NCITE NATIONAL COUNTERTERRORISM INNOVATION, TECHNOLOGY, AND EDUCATION CENTER

A U.S. DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

2023-2024 NCITE Research Projects Request for Proposals

Issue Date: December 21, 2022
Proposal Due Date: February 24, 2023

Submit proposals using our NU Ramp submission portal.

About NCITE

The National Counterterrorism Innovation, Technology, and Education Center (NCITE) is the Department of Homeland Security's (DHS) Center of Excellence for terrorism prevention and counterterrorism research. NCITE is a consortium of universities and industry partners whose mission is to conduct research, education, and workforce development activities that will respond to challenging problems and offer innovative solutions to issues faced by counterterrorism and targeted violence prevention professionals – both in the public and private sectors. Led by the University of Nebraska at Omaha, the focus of NCITE is to support operationally relevant research and development efforts. More information may be found at https://www.unomaha.edu/ncite/.

Table of Contents

NCITE Research Grant Program Overview

NCITE's vision is to be the premier U.S. academic provider of counterterrorism research, technology, and workforce development.

NCITE's research seeks to innovate, educate, and create new counterterrorism and prevention strategies while building a workforce pipeline where it's desperately needed: in STEM and Homeland Security fields.

As DHS' trusted partner for counterterrorism and terrorism prevention research, NCITE seeks to bring together the brightest minds in the field and leverage the capabilities of colleges, universities, federal laboratories, industry, and nonprofit organizations to help thwart terrorism.

Our mission is to make these research findings relevant and ready. Our hope is to help America's Homeland Security frontline be known as first in-class in terrorism and targeted violence prevention.

Because NCITE is sponsored by the Office of University Programs in DHS' Science and Technology Directorate, the intent of this call is to spark innovation from university labs and research teams. As such, only proposals led by universities will be considered for funding. However, we do welcome collaborative proposals that include non-government organizations, individual consultants, and technology partners (although such partners are not required).

Moving from Year 3 to Year 4, NCITE is requesting proposals across our four research themes:

1. The nature of counterterrorism and targeted violence operations
2. The nationwide suspicious activity reporting initiative
3. Terrorism and targeted violence prevention and program evaluation
4. Counterterrorism and targeted violence workforce development

With those objectives in mind, NCITE requests proposals intended to address research questions and challenges that NCITE, DHS, and/or its partners in the Homeland Security Enterprise (HSE) have posed. NCITE will lead a scientific review of proposals and facilitate a DHS relevancy review after scientific merit has been evaluated.

Estimated Funding

Pending receipt of funding, NCITE intends to award approximately 3-4 new projects in 2023-2024. These projects will be conducted from approximately July 1, 2023, through 12 to 36 months following grant award, with the opportunity for continuation pending performance and DHS funding availability. Average award in 2022-2023 for a one-year period of

performance was $153K, and individual awards varied depending on level of effort and evaluation of impact to DHS mission areas.

Eligible Grantees

As noted above, organizations eligible to receive NCITE grants for 2023-2024 are institutes of higher education. NCITE does not award grants to individuals, private non-higher education organizations, or to federal, state, county, or local government entities — though those groups may be partners in the work conducted by the grant recipient. The proposal's designated principal investigator must be an employee of the higher-education organization applying for an NCITE grant.

Eligible Projects

In 2023-2024, NCITE will fund projects that should either generate new knowledge (research projects) or inspire and develop the current and/or future HSE workforce. Funding decisions will be based on how well an invited proposal meets the evaluation criteria detailed in Appendix D. Quantitative scoring of the evaluation criteria will be provided by scientific reviewers and then advanced to DHS for a relevancy review. We are particularly interested in funding projects that align to the challenge questions listed in Appendix A.

Please note that all selected projects must be able to complete the proposed research using non-DHS data sources or simulated and/or synthetic data. DHS is unable to provide operational data suitable for algorithm development and testing to performers under this award. Each proposal must identify how and where it will acquire real, simulated, or other synthetically generated data.

NCITE reserves the right to fund, in whole or in part, any, all, or none of the applications submitted in response to this request for proposals. Submission requirements for this grant program may be waived at the discretion of NCITE.

In accordance with University of Nebraska at Omaha policy, NCITE does not discriminate on the basis of race, color, age, ethnicity, religion, national origin, pregnancy, sexual orientation, gender identity, genetic information, sex, marital status, disability, or status as a U.S. veteran.

Submission Guidance

Deadline

The due date for grant proposals is 11:59 p.m. EST on February 24, 2023, via NU Ramp. https://nuramp.nebraska.edu/ems/event.php?EMSEventUUID=1b47d644-c832-42b3-b49c-3c3013911561

Format

See Appendix B for cover page guidelines and Appendix C for details on proposal requirements.

Multi-Year Project Proposals

Applicants may submit multi-year proposals with deliverables and budgets with a period of performance beginning July 1, 2023. Budgets submitted in the proposal will be reviewed each year. Continued funding after the initial 12-month period of performance will be contingent upon acceptable performance in reviews by NCITE and DHS, available funding, and continued need. In funding a project one year, NCITE makes no guarantee that it will continue to fund the program in successive years.

Partners awarded multi-year projects must follow the same reporting schedule for semiannual and annual reports.

Applicant Notification and Timeline

NCITE will strive to notify applicants regarding our intent to fund in June 2023 for a period of performance beginning on July 1, 2023. Please note that research project start is contingent upon IRB, DHS Compliance Assurance Program Office (CAPO), and DHS Privacy approvals.

Privacy Guidelines

Research grant awards will be subject to the terms and conditions found on the NCITE webpage at www.unomaha.edu/ncite under the RFP tab. Applicants are encouraged to review the terms and conditions prior to drafting and submitting a proposal to determine their ability and/or willingness to adhere to the proposal requirements and to accept the terms and conditions in a subaward should one be awarded.

Due to the nature of the cooperative agreement that governs the NCITE grant from DHS, subaward projects are subject to additional privacy guidelines. NCITE's review of proposals will include an evaluation of risk to individuals' privacy, civil rights, and civil liberties. As a result, applicants must include a description of data they intend to use in the proposed

project (particularly third-party data, defined below) and how they will acquire and manage that data, to include the use of privacy enhancing technologies.

- Third-party data is data which is not generated via project activities. This could include social media data, existing datasets shared by other researchers, commercial datasets, etc. Examples of data that is not third-party would include data generated through surveys, interviews, focus groups, or experiments conducted by the research team.

If a project that includes methods or data sources that could result in the collection, generation, or use of personally identifiable information (PII), sensitive PII, or other privacy sensitive information is awarded, the principal investigator shall incorporate safeguards to ensure alignment with the Fair Information Practice Principles (FIPPs) and to adequately protect the data. Information on those safeguards should be provided in the proposal, and NCITE will work with awardees to ensure they are in accordance with the FIPPs.[1]

- Personally Identifiable Information (PII) is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department.
- Sensitive PII is PII which, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.
- Privacy sensitive means that the research activity could have an impact on an individual's privacy – be it bodily privacy, communications privacy, territorial privacy, or information privacy.

Examples of projects that meet the definition of privacy sensitive may include those that use social media data or those that involve commingling information with other data sources that may make it privacy sensitive. Although, in general, NCITE can fund projects that are privacy sensitive, please be advised that those projects may require additional levels of review by NCITE and DHS. This process can take up to 3-6 months, so it is important that researchers build privacy reviews from the funder into their workplans as a funded activity.

Questions about this Request for Proposals

Applicants should direct questions about this request for proposals to kaylawalters@unomaha.edu with the subject line "Question re: NCITE Y4 RFP." Written questions will be accepted until Friday, February 3, 2023.

NCITE will publish a document with all written questions and responses to the RFP page on our website by February 10, 2023, for review by all prospective applicants.

[1] https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

Appendix A: Challenge Questions

The NCITE challenge questions are research questions or homeland security challenges from NCITE, the Department of Homeland Security (DHS), and other partners in the homeland security enterprise (HSE) that new proposals should seek to address. They are aligned to the four NCITE research themes and will guide the direction of new projects for Year 4. As you develop proposals to address the identified challenges, please consider how your proposed project aligns to:

- DHS Strategic Framework for Countering Terrorism and Targeted Violence
- National Strategy for Countering Domestic Terrorism
- FBI and DHS Strategic Intelligence Assessment and Data on Domestic Terrorism

Please keep in mind that proposals should be research-based and leverage your academic expertise and training to provide foundational knowledge to inform the HSE's strategy and policy for the counterterrorism mission over the next 5-10 years.

Challenge Area 1: Nature of Counterterrorism and Targeted Violence Operations

1. What is the nature of novel terrorism and targeted violence threats against the United States? What novel terrorist violence techniques and targets will emerge in the next 3-5 years? How is threat trajectory likely to evolve in coming years?

2. How can terrorists make malign use of emerging technologies (e.g., Unmanned Aircraft Systems (UAS), artificial intelligence, extended reality, cryptocurrencies, deep fakes, 3D printing), and what groups and/or individuals are most likely to adopt them? What specific factors could spur increases or decreases in emerging technology adoption by terrorist groups or violent extremists?

3. What emerging technologies and internal processes can improve information sharing across the homeland security workforce and stakeholder community to counter terrorism and targeted violence?

4. What emerging technologies and internal processes can augment the homeland security workforce's operations against current and emerging threats of terrorism and targeted violence?

5. What upcoming state, local, tribal, or territorial legislation might impact terrorism or targeted violence (e.g., abortion-related violence, climate-related violence) in the United States? How might CT resource shifts affect terrorist threats? What disruption and policy measures have the potential to diminish current and emerging threats?

6. To what extent and why are we seeing U.S.-based terrorism actors influenced by a mix of different violent extremist ideologies?

7. To what extent are we seeing online, financial, and in-person connectivity between U.S.-based and overseas-based domestic terrorism actors, including travel to conflict zones overseas? What emerging technologies, approaches, and countermeasures are likely to influence those capabilities and intentions in coming years?

8. To what extent are foreign and domestic terrorism actors exploiting publicly available information concerning U.S. critical infrastructure (e.g., agriculture, energy) to identify vulnerabilities? To what extent are foreign and domestic terrorists targeting U.S. critical infrastructure for physical and cyber-attacks?

9. To what extent are aspects of violent extremist ideologies and conspiracy theories being normalized in the U.S. and other Western countries, why we are seeing a mainstreaming of these narratives, and what opportunities exist to improve society's digital literacy and information sharing with online platforms where these narratives often are circulated?

10. How can we evaluate and prioritize threats from terrorist actors and groups by using innovative applications of data and advanced analytic methodologies to explain the global threat landscape's complexity? How can we assess risk globally, against U.S. interests, and inside the U.S. homeland?

11. How is violence perceived among today's youth and what methodologies/techniques do young adults (16-24 years old) use to plan and execute violent acts compared to older adults?

12. How can we measure violence from insurgency versus terrorism? What are the key indicators to differentiate them? What factors point to insurgencies transitioning to or being coopted by terrorists?

13. What and where are the localized insurgencies and political uprisings that possibly may generate terrorist threats to U.S. interests in the next 3-5 years? What makes those uprisings more likely to spur terrorism versus other types of political engagement? Are there novel ways to counteract and disengage groups from such a path?

14. How do terrorist groups raise, move, store, and spend funds? How do their financials operate internationally and what are the differences between local and transnational efforts? What emerging technologies are they drawing on, and how can those transactions be detected? What are the evolving illicit financing trends and techniques used by violent extremists, and how can CT practitioners and first responders equip to detect and counter them?

15. Which emerging technologies pose the greatest risk to critical infrastructure sectors for which CISA is the sector risk management agency (SRMA), and what are the first and second order consequences?

16. What factors influence target selection for practitioners of terrorism, and can those factors be modeled to calculate impacts based on target characteristics and terrorist capabilities?

17. What data accurately characterize terrorists' interest in and capability to use chemical, biological, radiological, and nuclear (CBRN) materials in an attack? What trends does that data show regarding the CBRN threat to the United States? What are the current trends in CBRN tactics used by terrorists and violent extremists, and what are the implications of a potential attack? Who are the key terrorist and violent extremist leaders, supporters, and online networks involved in CBRN development, plotting, procurement, and proliferation of information and materiel? How can those actors be detected, deterred, or disrupted?

18. What factors affect terrorist preference when choosing communications platforms? How can the U.S. Government and other CT practitioners predict or anticipate movement to new platforms?

19. What are the evolving messaging trends and techniques used by violent extremists, online and offline, to recruit and radicalize? How can first responders equip to detect and combat them?

20. How can we identify and detect trends in the extent that foreign terrorist organizations focus outreach on U.S. audiences and what opportunities exist to counter those messages?

21. How can data science and machine learning be used to identify future mobilization hotspots?

Challenge Area 2: Nationwide Suspicious Activity Reporting Initiative

1. How can we facilitate partners' abilities to identify, evaluate, and share tips/leads associated with terrorism and targeted violence? Is the Nationwide Suspicious Activity Reporting Initiative (NSI) achieving what it was set up to do? This system and process was set up after September 11th, 2001, to increase collaboration and information sharing throughout the country on terrorism-related information.

2. How can we reinvigorate the need and obligation for increased information sharing between agencies, states, and jurisdictions?

3. What can we do to protect civil rights and liberties in evaluating new technology to support the National Threat Evaluation and Reporting (NTER) Program?

4. How do we follow up with the reporter after he or she makes a report? If the reporter is a parent, or a medical provider, what information can be given to the reporter? Should there be further collaboration? Are there any best practices in place to address that?

5. How can U.S. Government officials who encounter known and suspected terrorists at a U.S. port of entry identify and determine whether or not a subject has links to extremist activities beyond an immediate physical threat (i.e., suspicious financial transactions, use of secure communications platforms, etc.)?

Challenge Area 3: Terrorism and Targeted Violence Prevention & Program Evaluation

1. What can NCITE do to support Regional Prevention Coordinators and CISA protective security advisors?

2. When making decisions to commit a violent act, how much influence do parents, peers, friends, neighbors, and bystanders have on an individual?

3. What are innovative methods for scaling the outcome and impact evaluations of terrorism and targeted violence prevention programs? What role can technology play in evaluating programs designed for early-, middle-, and late-phase violence prevention?

4. How can federal partners support state, local, tribal, and territorial efforts to build violence prevention strategies?

5. What are the standard baseline capabilities needed for threat assessment teams across community types and sizes (e.g., data sharing, communications, team composition)? How can NCITE and DHS support threat assessment teams across the country?

Challenge Area 4: Research on Counterterrorism and Targeted Violence Workforce Development

1. What counterterrorism training is needed for Federal and SLTT law enforcement partners to ensure HSE has the most up-to-date training on terrorism and targeted violence?

2. What best practices from the broader Intelligence Enterprise (IE) can be applied to resource allocation, career pathing, and training curriculums for the DHS CT workforce?

3. Using the National Intelligence Council's 2040 Global Trends Report, forecast what work-related competencies might be needed for the counterterrorism professional. With a changing regulatory, social, and technological landscape, what CT-related jobs are emerging that either do not currently exist or need to be scaled up across the U.S.? What are the anticipated or emerging requirements (e.g., KSAOs) of those jobs? What tools (e.g., technologies) will be required for those jobs?

4. What steps can DHS take to create a more cohesive culture across its many components and to improve its public image? Similarly, what strategies can the Department employ to attract and retain top talent, particularly in competitive fields like data science?

5. What CT-related skills would help fortify non-governmental critical infrastructure owners and operators in securing against new or existing threats?

6. What fields or areas of study will be required to help prepare the future HSE workforce to address emergent issues in 3-5+ years?

7. What are the key challenges impacting the recruitment and retention of professional safety and security personnel? What can DHS do to address these challenges?

8. What educational programs for the future are needed to train and develop prevention experts who are in positions of influence (e.g., licensed clinical social workers, first responders)?

Appendix B: Cover Page

Information to be included in your cover page:

- Project Title
- NCITE Research Theme
- Challenge Question (if applicable)
- Project Information
    - Principal Investigator (Name, Institution, and Contact Information)
    - Co-Principal Investigators (Name, Institution, and Contact Information)
    - Administrative Contact (Name, Institution, and Contact Information)

Appendix C: Proposal Requirements

All project proposals – either research and development or workforce development – in response to this call must explicitly include the following sections below. Proposals should be no more than 12 single-spaced pages.

Proposal Sections

Proposals must contain all the following elements. Applicants should strictly abide by this framework.

1. A completed cover page that contains the information shown in Appendix B, identifying the research question/challenge need that your research project will address. Note: cover page is not included in the 12-page limit.

2. Detailed descriptions of your project to include the following sections:

    a. **Abstract (a summary of objectives, outcomes, value proposition)**
    Provide a summary overview of the research concept being proposed, to include a description of:
        - Your research objectives (at a high level)
        - The intended outcomes of your project
        - The value proposition for your project.

    b. **Objectives/Purpose**
    Provide a description of:
        - The tangible objectives and outcomes of your research and detail how those outcomes map onto the DHS Strategic Framework for Countering Terrorism and Targeted Violence.
        - The purpose of the research, including key literature references, demonstrating that this concept will help address a resiliency need identified by DHS, its federal partners, or the homeland security enterprise that is NOT currently being adequately addressed.

    c. **Baseline**
    Identify the baseline state of knowledge or practice in your target domain (e.g., currently, the counterterrorism mission center does not know the future impact of pending FSLTT laws on domestic terrorism in the U.S.).

    d. **Methodology**
    Clearly describe your research methodology to include the proposed method, required data, and analytic technique.

    e. **Data**

Describe in detail the types of data and data sources you anticipate using to complete the proposed research.

- Identify if you will be using any third-party data or privacy-sensitive data (e.g., social media data, data requiring execution of a license or consent/cooperation of current owner or custodian, PII or sensitive PII, protected critical infrastructure information, 1st amendment rights information).
- Describe how you anticipate using, storing, and protecting all data.

f. **Project Milestones and Deliverables**

There are several required deliverables and reporting metrics throughout the course of the project as outlined below:

i. Required to begin work
   - Submission of project to your university's Institutional Review Board (IRB)
   - Submission of institutional approvals to the DHS Compliance Assurance Program Office (CAPO) and Privacy Office via NCITE administrative team and OUP Program Manager
   - Submission of Data Acquisition and Management Plan. A template will be provided, and is available on our RFP tab on the NCITE website for a realistic preview of what working with NCITE will entail.
   - Government kick-off meeting via Microsoft Teams

ii. Required Reporting
   - Semiannual Report (mid-December) describing scientific and applied outcomes of research, as well as students impacted, government engagement, and field & industry outreach. A template will be provided.
   - Annual Report (early July) describing scientific and applied outcomes of research, as well as students impacted, government engagement, and field & industry outreach. A template will be provided.

iii. Required Participation
   - Participation in annual NCITE meeting in Omaha, D.C., or virtual

Using the provided table below, outline your project milestones and deliverables in addition to the required items, organizing by date.

- A milestone would be identified for conceptual moments and project steps.
- A deliverable would be considered a tangible product, report, or final outcome.

Milestone or Deliverable	Description of Proposed Activity	Projected Date
Milestone	Submission of IRB Approvals [Required]	ASAP

Milestone	Hold Kickoff Meeting with Project Team/NCITE/Government [Required]	July – August 2023
Deliverable	Data Acquisition and Management Plan [Required]	Within 30 days initiating work
Deliverable	Semiannual Progress Report [Required]	December 1, 2023
Milestone	Attendance at Annual Meeting [Required]	Spring 2024
Deliverable	Annual Progress Report [Required]	July 20, 2024

g. **Performance Metrics**
Describe the metrics you will use to evaluate progress or impact of your project.

h. **Transition Plan**
Describe how you deliver end-user value to include how you will disseminate knowledge products or develop, protect, and market technology products.

i. **Stakeholder Engagement**
List and describe current DHS or HSE stakeholders and partner relationships. Describe the benefits that would accrue to DHS and/or the HSE through successful completion of your research. Identify specific DHS components and other HSE agencies, owners, and operators that would benefit. Describe your prosed plan to engage with them throughout the project.

j. **Potential Programmatic Risks**
Describe any potential risks or barriers to completing the work as described.

k. **Project Outcomes and Outputs**
Describe the anticipated outcomes and outputs of your project, including information on how those outcomes and outputs will advance or impact current policies, procedures, technologies, or capabilities. Describe how your project will improve upon the current state of knowledge and practice.

l. **Qualifications**
Provide a summary of the expertise and capabilities of the research team, including:
- The applicant's credentials in this topic area, including past accomplishments.
- The names of public- and private-sector partners.
- Commitments from partners in terms of collaboration and resources.

m. **Citations** (not included in the 12-page limit)

n. **Estimated Cost**

Detail the total estimated cost for the project using a 12-month (or multi-year) period of performance with submission of the budget template and budget justification (templates found on the NCITE webpage at www.unomaha.edu/ncite under the RFP tab).

Note that upon award, NCITE may require additional documentation, such as a human-subject research plan or a research safety plan, if applicable and per the deliverable requirements to conduct this work.

Applicants may append any additional documentation they feel will help the decision process of NCITE. Examples of such information may include resumes of key personnel and letters of commitment from research partners. Although such appendices are not subject to the 12-page limit, applicants should exercise discretion in providing additional material.

Project Reporting

If awarded a research grant – in addition to other promised deliverables – the grantee shall provide NCITE with progress reports throughout the project period. These will include periodic meetings with NCITE and government end-users as well as semiannual and annual reports.

Final deliverables must be submitted within 30 days following the grant end date.

NCITE may track metrics on funded projects for up to two years after their completion. The metrics will include information on publications, patents, commercialization, student education, external sponsorship, and further collaborations among the partners that were facilitated by NCITE funding.

Templates and Supplemental Documents

The full written RFP along with project proposal templates can be found on the NCITE webpage at www.unomaha.edu/ncite under the RFP tab.

All proposals must include:

- Required sections listed above as outlined in the appropriate template,
- A written budget justification,
- An Excel budget sheet.

Research grant awards will be subject to the Terms and Conditions found at on the NCITE webpage at www.unomaha.edu/ncite under the RFP tab.

Appendix D: Proposal Evaluation Criteria

The technical description of the proposed project will be reviewed in two phases. First, NCITE will conduct a scientific review of proposals. Second, Department of Homeland Security (DHS) stakeholders will evaluate the relevance of proposed projects.

Scientific Review

Full proposals will be evaluated by NCITE on several criteria:

1. Scientific Contribution
    a. Novelty of research questions
    b. Usefulness of proposed research in addressing scientific problems
    c. Methodological quality
    d. Scientific expertise and viability
2. Planning Quality
    a. Identification and mitigation of programmatic risks
    b. Identification of performance metrics
    c. Identification of a clear transition plan for knowledge and deliverables
3. Stakeholder Relevance
    a. Demonstration of baseline understanding of current DHS knowledge or capabilities
    b. New improvements to the DHS baseline
    c. Anticipated impact on DHS operations
    d. Identification of potential DHS stakeholders

Included in this review are: validity of the proposed approach and likelihood of success based on current state of the art and on the scientific principles underpinning the proposed approach; development of a comprehensive and complete workplan and schedule with milestones and interrelated tasks that clearly lead to the successful completion of the project; identification of key technical risks and mitigation strategies to address them; appropriateness of proposed budget for the planned work; and considerations of protections of privacy and CRCL of U.S. persons.

NCITE also looks for teams that are multi-disciplinary and provide an appropriate level of expertise and capability to provide high confidence of success. As part of that, NCITE also encourages inclusion of plans to inspire students – the future generation of the counterterrorism workforce.

Relevancy Review

Following scientific review, projects are advanced to relevancy review. In this phase, DHS stakeholders will evaluate whether a project significantly advances NCITE's ability to address the operational needs identified by DHS and its partners.

Appendix E: Intellectual Property Guidelines

Intellectual Property (IP) that will either be brought into the project (Background Intellectual Property) or will be developed via the project will require a basic IP Management Plan prior to being awarded should your project be selected. The IP plan should address the following if applicable to your project:

1. Identify ownership of Project IP (who will own the IP?);

2. Licensing rights of project-developed IP, including revenue sharing amount for joint owners of project participants, if applicable (who will have what license rights to the IP?);

3. The project participant(s) that will have rights to enforce rights in project-developed IP (who can enforce those rights?);

4. Background Intellectual Property (BIP) needed for the Project and terms (if any) under which that BIP will be made available to Project Participants both during and after performance of the Project;

5. Terms under which the collective IP will be made available to government and/or industry upon its transition to general use;

6. Who will bear the filing and other costs of managing that Project IP, including the cost of prosecuting foreign and domestic patent rights;

7. An affirmation of the adoption, without exception, of the provisions of Article I, Section A, paragraph 15 and Article II, Section J, of the most current Terms & Conditions of Cooperative Agreement #20STTPC00001-03-01.