribute to achievement of societally relevant outcomes. Such outcomes include, but are not limited to: full participation of women, persons with disabilities, and underrepresented minorities in science, technology, engineering, and mathematics (STEM); improved STEM education and educator development at any level; increased public scientific literacy and public engagement with science and technology; improved well-being of individuals in society; development of a diverse, globally competitive STEM workforce; increased partnerships between academia, industry, and others; improved national security; increased economic competitiveness of the United States; and enhanced infrastructure for research and education.

Proposers are reminded that reviewers will also be asked to review the Data Management Plan and the Postdoctoral Researcher Mentoring Plan, as appropriate.

Additional Solicitation Specific Review Criteria

All proposals must clearly address the following solicitation-specific review criteria:

- **Science-driven**: To what extent is the proposed project science-driven? How will the project outcomes fill well-recognized science and engineering needs of the research community? What will be the broader impacts of the project, such as its benefits to science and engineering communities beyond its initial targets, under-represented communities, and education and workforce development? The project description should provide a compelling discussion of the potential to benefit its intended as well as broader communities.
- **Innovation**: To what extent is the proposed project innovative? What innovative and transformational capabilities will the project bring to its target communities? How will the project integrate innovation and discovery into the project activities?
- **Close collaborations among stakeholders**: To what extent does the proposed project involve close collaborations among stakeholders? How will the project activities engage cyberinfrastructure (CI) experts, specialists, and scientists working in concert with the relevant domain scientists who are users of CI?
- **Building on existing, recognized capabilities**: To what extent does the proposed project build on existing, recognized capabilities? How will the project activities build on and leverage existing NSF, national, and open source cyberinfrastructure and cybersecurity investments, as appropriate?
- **Project plans, and system and process architecture**: How well detailed are the project plans, and logical and physical architectures? The project description should include high-quality management plans. The project plan should include user interactions and provide a timeline including a proof-of-concept demonstration or prototyping of the proposed system or framework.
- **Sustained impact**: What potential does the proposed work have for providing benefits beyond the participants and the lifetime of the award?

B. Review and Selection Process

Proposals submitted in response to this program solicitation will be reviewed by Ad hoc Review and/or Panel Review.

Reviewers will be asked to evaluate proposals using two National Science Board approved merit review criteria and, if applicable, additional program specific criteria. A summary rating and accompanying narrative will generally be completed and submitted by each reviewer and/or panel. The Program Officer assigned to manage the proposal's review will consider the advice of reviewers and will formulate a recommendation.

After scientific, technical and programmatic review and consideration of appropriate factors, the NSF Program Officer recommends to the cognizant Division Director whether the proposal should be declined or recommended for award. NSF strives to be able to tell applicants whether their proposals have been declined or recommended for funding within six months. Large or particularly complex proposals or proposals from new awardees may require additional review and processing time. The time interval begins on the deadline or target date, or receipt date, whichever is later. The interval ends when the Division Director acts upon the Program Officer's recommendation.

After programmatic approval has been obtained, the proposals recommended for funding will be forwarded to the Division of Grants and Agreements for review of business, financial, and policy implications. After an administrative review has occurred, Grants and Agreements Officers perform the processing and issuance of a grant or other agreement. Proposers are cautioned that only a Grants and Agreements Officer may make commitments, obligations or awards on behalf of NSF or authorize the expenditure of funds. No commitment on the part of NSF should be inferred from technical or budgetary discussions with a NSF Program Officer. A Principal Investigator or organization that makes financial or personnel commitments in the absence of a grant or cooperative agreement signed by the NSF Grants and Agreements Officer does so at their own risk.

Once an award or declination decision has been made, Principal Investigators are provided feedback about their proposals. In all cases, reviews are treated as confidential documents. Verbatim copies of reviews, excluding the names of the reviewers or any reviewer-identifying information, are sent to the Principal Investigator/Project Director by the Program Officer. In addition, the proposer will receive an explanation of the decision to award or decline funding.

VII. AWARD ADMINISTRATION INFORMATION

A. Notification of the Award

Notification of the award is made to *the submitting organization* by a Grants Officer in the Division of Grants and Agreements. Organizations whose proposals are declined will be advised as promptly as possible by the cognizant NSF Program administering the program. Verbatim copies of reviews, not including the identity of the reviewer, will be provided automatically to the Principal Investigator. (See Section VI.B. for additional information on the review process.)

B. Award Conditions

An NSF award consists of: (1) the award notice, which includes any special provisions applicable to the award and any numbered amendments thereto; (2) the budget, which indicates the amounts, by categories of expense, on which NSF has based its support (or otherwise communicates any specific approvals or disapprovals of proposed expenditures); (3) the proposal referenced in the award notice; (4) the applicable award conditions, such as Grant General Conditions (GC-1)*; or Research Terms and Conditions* and (5) any announcement or other NSF issuance that may be incorporated by reference in the award notice. Cooperative agreements also are administered in accordance with NSF Cooperative Agreement Financial and Administrative Terms and Conditions (CA-FATC) and the applicable Programmatic Terms and Conditions. NSF awards are electronically signed by an NSF Grants and Agreements Officer and transmitted electronically to the organization via e-mail.

*These documents may be accessed electronically on NSF's Website at https://www.nsf.gov/awards/managing/award_conditions.jsp?org=NSF. Paper copies may be obtained from the NSF Publications Clearinghouse, telephone (703) 292-7827 or by e-mail from nsfpubs@nsf.gov.

More comprehensive information on NSF Award Conditions and other important information on the administration of NSF awards is contained in the NSF *Proposal & Award Policies & Procedures Guide* (PAPPG) Chapter VII, available electronically on the NSF Website at https://www.nsf.gov/publications/pub_summ.jsp?ods_key=pappg.

C. Reporting Requirements

For all multi-year grants (including both standard and continuing grants), the Principal Investigator must submit an annual project report to the cognizant Program Officer no later than 90 days prior to the end of the current budget period. (Some programs or awards require submission of more frequent project reports). No later than 120 days following expiration of a grant, the PI also is required to submit a final project report, and a project outcomes report for the general public.

Failure to provide the required annual or final project reports, or the project outcomes report, will delay NSF review and processing of any future funding increments as well as any pending proposals for all identified PIs and co-PIs on a given award. PIs should examine the formats of the required reports in advance to assure availability of required data.

PIs are required to use NSF's electronic project-reporting system, available through Research.gov, for preparation and submission of annual and final project reports. Such reports provide information on accomplishments, project participants (individual and organizational), publications, and other specific products and impacts of the project. Submission of the report via Research.gov constitutes certification by the PI that the contents of the report are accurate and complete. The project outcomes report also must be prepared and submitted using Research.gov. This report serves as a brief summary, prepared specifically for the public, of the nature and outcomes of the project. This report will be posted on the NSF website exactly as it is submitted by the PI.

More comprehensive information on NSF Reporting Requirements and other important information on the administration of NSF awards is contained in the NSF *Proposal & Award Policies & Procedures Guide*, available electronically on the NSF Website at https://www.nsf.gov/publications/pub_summ.jsp?ods_key=pappg.

VIII. AGENCY CONTACTS

Please note that the program contact information is current at the time of publishing. See program website for any updates to the points of contact.

General inquiries regarding this program should be made to:

- Kevin Thompson, Program Director, CISE/OAC, telephone: (703) 292-4220, email: kthompso@nsf.gov

For questions related to the use of FastLane, contact:

- FastLane Help Desk, telephone: 1-800-673-6188; e-mail: fastlane@nsf.gov.

For questions relating to Grants.gov contact:

- Grants.gov Contact Center: If the Authorized Organizational Representatives (AOR) has not received a confirmation message from Grants.gov within 48 hours of submission of application, please contact via telephone: 1-800-518-4726; e-mail: support@grants.gov.

IX. OTHER INFORMATION

The NSF website provides the most comprehensive source of information on NSF Directorates (including contact information), programs and funding opportunities. Use of this website by potential proposers is strongly encouraged. In addition, "NSF Update" is an information-delivery system designed to keep potential proposers and other interested parties apprised of new NSF funding opportunities and publications, important changes in proposal and award policies and procedures, and upcoming NSF Grants Conferences. Subscribers are informed through e-mail or the user's Web browser each time new publications are issued that match their identified interests. "NSF Update" also is available on NSF's website.

Grants.gov provides an additional electronic capability to search for Federal government-wide grant opportunities. NSF funding opportunities may be accessed via this mechanism. Further information on Grants.gov may be obtained at http://www.grants.gov.

ABOUT THE NATIONAL SCIENCE FOUNDATION

The National Science Foundation (NSF) is an independent Federal agency created by the National Science Foundation Act of 1950, as amended (42 USC 1861-75). The Act states the purpose of the NSF is "to promote the progress of science; [and] to advance the

national health, prosperity, and welfare by supporting research and education in all fields of science and engineering."

NSF funds research and education in most fields of science and engineering. It does this through grants and cooperative agreements to more than 2,000 colleges, universities, K-12 school systems, businesses, informal science organizations and other research organizations throughout the US. The Foundation accounts for about one-fourth of Federal support to academic institutions for basic research.

NSF receives approximately 55,000 proposals each year for research, education and training projects, of which approximately 11,000 are funded. In addition, the Foundation receives several thousand applications for graduate and postdoctoral fellowships. The agency operates no laboratories itself but does support National Research Centers, user facilities, certain oceanographic vessels and Arctic and Antarctic research stations. The Foundation also supports cooperative research between universities and industry, US participation in international scientific and engineering efforts, and educational activities at every academic level.

Facilitation Awards for Scientists and Engineers with Disabilities (FASED) provide funding for special assistance or equipment to enable persons with disabilities to work on NSF-supported projects. See the *NSF Proposal & Award Policies & Procedures Guide* Chapter II.E.6 for instructions regarding preparation of these types of proposals.

The National Science Foundation has Telephonic Device for the Deaf (TDD) and Federal Information Relay Service (FIRS) capabilities that enable individuals with hearing impairments to communicate with the Foundation about NSF programs, employment or general information. TDD may be accessed at (703) 292-5090 and (800) 281-8749, FIRS at (800) 877-8339.

The National Science Foundation Information Center may be reached at (703) 292-5111.

The National Science Foundation promotes and advances scientific progress in the United States by competitively awarding grants and cooperative agreements for research and education in the sciences, mathematics, and engineering.

To get the latest information about program deadlines, to download copies of NSF publications, and to access abstracts of awards, visit the NSF Website at https://www.nsf.gov

- **Location:** 2415 Eisenhower Avenue, Alexandria, VA 22314
- **For General Information** (NSF Information Center)**:** (703) 292-5111
- **TDD (for the hearing-impaired):** (703) 292-5090
- **To Order Publications or Forms:**

  Send an e-mail to: nsfpubs@nsf.gov

  or telephone: (703) 292-7827
- **To Locate NSF Employees:** (703) 292-5111

PRIVACY ACT AND PUBLIC BURDEN STATEMENTS

The information requested on proposal forms and project reports is solicited under the authority of the National Science Foundation Act of 1950, as amended. The information on proposal forms will be used in connection with the selection of qualified proposals; and project reports submitted by awardees will be used for program evaluation and reporting within the Executive Branch and to Congress. The information requested may be disclosed to qualified reviewers and staff assistants as part of the proposal review process; to proposer institutions/grantees to provide or obtain data regarding the proposal review process, award decisions, or the administration of awards; to government contractors, experts, volunteers and researchers and educators as necessary to complete assigned work; to other government agencies or other entities needing information regarding applicants or nominees as part of a joint application review process, or in order to coordinate programs or policy; and to another Federal agency, court, or party in a court or Federal administrative proceeding if the government is a party. Information about Principal Investigators may be added to the Reviewer file and used to select potential candidates to serve as peer reviewers or advisory committee members. See Systems of Records, NSF-50, "Principal Investigator/Proposal File and Associated Records," 69 Federal Register 26410 (May 12, 2004), and NSF-51, "Reviewer/Proposal File and Associated Records," 69 Federal Register 26410 (May 12, 2004). Submission of the information is voluntary. Failure to provide full and complete information, however, may reduce the possibility of receiving an award.

An agency may not conduct or sponsor, and a person is not required to respond to, an information collection unless it displays a valid Office of Management and Budget (OMB) control number. The OMB control number for this collection is 3145-0058. Public reporting burden for this collection of information is estimated to average 120 hours per response, including the time for reviewing instructions. Send comments regarding the burden estimate and any other aspect of this collection of information, including suggestions for reducing this burden, to:

Suzanne H. Plimpton
Reports Clearance Officer
Office of the General Counsel
National Science Foundation
Alexandria, VA 22314

National Science Foundation, 2415 Eisenhower Avenue, Alexandria, Virginia 22314, USA
Tel: (703) 292-5111, FIRS: (800) 877-8339 | TDD: (703) 292-5090 or (800) 281-8749