NSF 25-531: Cybersecurity Innovation for Cyberinfrastructure (CICI)

Program Solicitation

Document Information

Document History
- **Posted:** January 3, 2025
- **Replaces:** NSF 23-517

View the program page

U.S. National Science Foundation
Directorate for Computer and Information Science and Engineering
Office of Advanced Cyberinfrastructure

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

April 02, 2025

January 21, 2026

Third Wednesday in January, Annually Thereafter

Table Of Contents

Important Information And Revision Notes

The CICI program continues to support work that enables scientists and scientific discovery by improving the security, robustness, and trustworthiness of cyberinfrastructure. The current solicitation:

- Clarifies the requirement to target and benefit scientific cyberinfrastructure, users, and applications, and identify unique security requirements of the cyberinfrastructure or science application that motivates the approach; and

- Adds a requirement that any curated datasets are required to be shared publicly and made available through established community platforms and adhere to the Findability, Accessibility, Interoperability, and Reuse of digital assets (https://www.go-fair.org/fair-principles/ ☑) Guiding Principles for scientific data management and stewardship.

- Adds a fourth track focused on integrity, provenance, and authenticity for scientific datasets used in Artificial Intelligence.

Any proposal submitted in response to this solicitation should be submitted in accordance with the *NSF Proposal & Award Policies & Procedures Guide* (PAPPG) that is in effect for the relevant due date to which the proposal is being submitted. The NSF PAPPG is regularly revised and it is the responsibility of the proposer to ensure that the proposal meets the requirements specified in this solicitation and the applicable version of the PAPPG. Submitting a proposal prior to a specified deadline does not negate this requirement.

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 advance scientific discovery and innovation by enhancing the security and privacy of cyberinfrastructure. CICI supports efforts to develop, deploy and integrate cybersecurity that will benefit the broader scientific community by securing science data, computation, collaborations workflows, and infrastructure. CICI recognizes the unique nature of modern, complex, data-driven, distributed, rapid, and collaborative

science and the breadth of infrastructure and requirements across scientific disciplines, practitioners, researchers, and projects. CICI seeks proposals in four program areas:

1. **Usable and Collaborative Security for Science (UCSS):** Projects in this program area should support novel and/or applied security and usability research that facilitates scientific collaboration, encourages the adoption of security into the scientific workflow, and helps create a holistic, integrated security environment that spans the entire scientific cyberinfrastructure ecosystem.

2. **Reference Scientific Security Datasets (RSSD):** Projects in this program area should leverage instrumented cyberinfrastructure to capture metadata from scientific workflows and workloads as reference data artifacts that can help support reproducible security research, testing and evaluation.

3. **Transition to Cyberinfrastructure Resilience (TCR):** Projects in this program area should improve the robustness, trustworthiness, integrity, and/or resilience of scientific cyberinfrastructure through testing, evaluation, hardening, validation, and technology transition of novel cybersecurity research. The TCR area further encourages transition activities that advance the deployment and use of reproducibility in CI, workflows, and data.

4. **Integrity, Provenance, and Authenticity for Artificial Intelligence Ready Data (IPAAI):** Projects in this program area should enhance confidence and reproducibility in AI produced scientific results by improving the integrity, provenance, and authenticity of scientific datasets used by Artificial Intelligence systems.

Broadening Participation In STEM

NSF recognizes the unique lived experiences of individuals from communities that are underrepresented and/or under-served in science, technology, engineering, and mathematics (STEM) and the barriers to inclusion and access to STEM education and careers. NSF highly encourages the leadership, partnership, and contributions in all NSF opportunities of individuals who are members of such communities supported by NSF. This includes leading and designing STEM research and education proposals for funding; serving as peer reviewers, advisory committee members, and/or committee of visitor members; and serving as NSF leadership, program, and/or administrative staff. NSF also highly encourages demographically diverse institutions of higher education (IHEs) to lead, partner, and contribute to NSF opportunities on behalf of their research and education communities. NSF expects that all individuals, including those who are members of groups that are underrepresented and/or under-served in STEM, are treated equitably and inclusively in the Foundation's proposal and award process.

NSF encourages IHEs that enroll, educate, graduate, and employ individuals who are members of groups underrepresented and/or under-served in STEM education programs and careers to lead, partner, and contribute to NSF opportunities, including leading and designing STEM research and education proposals for funding. Such IHEs include, but may not be limited to, community colleges and two-year institutions, mission-based institutions such as Historically Black Colleges and Universities (HBCUs), Tribal Colleges and Universities (TCUs), women's colleges, and institutions that primarily serve persons with disabilities, as well as institutions defined by enrollment such as Predominantly Undergraduate Institutions (PUIs), Minority-Serving Institutions (MSIs), and Hispanic Serving Institutions (HSIs).

"Broadening participation in STEM" is the comprehensive phrase used by NSF to refer to the Foundation's goal of increasing the representation and diversity of individuals, organizations, and geographic regions that contribute to STEM teaching, research, and innovation. To broaden participation in STEM, it is necessary to address issues of equity, inclusion, and access in STEM education, training, and careers. Whereas all NSF programs might support broadening participation components, some programs primarily focus on supporting broadening participation research and projects. Examples can be found on the NSF Broadening Participation in STEM website.

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.

- Daniel F. Massey, telephone: (703) 292-5147, email: dmassey@nsf.gov
- 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

Estimated Number of Awards: 12 to 20

The estimated number of awards per program area is as follows: 3-6 Usable and Collaborative Security for Science (UCSS) awards; 2-5 Reference Scientific Security Dataset (RSSD) awards; 2-4 Transition to Cyberinfrastructure Resilience (TCR) awards; and 4-6 Integrity, Provenance, and Authenticity for Artificial Intelligence Ready Data (IPAAI) awards.

Anticipated Funding Amount: $8,000,000 to $12,000,000

Total funding for the CICI program is $8,000,000 to $12,000,000, subject to the availability of funds. Each program area will support awards pursuant to the following budget and duration:

1. Usable and Collaborative Security for Science (UCSS) awards will be supported at up to $600,000 total per award for up to 3 years;
2. Reference Scientific Security Datasets (RSSD) awards will be supported at up to $600,000 total per award for up to 3 years;
3. Transition to Cyberinfrastructure Resilience (TCR) awards will be supported at up to $1,200,000 total per award for up to 3 years;
4. Integrity, Provenance, and Authenticity for Artificial Intelligence Ready Data (IPAAI)awards will be supported at up to $900,000 total per award for up to 3 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 U.S., 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 sub-awards 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 U.S. campus.
- Non-profit, non-academic organizations: Independent museums, observatories, research laboratories, professional societies and similar organizations located in the U.S. that are directly associated with educational or research activities.

Who May Serve as PI:

There are no restrictions or limits.

Limit on Number of Proposals per Organization:

There are no restrictions or limits.

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

An individual can participate as PI, co-PI or senior/key 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/Key Personnel in the proposed activity, irrespective of whether that individual would receive financial support from the project.

In the event that any individual exceeds this limit, any proposal submitted to this solicitation with this individual listed as PI, co-PI, or Senior/Key Personnel after the second proposal is received at NSF will be returned without review. No exceptions will be made.

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 Research.gov: *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. submitting organization's local time):

  April 02, 2025

  January 21, 2026

  Third Wednesday in January, Annually Thereafter

Proposal Review Information Criteria

Merit Review Criteria:

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

Award Administration Information

Award Conditions:

Additional award conditions apply. Please see the full text of this solicitation for further information.

Reporting Requirements:

Standard NSF reporting requirements apply.

I. Introduction

Scientific research cyberinfrastructure (CI), including computing, networking, data, and Artificial Intelligence (AI), plays a central role in supporting collaborative, data-driven discovery across all scientific disciplines. However, science CI faces unique security and privacy challenges. Collaboration and resource sharing are integral to open science but must adhere to security policies and regulations while providing as seamless of a workflow as possible to domain scientist users. Simultaneously, data and workflow integrity, provenance, and authenticity are crucial to the scientific enterprise and the reproducibility of scientific results. Both unintentional and malicious cyberinfrastructure errors can lead to invalid results and this risk only increases due to growing adoption and use of AI systems. This solicitation broadly targets improving research CI through cybersecurity, thereby creating CI that facilitates scientific initiatives, projects, users, collaborations, and discoveries.

II. Program Description

Cyberinfrastructure (CI) plays a key role in modern scientific exploration and discovery. CI has become an integral enabler of research across disciplines as the amount of computationally accessible scientific data grows exponentially. Secure and robust scientific infrastructure is thus vital for multiple stakeholders. Operators wish to protect their infrastructure from misuse, ensure high availability, and avoid liability. Policy makers seek to promote science and FAIR (Findable, Accessible, Interoperable, and Reusable) principles while ensuring that sensitive research data (e.g., personally identifiable information or intellectual property), cannot be ex-filtrated or abused. The research community and public must maintain their confidence in the integrity and authenticity of the entire research process; this necessitates transparency and reproducibility along every step of the computational workflow(s) to ensure rigorous science and trust in the results. Further, the growing use of AI systems as part of the scientific process amplifies both the speed at which scientific data is analyzed and the importance of data integrity, provenance, and authenticity. Domain scientists require performant and available cyberinfrastructure. However, end-users of open scientific infrastructure may consider security processes valuable only insofar as they do not slow or otherwise impede their research. Ensuring the usability of security mechanisms is therefore critical to their adoption and use within the scientific community.

Scientific data and workloads can be fundamentally different from those seen in traditional network, storage, and computing scenarios. Individual platforms, projects, and data may have significantly different security sensitivities, threats, and constraints. Similarly, scientific CI applications frequently employ unique hardware, software, and configurations that may be unmaintained, less well-vetted, or introduce entirely new classes of vulnerabilities. Solutions to protecting scientific data, computation, and workflows must thus both balance and expose these trade-offs, all while accommodating a variety of policies and stakeholders. The objective of the Cybersecurity Innovation for Cyberinfrastructure (CICI) program is to develop, integrate, and transition cybersecurity, privacy, and usability solutions that benefit cyberinfrastructure and the wider scientific community.

This solicitation seeks research to make scientific data, workflows, and infrastructure more secure and robust while explicitly considering usability, the nature of modern scientific collaboration, data sharing, reproducibility, and the use of AI as part of the scientific process. Applied research proposals should lead to new understandings of scientific infrastructure security properties, secure scientific workflows and benefit domain scientists, transition novel cybersecurity techniques to research cyberinfrastructure, discover vulnerabilities in existing infrastructure, create new pathways for

ensuring reproducibility through cybersecurity, or gather meta-data critical to advancing the security of science infrastructure.

The CICI program targets applied security research directly relevant to scientific cyberinfrastructure in support of cross-science discovery, and is intended to complement other OAC programs enabling CI such as Campus Cyberinfrastructure (CC*) and Cyberinfrastructure for Sustained Scientific Innovation (CSSI). CICI is not the appropriate mechanism for non-cybersecurity infrastructure efforts. It is also not intended to provide support for fundamental cybersecurity or privacy research; such projects may be better served as submissions to the Secure and Trustworthy Cyberspace (SaTC) program.

CICI comprises four Program Areas outlined below:

1. **Usable and Collaborative Security for Science (UCSS)**

   The modern scientific enterprise requires rapid, flexible, and reliable collaboration among participants from varied backgrounds who are using distributed infrastructure and working on problems with a variety of security requirements. Resource sharing, whether in the form of computation or data, is integral to the modern, CI-intensive scientific process and requires that significant infrastructure exists to facilitate such collaboration. Collaborative scientific experiments may include participants from multiple institutions, laboratories, or organizations physically or logically distributed across campuses, sites, or countries. Complex technical relationships may exist between users, institutions, and information technology service providers. The security and availability of end-to-end scientific workflows is crucial to the integrity, scalability, speed of discovery, and reproducibility of scientific analyses. However, domain scientists may lack the knowledge, background, or resources to secure – or understand the security of – research workflows, computation, data, and policies. Ensuring the usability and benefit of cybersecurity for the domain scientists is therefore crucial.

   One specific type of proposal in the UCSS area may focus on the initialization of collaborative security operations for research and education activities that support development of secure computing enclaves. Researchers and network operators must work collaboratively to ensure the cyberinfrastructure achieves an appropriate level of both security and usability. As operational cybersecurity continues to mature, network operators often rely on the concept of a Security Operation Center (SOC). Workshops such as the Workshop on SOC Operations and Construction ⧉ illustrate advances in both the maturity of SOC operations and the research challenges associated with SOCs. In the context of research cyberinfrastructure, this could include a multi-organization SOC such as a SOC that creates a regional enclave or SOC that creates an enclave for scientific drivers across many institutions. In other scenarios, a SOC may be associated with a single institution and may even be associated with a single laboratory or experiment. Correspondingly, the implementation of the SOC may vary from a complex advanced center similar to those found at large companies to a small bespoke collection of tools operated by a single staff or student. Regardless of the scale and configuration, collaboration between researchers and operators is valuable for achieving usable and collaborative security for science. NSF especially encourages SOC proposals focusing on small and under-resourced institutions that would facilitate the establishment of regional enclaves. In addition to the benefits that can be provided to the underlying CI, NSF views campus and multi-SOC activities as significant opportunities to engage students and train the next generation of security experts.

   This program area seeks security and usability research that facilitates scientific collaboration, encourages the adoption of security into the scientific workflow, and/or fosters a holistic, integrated security environment that spans the entire scientific CI ecosystem. Work in this space should specifically address overcoming security obstacles to data and resource sharing in current science CI and projects, and how to enable domain scientists to more easily and seamlessly integrate security considerations into their scientific workflow. Such usability-focused efforts are encouraged to take human factors into account and allow scientists to reason over the trade-off between their research goals and security and privacy concerns specific to the research domain. Proposals in this area are strongly encouraged to identify new collaborations, linkages with existing CI, and new functionality that will be enabled by the proposed security or privacy research.

2. **Reference Scientific Security Datasets (RSSD)**

Scientific cyberinfrastructure, data, and workflows are frequently different from their non-science counterparts, while experiments, collaborations, and analyses may induce different workloads. For instance, data from a science instrument or sensor may present a unique traffic distribution (e.g., machine-to-machine communication, long-lived or high-volume flows, periodicity), memory access, or authentication patterns. Characterization of normal behavior and usage patterns on cyberinfrastructure can aid in detecting anomalies, including outliers, faults, and attacks. Further, a better understanding of the characteristic properties of domain or task-specific workloads can help advance the state of the art in testing and evaluation of cybersecurity mechanisms for science CI, engender reproducible security research, and help protect the scientific process.

This area seeks to gather meta-data from operational or otherwise representative CI that can serve as an open community resource for advancing the cybersecurity posture of these systems. Research of interest in this area includes but is not limited to: instrumenting CI to gather comprehensive and high-fidelity measurements, developing novel methods for collecting, labeling, and curating data from science CI, and methods to share and disseminate security datasets. Efforts toward developing data collection methods and techniques as well as the creation of data artifacts are welcome. Responsive proposals in this sub-area should consider:

- Generality and granularity of the data to be collected, its potential value to advancing research in cybersecurity, and potential to protect scientific CI.
- Examples of specific communities that will benefit from the collected data.
- Responsible and ethical data collection and sharing, including protecting any sensitive or personally identifiable information, for instance through anonymization or other means as applicable.
- The accuracy of any data labels, including anomalous events.
- The plan to store and share the datasets, including long-term preservation and maintenance.
- Metrics for assessing community use and adoption of the datasets.

The intended outcome of an RSSD project is a publicly available dataset that provides the cybersecurity research community a rich source of data to: i) understand operational and/or realistic scientific CI; ii) develop new and novel cybersecurity technologies; and iii) provide realistic data for rigorous and realistic testing, evaluation, and validation of cybersecurity research.

All curated datasets are required to be shared publicly and made available through established community platforms. Awarded projects will work with their program officer to identify the best suited community platform. Proposals are also expected to adhere to FAIR principles ☑. Costs associated with hosting an object store are permissible in the budget.

3. **Transition to Cyberinfrastructure Resilience (TCR)**

Transitioning cybersecurity research to operational scientific CI can provide benefits to both the CI as well as the target cybersecurity research endeavor itself, and in so doing realize the benefits of translational research. The primary objective is to improve the security posture of scientific CI by employing the latest cybersecurity innovations. Scientific CI must frequently innovate and evolve to accommodate the challenging requirements of domain scientists, experiments, and collaborations. Further, scientific CI frequently employs unique hardware, software, and configurations data and workloads. This complexity and traditional lack of security emphasis by domain scientists creates unique and challenging security sensitivities, threats, and constraints for scientific CI. Rather than lag behind on operational cybersecurity practices, scientific CI should instead strive to lead the way in cybersecurity innovation and employ the most promising novel advances in cybersecurity research. This area therefore welcomes test and evaluation efforts by third- parties, e.g., independent deployment and validation of security and privacy technologies, that result in improved CI security posture.

While the primary objective is to improve the security posture of Scientific CI, the relative openness, flexibility, and agility of research infrastructure presents a potential transition pathway for testing, evaluating, and deploying cybersecurity research. The unique and often complex ecosystem of software, hardware, configurations, instruments, data, and users in scientific CI can serve to evaluate and validate cybersecurity innovations more

comprehensively. Further, test and evaluation of cybersecurity research within scientific environments can potentially gain insights from real-world conditions, permit causal analysis, and allow for cybersecurity results and experimental data to be shared more broadly within the research community. Work that transitions either bespoke cybersecurity research innovations tailored for scientific environments or more general cybersecurity research that benefits science CI is welcome. Proposals are encouraged to demonstrate how the approach will directly improve the security posture of scientific CI and have a secondary benefit of demonstrating how cybersecurity innovations can transition into operational practice.

Proposals in this area should seek to improve the robustness of scientific CI through operational or at-scale deployment, test and evaluation of novel cybersecurity research and techniques. Approaches in this area may include, but are not limited to, applied research in, and transition of: scientific workflow integrity, scientific data sharing, usable security, red-teaming, program analysis, fuzzing, penetration testing, and hardening existing systems and components. As the scale of datasets used in scientific CI increase and the location of the data becomes more diffused, NSF especially encourages the adoption of information centric approaches that support the use of nearby secure dataset caching rather than having to retrieve data directly from a repository. The ability to associate integrity and authenticity directly with the data is preferable to approaches the authenticate the data based on its source. Other types of innovative network access techniques might incorporate advances from cellular communication and/or non-terrestrial network communication. By extending scientific CI to challenging locations, one could potentially increase the ability of researchers to gather data while simultaneously providing emerging network access techniques with an operational user-base to demonstrate the new innovations feasibility.

The TCR area further encourages transition activities that advance the deployment and use of reproducibility in CI, workflows, and data. Reproducibility is core to scientific progress and establishing trust in scientific results. However, mechanisms to support reproducibility are often missing from CI or deployed in an ad- hoc manner. Proposals focused on transition to support reproducibility are encouraged to consider reproducibility holistically (e.g., inclusive of provenance, integrity, and long-term sustainability) and broadly (e.g., across science domains and infrastructures).

Proposals are encouraged to leverage existing research CI, facilities, testbeds, and testing frameworks as applicable. Proposals must explicitly detail the transition plan; transition platform, pathway, and partners; and quantitative metrics of expected technology maturation or transition success.

4. **Integrity, Provenance, and Authenticity for Artificial Intelligence Ready Data (IPAAI)**

   Artificial Intelligence (AI) plays an increasingly important role in scientific CI. Using AI, researchers can incorporate vast datasets from multiple locations and conduct experiments at a scale that was previously considered infeasible. This creates tremendous new scientific opportunities, but also raises new cybersecurity challenges related to the integrity, provenance, and authenticity of the datasets upon which AI relies. Unintentional errors in the data used to train AI systems could impact the outcome of experiments across a variety of science drivers. Further, intentional malicious manipulation of datasets could be used to drive AI systems toward invalid and/or misleading results. The sheer scale of datasets and the ability to ingest datasets from a variety of sources increase the research potential, this same increase also raises potential cybersecurity vulnerabilities.

   Researchers require tools and techniques to enhance the integrity, provenance, and authenticity of datasets before the data is incorporated into AI models and systems. Ideally, scientific CI should help ensure the integrity, provenance, and authenticity of datasets, the network connectivity used to provide the data, and the computation systems used in the analysis of the data. The scale and automation enabled by AI can also make these errors difficult and perhaps impossible to detect. Further, confidence in results and reproducibility can only be achieved if the data used by a model is logged and documented so that the researchers can identify what datasets were used to produce a given result. In the event a dataset is found to be compromised or simply inaccurate, researchers must be able to determine whether that dataset was used in their results. If a dataset is found be compromised or inaccurate and a researcher is able to determine that AI techniques used that data, it is not clear how the researcher should remove the data from their model. Unlike a static experiment that could simply be

repeated without the problematic data, an AI system may have incorporated aspects of the data into its model. It is anticipated that simply restarting and retraining an AI system from scratch may be infeasible for future large models and systems.

The IPAAI area encourages proposals that help ensure the integrity, provenance, and authenticity of dataset and/or communication and/or computation used by scientific AI systems. By increasing the integrity, provenance, and authenticity of the input to AI systems, the confidence in the resulting output is also increased. For example, an AI system that incorporates data from a scientific instrument might include techniques to ensure the integrity of the data received from the instrument. AI systems that incorporated medical data might include techniques to determine the data provenance and ensure the dataset does not violate privacy requirements. AI systems that incorporate cached public datasets might include techniques to ensure the cached copy is an authentic version of the original dataset. In all three of these cases, it is unclear how an AI system might discard the invalid data and recover if say the sensor data was corrupted, medical data violated privacy restrictions, or cached data was (intentionally or unintentionally) modified to remove or replace key features. Proposals are not limited to these dataset example and these are intended only as examples of why integrity, provenance, and authenticity are critical for AI data.

Proposals in this area should seek to improve the integrity, provenance, and authenticity of scientific CI through novel cybersecurity research and techniques. Proposals that help provide verifiable indicators of integrity, provenance, and authenticity are welcome. Further, inclusion of a comprehensive approach to logging data would be an additional feature, but is not a requirement. The objective for such a feature would be to verify what data was used to produce AI generated results. This allows for reproducibility by other researchers and also allows a researcher to determine if their results relied on data later found to be compromised. The focus of the IPAAI topic is on integrity, provenance, and authenticity that helps prevent an AI result from incorporating compromised data and optionally provides a verifiable log of what data was used. A reliable log provides both reproducibility by other researchers and for detection if data is determined to be compromised after inclusion. Any proposal should clearly demonstrate the use of scientific data and corresponding science drivers. Approaches may also benefit other applications, but the primary focus of the proposal should be directed toward the use of AI in science.

CICI program-wide guidelines:

All CICI proposals, across all four program areas, must include a description of:

- Existing scientific infrastructure and distributed scientific environments that will benefit from the proposed research;
- How the proposed security mechanisms or infrastructure enhancements will advance scientific discoveries, collaborations, and innovations, and benefit scientific applications, users, and communities;
- Any unique properties of the scientific domain or infrastructure that influence the desired security functionality, design, or mechanisms;
- The software license that will be used for any released software, and justification for why this license has been chosen;
- A sustainability plan describing how the proposed system will be supported beyond the project duration; and
- Any ethical and operational concerns of the work, including obtaining explicit consent of target CI or entities under test, protecting the privacy of sensitive datasets, and establishing processes for informed disclosure as required.

All CICI proposals are encouraged to:

- 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 included in the Supplementary Documents section of the proposal.

- 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 Risk Profile (OSRP) ↗.
- Make any software developed under proposed activities publicly available under an open-source license;
- Provide a plan for gathering quantitative metrics to assess the anticipated security benefits on CI from the proposed work, e.g., science projects or researchers impacted, harms mitigated, etc; and
- Describe how the proposed work has potential for benefits beyond the lifetime of the award and will benefit groups beyond the proposers themselves.

III. Award Information

Anticipated Type of Award: Continuing Grant or Standard Grant

Estimated Number of Awards: 12-20

Anticipated Funding Amount: $8,000,000 - $12,000,000

Total funding for the CICI program is $8,000,000 to $12,000,000, subject to the availability of funds. Each program area will support awards pursuant to the following budget and duration:

1. Usable and Collaborative Security for Science (UCSS) awards will be supported at up to $600,000 total per award for up to 3 years;
2. Reference Scientific Security Datasets (RSSD) awards will be supported at up to $600,000 total per award for up to 3 years; and
3. Transition to Cyberinfrastructure Resilience (TCR) awards will be supported at up to $1,200,000 total per award for up to 3 years; and
4. Integrity, Provenance, and Authenticity for Artificial Intelligence Ready Data (IPAAI)awards will be supported at up to $900,000 total per award for up to 3 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 U.S., 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 sub-awards 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 U.S. campus.
- Non-profit, non-academic organizations: Independent museums, observatories, research laboratories, professional societies and similar organizations located in the U.S. that are directly associated with educational or research activities.

Who May Serve as PI:

There are no restrictions or limits.

Limit on Number of Proposals per Organization:

There are no restrictions or limits.

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

An individual can participate as PI, co-PI or senior/key 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/Key Personnel in the proposed activity, irrespective of whether that individual would receive financial support from the project.

In the event that any individual exceeds this limit, any proposal submitted to this solicitation with this individual listed as PI, co-PI, or Senior/Key Personnel after the second proposal is received at NSF will be returned without review. No exceptions will be made.

Additional Eligibility Info:

Collaborative proposals submitted from different organizations, with each organization requesting a separate award, are not allowed. Instead, proposals involving multiple organizations must be submitted as a single proposal, in which a single award is being requested (with sub-awards 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 Research.gov or Grants.gov.

- Full Proposals submitted via Research.gov: Proposals submitted in response to this program solicitation should be prepared and submitted in accordance with the general guidelines contained in the *NSF Proposal and Award Policies and 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) 292-8134 or by e-mail from nsfpubs@nsf.gov. The Prepare New Proposal setup will prompt you for the program solicitation number.

- 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) 292-8134 or by e-mail from nsfpubs@nsf.gov.

See PAPPG Chapter II.D.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 one of the four program area acronyms below:

- Usable and Collaborative Security for Science: **UCSS**;
- Reference Scientific Security Datasets: **RSSD**;
- Transition to Cyberinfrastructure Resilience: **TCR**; or

- Integrity, Provenance, and Authenticity for Artificial Intelligence Ready Data: **IPAAI**

For example, if you are submitting a Usable and Collaborative Security for Science proposal, then your title would be: **CICI:UCSS:title**.

Project Description: Refer to Section II. Program Description, for additional information about requirements for each of the four 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 Organizations (Note - In proposals with sub-awardee organizations, only the organization submitting the proposal should provide this information): Provide current, accurate information for **all personnel and organizations involved in the project.** NSF staff will use this information to manage reviewer selection. The list should include all PIs, co-PIs, Senior/Key Personnel, funded/unfunded Consultants or Collaborators, sub-awardees, postdoctoral researchers, 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. Mei Lin; XYZ University; PI

2. Jak Jabes; University of PQR; Senior/Key Personnel

3. Jane Brown; XYZ University; Postdoctoral Researcher

4. Rakel Ademas; ABC Inc.; Funded Consultant

5. Maria Wan; Welldone Institution; Unfunded Collaborator

6. Rimon Greene; ZZZ University; Sub-awardee

2. Letters of Collaboration: Partnership documentation from personnel not included in the proposal as PI, co-PI, or senior/key personnel should be in the form of a letter of collaboration included in the Supplementary Documents section of the proposal.

Letters should document collaborative arrangements of significance to the proposal and MUST stay within the PAPPG requirement to state only the intent to collaborate. They should not contain endorsements or evaluation of the proposed project.

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, to attend one annual Principal Investigators' meeting each year the award is active. All curated datasets are required to be shared publicly and made available through established community platforms. Costs associated with hosting an object store are permissible in the budget.

C. Due Dates

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

  April 02, 2025

  January 21, 2026

Third Wednesday in January, Annually Thereafter

D. Research.gov/Grants.gov Requirements

For Proposals Submitted Via Research.gov:

To prepare and submit a proposal via Research.gov, see detailed technical instructions available at: https://www.research.gov/research-portal/appmanager/base/desktop? _nfpb=true&_pageLabel=research_node_display&_nodePath=/researchGov/Service/Desktop/ProposalPreparationa For Research.gov user support, call the Research.gov Help Desk at 1-800-381-1532 or e-mail rgov@nsf.gov. The Research.gov Help Desk answers general technical questions related to the use of the Research.gov 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: https://www.grants.gov/applicants. 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 Research.gov for further processing.

The NSF Grants.gov Proposal Processing in Research.gov informational page provides submission guidance to applicants and links to helpful resources including the NSF Grants.gov Application Guide, Grants.gov Proposal Processing in Research.gov how-to guide, and Grants.gov Submitted Proposals Frequently Asked Questions. Grants.gov proposals must pass all NSF pre-check and post-check validations in order to be accepted by Research.gov at NSF.

When submitting via Grants.gov, NSF strongly recommends applicants initiate proposal submission at least five business days in advance of a deadline to allow adequate time to address NSF compliance errors and resubmissions by 5:00 p.m. submitting organization's local time on the deadline. Please note that some errors cannot be corrected in Grants.gov. Once a proposal passes pre-checks but fails any post-check, an applicant can only correct and submit the in-progress proposal in Research.gov.

Proposers that submitted via Research.gov may use Research.gov 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 acknowledgment 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 *Leading the World in Discovery and Innovation, STEM Talent Development and the Delivery of Benefits from Research - NSF Strategic Plan for Fiscal Years (FY) 2022 - 2026*. 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.D.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.D.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 other

underrepresented groups 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?

- **Open and FAIR datasets:** Will any curated data sets generated in this solicitation be shared publicly and made available through an established community platform? Did the Data Management Plan adhere to the Findability, Accessibility, Interoperability, and Reuse of digital assets (https://www.go-fair.org/fair-principles/ 🔗 Guiding Principles for scientific data management and stewardship?

- **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 CI 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 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 proposers whether their proposals have been declined or recommended for funding within six months. Large or particularly complex proposals or proposals from new recipients 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 or the Division of Acquisition and Cooperative Support 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 an NSF Grants and Agreements Officer. 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)*; 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) 292-8134 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.

Administrative and National Policy Requirements

Build America, Buy America

As expressed in Executive Order 14005, Ensuring the Future is Made in All of America by All of America's Workers (86 FR 7475), it is the policy of the executive branch to use terms and conditions of Federal financial assistance awards to maximize, consistent with law, the use of goods, products, and materials produced in, and services offered in, the United States.

Consistent with the requirements of the Build America, Buy America Act (Pub. L. 117-58, Division G, Title IX, Subtitle A, November 15, 2021), no funding made available through this funding opportunity may be obligated for infrastructure projects under an award unless all iron, steel, manufactured products, and construction materials used in the project are produced in the United States. For additional information, visit NSF's Build America, Buy America webpage.

Special Award Conditions:

All curated datasets are required to be shared publicly and made available through established community platforms. Awarded projects will work with their program officer to identify the best suited community platform. Proposals are also expected to adhere to FAIR principles ⬚.

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* (PAPPG) Chapter VII, 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:

- Daniel F. Massey, telephone: (703) 292-5147, email: dmassey@nsf.gov
- Kevin Thompson, Program Director, CISE/OAC, telephone: (703) 292-4220, email: kthompso@nsf.gov

For questions related to the use of NSF systems contact:

- NSF Help Desk: 1-800-381-1532
- Research.gov Help Desk e-mail: rgov@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 https://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.F.7 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**   (703) 292-5111
  (NSF Information Center)**:**
- **TDD (for the hearing-impaired):**   (703) 292-5090

- **To Order Publications or Forms:**

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

    or telephone: (703) 292-8134

- **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 proposers 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/recipients 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 proposers 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 System of Record Notices, NSF-50, "Principal Investigator/Proposal File and Associated Records," and NSF-51, "Reviewer/Proposal File and Associated Records." 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
Policy Office, Division of Institution and Award Support
Office of Budget, Finance, and Award Management
National Science Foundation
Alexandria, VA 22314