CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

FY2018 CIRI RESEARCH GRANTS
REQUEST FOR WHITE PAPERS

Issue date: June 15, 2018
Extended white paper submission due date: August 17, 2018

217-300-2206 | ciri-grants@illinois.edu | ciri.illinois.edu

CIRI
CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE
A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

REQUEST FOR WHITE PAPERS 2018

CIRI FY2018 RESEARCH GRANTS

Issue date: June 15, 2018

CIRI CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE
A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

217-300-2206 | ciri-grants@illinois.edu | ciri.illinois.edu

About the Critical Infrastructure Resilience Institute

The Critical Infrastructure Resilience Institute (CIRI), led by the University of Illinois at Urbana-Champaign, is a Department of Homeland Security Science and Technology Directorate Center of Excellence that conducts research and education that enhances the resilience of the nation's critical infrastructures and the businesses and public entities that own and operate those assets and systems. CIRI achieves its mission through innovative research, technology transition, and education and workforce development. CIRI explores the organizational, policy, business, and technical dimensions of critical infrastructure with a particular emphasis on developing tools and solutions for industry and government agencies to understand and improve resiliency.

Through a multi-disciplinary team of researchers from academia, national laboratories, and the private sector, CIRI delivers transformational technology-driven solutions, data-informed policy recommendations, and decision-making tools for businesses and government agencies; training for today's homeland security workforce; and education for a more resilience-aware and resilience-motivated workforce of tomorrow.

More information on CIRI may be found at http://ciri.illinois.edu/.

CONTENTS

CIRI Research Grant Program Overview

An objective of the Critical Infrastructure Resilience Institute (CIRI) is to bring together capabilities of colleges, universities, federal laboratories, industry, and nonprofit organizations to assess and improve resilience in the ten critical infrastructures for which the Department of Homeland Security (DHS) is the designated sector-specific agency:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Emergency Services
- Government Facilities
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems

CIRI activities are organized around four mission objectives:

1. Building the business case for resilience
2. Informing the policy, regulatory, and standards-setting environment
3. Building and transitioning to use tools and technologies to improve infrastructure resilience
4. Educating and developing a resilience-focused workforce

With those objectives in mind, CIRI is seeking white papers sketching research ideas intended to address a set of resiliency questions/challenges that CIRI, DHS, or its federal partners have posed. CIRI leadership and DHS sponsors will review white paper submissions to identify those for which a full proposal will be requested. The purpose of a white paper is to convey to us the essential problem area, demonstrate knowledge of prior art, identify a research gap, describe the work to be done to close that gap, and identify which of the four aforementioned CIRI mission objectives are supported by the work. A formal proposal review process, including evaluation by external subject matter experts will be conducted to select those for which a grant award will be offered. A formal request for a proposal does not guarantee a grant award.

Estimated Funding

Pending receipt of funding, CIRI intends to set aside approximately $1,000,000 to award projects conducted from approximately October 1, 2018 through 12 months following grant award. Typical awards will be from $150,000 to $300,000.

Eligible Grantees

Organizations eligible to receive CIRI grants are educational institutions, private industry, and private nonprofit organizations and foundations. CIRI does not award grants to individuals or to federal, state, county, or local government entities — though those groups may be partners in the work conducted by the grant recipient. Collaborations among organizations are encouraged, but not required.

The proposal's designated principal investigator must be an employee of the organization applying for a CIRI grant.

Eligible Projects

Funding decisions will be based on how well an invited proposal meets the evaluation criteria detailed at Appendix D. Quantitative scoring of the evaluation criteria will be provided by external expert reviewers.

Eight specific Challenge Areas and an eighth "Other Areas of Interest" are listed below. Two of the Challenge areas require cooperation between US and Canadian institutions. Each white paper must identify which area it addresses.

Challenge Area 1: Data Analysis in Support of Disaster Planning, Response, and Recovery

Disaster response is an important component of resilience. CIRI seeks novel ideas in data analysis (possibly including but not exclusively AI and/or machine learning) which aid humans in identifying lessons learned from past responses, plan for future responses, dynamically respond to a disaster as it unfolds, and execute recovery operations in the aftermath.

Activities to be affected by such capabilities might include:

- identification of long term resource needs,
- long term strategies for placement of resources to be used in response,
- pre-positioning of response resources as a disaster (e.g. hurricane) is imminent,
- deployment of resources to observe, mitigate and recover from disaster,
- law enforcement and governance during and after an event.

Analysis of operational data which refines operational and tactical planning, and data which couples anticipated or observed impacts such as physical damage and displacement/isolation of humans with the ability of responders to react is of highest importance. The research output must establish a strong connection between the proposed research and a quantifiably improved ability to respond and/or plan for future events.

*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.

Context: Disaster response aligns with the DHS mission to strengthen National Preparedness and Resilience. FEMA and the US Coast Guard are DHS components with responsibility for disaster response, as are state and local governments, and proposed research ought to be broadly applicable to these various constituencies.

Challenge Area 2: Text Analysis for Critical Infrastructure Resilience Assessment

Protection of critical infrastructures is a human-intensive activity. Humans gather information for risk assessment, and perform the analysis. Humans develop plans for recovering from deleterious events based on data gleaned from past events and they analyze emergencies, and make decisions leading to remediation. Humans comb through documents looking for correlations that guide policy formulation for resilient critical infrastructures. The data needed for these kinds of analyses are embedded in natural language communications of diverse types. CIRI seeks ideas on developing and applying technologies to automate the gathering and classification of information needed for policy formulation and/or assessment of critical infrastructure resilience. Example technologies include un-supervised machine learning and

natural language processing. Automated means of tagging data for use in supervised machine learning is also of interest.

The context for the research must clearly be text related to critical infrastructures (which may span the spectrum from government publications, to inter-departmental communications, to private postings on social media.) The identified context should clearly connect the research output to particular types of critical infrastructure assessments.

*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.

Context: The February 2018 DHS sponsored Workshop on Artificial Intelligence and Quantum Information Applications in Homeland Security identified a number of challenge areas needing additional research. Automated analysis of text in support of Homeland Security applications was identified as one such Challenge Area.

Challenge Area 3: Security and Resilience of Mobile and IoT Infrastructure, Networks and Devices

Research is needed to develop and/or apply methodologies and tools to help understand the supply chain oriented risks to the Mobile and IoT infrastructure, networks, and devices providing answers to questions such as:

- What are the scalable methods to map the mobile infrastructure network and how is the mobile network infrastructure laid out from a supply chain point of view?
- What entities control and provide services for the Core network (e.g. Evolved Packet Core)?
- What are the risks associated with the structure of the mobile infrastructure network supply chains, including the equipment itself and the deployment strategies utilized?
- Who are the actors engaged in these supply chains and what assets do they control?
- What specific services (e.g. SS7/Diameter) are outsourced and who are the suppliers of such equipment that support Core/RAN capabilities? What are the associated risks?

There are supply chain risks to individual devices as well. Research is needed to apply and/or develop methodologies and tools capable of addressing questions such as:

- What is the supply chain attack surface for a mobile device (e.g., iPhone, Samsung Galaxy, etc.) that an attacker could use to subvert the supply chain to intentionally install malicious functionality? Specifically, what are the points of vulnerability?
- What is the likelihood/probability of an attack in each of the identified points?

Context: Mobile phones have become ubiquitous as not only a means of communication but also as a means of accessing and interacting with web/cloud-based applications, including transactional applications. The Internet of Things (IoT) which promises to underpin the future critical infrastructure is reliant on the same mobile communications technology and infrastructure supporting mobile phones. This critical infrastructure is comprised of a vast ensemble of technologies developed all over the world. This scale and heterogeneity provides a rich attack surface and an increasingly tempting target for cyber exploitation and disruption.

Challenge Area 4: Security and Resilience of Federal Cloud Computing Services

Research is needed to develop and/or apply methodologies and tools to help understand the supply

chain attack surface for a FedRAMP Authorized Cloud Service Provider. The research should be able to:

- Map the supply chain for a FedRAMP Authorized Cloud Service provider. Identify the depth of the mapping needed to adequately capture the cyber risk posed by the supply chain.
- Specifically identify attack locations, and their vulnerability.
- Quantify the likelihood of an attack at each of the identified points.

Context: Cloud infrastructures are increasing becoming the backbone of computer systems involved in critical infrastructure. The vulnerability of critical infrastructures to subversion of cloud services is a serious concern. Cloud services are composed of an ensemble of hardware and software from many manufacturers from all over the world, which means that their supply chain creates vulnerabilities.

Challenge Area 5: US/Canada Cooperative Research in Applications of QIP to Homeland Security

Quantum Information Processing (QIP) has the potential for a variety of applications, including securing communication, and enhancing measurement, e.g., improving inertial sensors, magnetometers, and telescopy. CIRI seeks ideas of developing and applying QIP with a relatively near-term goal of improving applications in Homeland Security. We are open to different ideas of what those applications would be. Proposals need to establish cooperative research between US and Canadian institutions.

Context: The December 2017 DHS sponsored Workshop on Artificial Intelligence and Quantum Information Applications in Homeland Security was a collaborative effort between DHS and Defense Research and Development Canada. One of the desired non-technical outcomes of the Workshop was cooperative research between US and Canadian institutions. One of the desired technical outcomes of the Workshop was development of nearer term QIP technology to relevant problems in Homeland Security.

Challenge Area 6: US/Canada Cooperative Research in Applications of AI to Homeland Security

The fields of artificial intelligence (AI), machine learning (ML), and deep learning (DL) are making rapid advances and may enhance the ability of professionals in the Homeland Security Enterprise to perform more and better analysis and planning for resilience in critical infrastructures. CIRI is interested in proposals that develop and/or apply AI technologies to applications in homeland security. These proposals involving ML and DL need to provide a risk assessment of the impact that these technologies fragility has on the application. CIRI is open to different ideas of what those applications would be. Proposals need to establish cooperative research between US and Canadian institutions.

*DHS is unable to provide operational data suitable for algorithm development and testing to performers under this award. Each white paper must identify how the applicant will acquire real, simulated, or other synthetically generated data.

Context: The December 2017DHS sponsored Workshop on Artificial Intelligence and Quantum Information Applications in Homeland Security was a collaborative effort between DHS and Defense Research and Development Canada. One of the desired non-technical outcomes of the Workshop was cooperative research between US and Canadian institutions. One of the desired technical outcomes of the Workshop was development and/or application of nearer term AI technology to relevant problems in Homeland Security.

Challenge Area 7: Transportation Independencies and Implications on Critical Infrastructures

There are strong interdependencies between transportation and other critical infrastructures, especially energy, communications, and information technology. Disturbances in one infrastructure can impact the ability of the transportation system to properly function. This interdependence may complicate the decision-making of stake-holders in transportation with respect to understanding:

- What the risks actually are, particularly when the source of the risk lies in a different infrastructure sector which is separately managed and operated.
- How to mitigate risks that are identified. What is the role of policy, governance, information sharing, technology?
- How to model and analyze these interdependent systems in a way and at a level that provides useful decision support for transportation stakeholders.

CIRI seeks proposals that address one or more of these issues, or others that arise from consideration of the dependence of transportation on other critical infrastructures.

Context: The nation's transportation system (air, rail, ground, and maritime shipping) moves people and goods throughout the country, and overseas. Resiliency of this system to natural and man-caused disruptions is crucial to public safety and the US economy. Addressing the resiliency issues facing the transportation sector is a significant challenge – exacerbated by the interdependency of the sector on other critical infrastructure sectors – and vice versa.

Challenge Area 8: Resilience Dependency on IT and Communication

As the full range of sectors become increasingly reliant on IT and communications infrastructure, that infrastructure can be the source of wide-scale failures in others. How can we identify and mitigate risk caused by unrecognized single points of failure? For example, if all banks begin to use a certain brand and piece of equipment for critical communications, the integrity of that piece of equipment becomes critical, even though it may be a simple piece of a longer process. The challenge here is that the detailed equipment and configuration choices made by companies may be business confidential and are likely not known by senior managers who often make risk management decisions. CIRI seeks proposals that address the problem of unrecognized single points of failure in IT and communication infrastructures, against the real-world constraints of data sensitivity and confidentiality.

Context: IT and communication are the backbone of most critical infrastructures, and their vulnerability to IT/communications is a serious concern. These systems are privately owned and managed, and operational details that might illuminate their own vulnerabilities are not easily acquired.

Challenge Area 9: Other Areas of Interest to CIRI

This call for white papers does not preclude submissions in areas other than the pre-called-out challenge areas. However, white papers linked to this challenge area need to clearly articulate their relevance to DHS in general, CIRI responsibilities in particular, and the CIRI mission. Examples include but are not limited to:

- R&D to further our understanding of electro-magnetic puluse impacts and potential mitigations for sectors other than the electricity sector.
- Facilitating and exploiting market forces that will spur greater investment in enhancing the security and resilience of critical infrastructure.
- The application of policy prescriptions and industry standards to enhance the security and resilience of critical infrastructure.
- The role of information sharing and resource sharing in risk identification and mitigation.

- Addressing the risks associated with interdependencies of critical infrastructure.
- Assessment and quantification of risks to critical infrastructure systems.
- Planning, prevention, mitigation, and compliance measures.
- Security of cyber and cyber-physical systems.

ALL SELECTED PROJECTS MUST BE ABLE TO COMPLETE THE PROPOSED RESEARCH USING SIMULATED AND/OR SYNTHETIC DATA OR VIA NON-DHS DATA SOURCES. PROJECTS NEED TO IDENTIFY THEIR ANTICIPATED DATA SOURCES.

Deadline

Due date for white papers has been extended to 7 pm (Central Daylight Time) on **August 17, 2018**.
All white papers must be submitted through the CIRI grant application portal at ciri.illinois.edu.
White papers should not exceed 6 pages, excluding bibliography and CVs, and must be uploaded as a single PDF file. White papers should use 1 inch margins, and 11-point font. Submissions that exceed the stated page limit may be rejected without review.

CIRI will treat white papers as proprietary. If a white paper is selected for submission of a full proposal, and a grant is awarded, that proposal may become subject to public disclosure. Non-selected white papers may be retained by CIRI for possible future consideration and, if retained, will continue to be treated as proprietary. Please note that white papers may be reviewed by external expert reviewers and that there will be public disclosure of funded projects.

Applicant Notification

CIRI will strive to notify applicants within 3 weeks after white paper submission whether a full proposal will be requested. The grant award process may take an additional 4 to 6 weeks after submission of proposals, so applicants should adequately accommodate this in the project planning.

NOTE: Applicants invited to submit a full proposal will be required to submit a proposal meeting the requirements identified below in Appendix C, Proposal Requirements. Research grant awards will be subject to the Terms and Conditions found below at Appendix E. Potential applicants are encouraged to review this Appendices prior to drafting and submitting a white paper to determine their ability and/or willingness to adhere to the proposal requirements and to accept the terms and conditions in a sub-award should one be awarded.

Questions about this Request for White Papers

Specific questions about this request for white papers should be addressed in writing to David M. Nicol, Director of the Critical Infrastructure Resilience Institute, at ciri-grants@illinois.edu.

The Critical Infrastructure Resilience Institute 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 CIRI.

In accordance with University of Illinois policy, CIRI 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. Inquiries can be directed to the Office of Diversity, Equity, and Access; 1004 South Fourth Street, Champaign, Illinois 61820; diversity@illinois.edu; (217) 333-0885.

Appendix A

Cover Page Information to be Entered Online

Department of Homeland Security question being addressed

Project information:

- Principal investigator contact information
- Co-principal investigators
- Administrative contact
- Project title

Appendix B

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.

- Identify ownership of Project IP (who will *own* the IP?);
- Licensing rights of project-developed IP, including revenue sharing amount joint owners of project participants, if applicable (who will have what license rights to the IP?);
- The project participant(s) that will have rights to enforce rights in project-developed IP (who can enforce those rights?)
- 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;
- Terms under which the collective IP will be made available to government and/or industry upon its transition to general use;
- Who will bear the filing and other costs of managing that Project IP, including the cost of prosecuting foreign and domestic patent rights;
- An affirmation of the adoption, without exception, of the provisions of Article I, Section A, paragraph 15 and Article II, Section J, of the Terms & Conditions of Cooperative Agreement #2015-ST-061-CIRC01.

Appendix C

Proposal Requirements

Invited proposals must follow a more stringent form than the white papers. Full proposals need to explicitly include the following sections:

Cover page information (see Appendix A) should be entered separately through the grant application portal. The portal includes a downloadable MS Excel budget form that should be completed and then uploaded to the system.

White papers must contain all of the following elements. Applicants should strictly abide by this framework:

1. A completed cover page, generated online, that contains the information shown in Appendix A.

2. A project narrative with the following sections:

a) Overview

i) Identify the research question/challenge and/or critical infrastructure resilience need that your research project will address.
ii) Provide an overview/abstract of the research concept being proposed
iii) Describe your research hypothesis.
iv) Detail how you will test your hypothesis.

b) Background

i) A description of the tangible outcomes of your research and detail how those outcomes will make the nation's critical infrastructure more resilient against natural or manmade disruptions.
ii) Describe in detail the goals and objectives of the project with particular emphasis on the immediate period of performance (first 12 months). Goals and objectives of subsequent periods of performance can be summarized.
iii) Improvement over current concept of operations in the target critical infrastructure domain:
- Identify the current best practices concept of operations in your target domain.
- Describe how your project will improve upon that concept of operations.
- Describe your customer engagement plan – specifically including DHS components and end-user owners and operators – for the entire period of your proposed research.

c) Scope of Work

A discussion of the proposed work, including:

i) A description of the project concept.
ii) A justification, including key literature references, 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.
iii) Clearly describe your research methodology.
iv) An identification of key risks and mitigation strategies to address them.
v) A table with comprehensive descriptions of anticipated deliverables to be provided to CIRI, including mid-project and final reports. Include estimated completion date after receipt of order (ARO). (Copy and paste the table below into your white paper. Add rows as necessary.)

Description of Proposed Deliverable	*Completion Date After Receipt of Order*
Example: Report - Results of Literature Review	*4 weeks*

d) Benefits to DHS and/or the Homeland Security Enterprise

Describe the benefits that would accrue to DHS and/or the Homeland Security Enterprise through successful completion of your research. Identify *specific* DHS components and agencies and owners and operators that would benefit and describe your proposed plan to engage with them throughout the project.

e) Qualifications

A summary of the expertise and capabilities being brought to bear, including:

i) The applicant's credentials in this topic area, including past accomplishments.
ii) The names of public- and private-sector partners.
iii) Commitments from partners in terms of collaboration and resources.

f) Estimated Cost

Detail the total estimated cost for the research discussed in the white paper for the first 12-month period of performance. If the research project is expected to span multiple 12-month periods then provide estimates of the total cost for each 12-month period of performance.

Note that upon award, CIRI may require additional documentation, such as a human-subject research plan or a research safety plan, if applicable.

Applicants may append any additional documentation they feel will help the decision process of CIRI. 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 5-page limit, applicants should exercise discretion in providing additional material.

Project Reporting

If ultimately awarded a research grant - in addition to other promised deliverables, the grantee shall provide CIRI with progress reports throughout the project period – usually via teleconference. Final deliverables must be submitted within 30 days following the grant end date.

CIRI 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 CIRI funding.

Proposal Evaluation

Invited full proposals will be evaluated according to the criteria found in Appendix D. CIRI will be looking for strength in:

- Technical merit
- Impact
- Capability

- Collaboration
- Cost

Appendix D
Invited Proposal Evaluation Criteria

Weight	Criteria
25%	Technical Merit
30%	Impact
20%	Capability
15%	Collaboration
10%	Cost

The technical description of the proposed project and the work plan convincingly present and justify the following:

1. 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.
2. Development of a comprehensive and complete workplan and schedule with milestones and interrelated tasks that clearly lead to the successful completion of the project.
3. The identification of key technical risks and mitigation strategies to address them.
4. A clear set of deliverables.

The project significantly advances CIRI's ability to address the resiliency needs identified by the Department of Homeland Security and its federal partners.

1. The team provides an appropriate level of expertise and capability.
2. Past performance of the team provides high confidence of success.
3. The team has sought collaboration with critical infrastructure stakeholders to better address the federal government's needs.
4. The proposed budget is appropriate and reasonable for the planned work.

Appendix E
Research Grant Terms and Conditions

CENTER OF EXCELLENCE (COE)
COOPERATIVE AGREEMENT TERMS AND CONDITIONS
GRANTS AND FINANCIAL ASSISTANCE DIVISION (GFAD)

In addition to the DHS Standard Terms and Conditions as outlined here: http://www.dhs.gov/publication/fy15-dhs-standard-terms-and-conditions , the following Terms and Conditions apply specifically to this award as administered by the Grants and Financial Assistance Division (GFAD):

ARTICLE I. ADMINISTRATIVE TERMS AND CONDITIONS

A. RESEARCH PROJECT AWARD SPECIFIC TERMS AND CONDITIONS AND/OR RESTRICTIONS

1. The "Additional Award Specific Terms and Conditions" Appendices 1 and 2 attached to the award letter are hereby incorporated into these Terms and Conditions.

2. All funding, with the exception of $750,000, is restricted contingent upon agreement with the award Terms and Conditions, Appendix 1 and Appendix 2, and approval of the first (partial) year's work plan.

3. The requirement under section "G. PERFORMANCE REPORTING" for this award is revised to a semi-annual report the first repeort due at or before the time of each annual work plan submission and the last report due 30 days after the end of the Budget Period. Content and format to be discussed

4. Recipient shall submit all projects and programs funded under this Award to DHS for review and approval.

5. Recipient shall compete fully and fairly, all projects funded under this Award unless DHS has approved otherwise.

6. Recipient shall submit annual work plans for the activities for this Award to DHS for review and approval ahead of the next budget period, including individual recipient activities or projects. Modifications to any project or program funded under this award should be submitted to DHS for review and approval before initiating new work.

a. Annual work plans must provide information on the overall activities of the Center. The work plan shall include:

i. Summary of the Center's strategic vision and activities;

ii. Summary of Center management efforts;

iii. Detailed descriptions on each Center project (including sub-recipient projects) to include:

- o Methodology
- o Project milestones
- o Performance metrics used to evaluate progress,
- o Transition plans
- o Stakeholder engagement

o Potential programmatic risks to completion; and,
o Project outcomes and outputs, including information on how project outcomes will advance or impact current policies, procedures, technologies or capabilities.

iv. Budget information categorized by both object class and project, including budget justification

7. Recipient shall organize and participate in technical review of the research and education efforts funded under this Award annually, at a minimum, or as determined by the DHS Program Officer.

8. Recipient shall participate in a DHS managed, biennial review of the Center's progress against milestones, scientific quality, and commitment from the end user for the activities funded under this Award. The DHS Program Officer will select a review panel of subject matter experts representing government, industry and academia, to the extent practicable.

9. Recipient shall participate in at least two DHS Science and Technology (S&T) outreach events per year for the purposes of sharing information on the research, development, and education efforts funded under this Award.

10. Recipient agrees to work with the technology transfer office of recipient's institution to engage in technology transfer and commercialization activities, as appropriate.

11. DHS has an interest in publications generated from DHS-funded research for program awareness. Recipient shall forward one electronic and one hard copy of all publications generated under this Award to the Program Officer at the time of publication, and shall send a near-final pre-publication draft to the DHS Program Officer.

12. Co-Authoring of Reports and Articles. Papers, presentations, or other documents co-authored by a DHS employee and a COE researcher will be subject to DHS's publications approval process prior to dissemination of the publication by the authors. Recipient shall submit these publications to the DHS author for DHS clearance at least sixty (60) days prior to dissemination of the publication. Recipient agrees to submit all required DHS clearances with the publication materials to the DHS Program Officer of Record.

13. Data Acquisition and Management Plan

a. Prior to initiating work on any research project that requires access to third party data, including data provided by DHS Component agencies, the Recipient must provide a plan for acquiring data as described in (b) below. The Recipient shall coordinate review of the plan with the University Privacy Officer prior to submission to DHS. The Recipient shall submit its plan to the DHS Program Officer for review and comment prior to initiating research. DHS will review the plan and notify the Recipient of any concerns that may be identified. The Recipient shall review the Data Acquisition and Management Plans at least annually and identify or update, as necessary, any new areas of research that require access to third party data.

b. The plan must include the following information for each project:

i. The purpose for collecting the data and characteristics of the data. If the data is deemed privacy sensitive, the Recipient must comply with the applicable federal, state, and local privacy laws, as well as DHS and university/research institute policies regarding the collection and use of personally identifiable information (PII).

ii. The uses of the data.

iii. A written commitment from the data's owner(s) to provide the Recipient the required data and the conditions under which the data will be provided.

iv. A plan for the disposal or retention of the data after the research ends.

c. Flowdown Requirements: The Recipient shall include the substance of this section in all sub-awards/contracts at any tier where the sub-Recipient may use, generate or have access to government facilities and sensitive or classified information.

14. Information Protection Plan

a. Prior to initiating work on any research project that requires access to third party data, including data provided by DHS Component agencies, the Recipient must provide a plan for acquiring data as described in (b) below. The Recipient shall coordinate review of the plan with the University Privacy Officer prior to submission to DHS. The Recipient shall submit its plan to the DHS Program Officer for review and comment prior to initiating research. DHS will review the plan and notify the Recipient of any concerns that may be identified. The Recipient shall review the Data Acquisition and Management Plans at least annually and identify or update, as necessary, any new areas of research that require access to third party data.

In order to ensure research under this Award does not involve, use, or generate sensitive or classified information, intentionally or accidentally, Recipient shall develop an Information Protection Plan that incorporates policies and procedures that properly define, recognize, and protect such sensitive or classified information. Recipient will submit its plan to the DHS Program Officer for review and comment within 30 days of award. The Recipient will be notified of any concerns that may be identified once the plan is reviewed by DHS. The recipient will review the Information Protection Plan at least annually and update as necessary for new or existing areas of research that may involve sensitive information. Recipient will submit any updates to the Information Protection Plans along with annual reports to the DHS Program Officer for review and comment.

Recipient further understands and agrees that despite the best efforts of the Parties to avoid research under this Award that involves, uses, or generates sensitive or classified information, the possibility exists that such information could nonetheless be involved, used or generated and be subject to protection by law, executive order, regulation or applicable DHS policies. The Recipient is, therefore, responsible for compliance with all applicable laws, regulations and policies. Nothing in this Award shall be construed to permit any public disclosure of sensitive and/or classified information in violation of these restrictions.

The Information Protection Plan will ensure the Recipient identifies, secures, and prohibits public disclosure of "sensitive or classified information." Recipient maintains responsibility for their due diligence in identifying and properly marking any information governed by U.S. export controls regulations. For further information on applicable export controls, please see **Article II, Section H** of this award.

b. Required Notifications to DHS:

i. If Recipient determines that research under this Award involved, used, or generated sensitive or classified information, it agrees to secure the information in accordance with its Information Protection Plan and notify the DHS Program Officer immediately.

ii. The Recipient shall inform the DHS Program Officer in writing within 24 hours of the Recipient becoming aware of any potential security lapses involving either: the handling requirements for sensitive or classified information; or material failure of individuals to follow the Information Protection Plan.

c. Flowdown Requirements: The Recipient shall include the substance of this section in all sub-awards/contracts at any tier where the sub-Recipient may use, generate or have access to government facilities and sensitive or classified information.

d. Definitions: For purposes of this section.

i. Sensitive Information. General Definition. Any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, and any supplementary guidance officially communicated in writing by an authorized official of the Department of Homeland Security (including the PCII Program Officer or his/her designee);

Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of federal programs, or other programs or operations essential to the national or homeland security interest; and

Personally Identifiable Information (PII). 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.

ii. Classified Information. Defined as information designated in accordance with Executive Order 12958.

15. Intellectual Property Management

a. It is vitally important that both Parties understand their respective intellectual property rights and applicable obligations under this Award.

b. Recipients should refer to both 2 C.F.R. § 215 "Uniform Administrative Requirement for Grants and Agreements with Institutions for Higher Education, Hospitals" and 37 C.F.R. § 401 "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements" for a complete summary of their rights and responsibilities.

c. Flowdown Requirements: The Recipient shall include the substance of this section in all sub-awards/contracts at any tier where the sub-Recipient may use, generate or have access to government facilities and sensitive or classified information.
d. Definitions: Please refer to Article II. Section J.

16. Research Safety Plan

a. DHS COE research addresses issues of importance to intelligence and counter-terrorism agencies, law enforcement, or emergency responders, all of which involve inherent risks. To ensure that researchers and research facilities funded through this Award meet the highest safety standards possible, DHS requires every Recipient of a COE award to develop a Research Safety Plan. The Recipient shall review the Research Safety Plan at least annually and identify or update, as necessary, any new areas of research or sub-recipients conducting research activities under this plan. This review will also ensure that all sub-recipients conducting research covered by this plan have developed and implemented appropriate safety plans and periodic safety training in accordance with their institutional policies and procedures. Recipient will submit any updates to the Research Safety Plan to the DHS Program Officer for review and comment.
b. The Research Safety Plan must include, at a minimum, the following:
   i. Identification of possible research hazards associated with the types of research to be conducted under this Award;
   ii. Research protocols or practices that conform to generally accepted safety principles applicable to the nature of the research;
   iii. The Recipient's processes and procedures to ensure compliance with the applicable protocols and standards;
   iv. The Recipient's processes and procedures to ensure the prevention of unauthorized activities conducted in association with this Award;
   v. Faculty oversight of student researchers;
   vi. Research safety education and training to develop a culture of safety;
   vii. Access control, where applicable;
   viii. Independent review by subject matter experts of the safety protocols and practices; and
   ix. Demonstrated adherence to all safety-related terms and conditions contained elsewhere in this Award.
c. Flowdown Requirements: The Recipient shall include the substance of this section in all sub-awards/contracts at any tier where the sub-Recipient may conduct research where safety protocols are necessary to conduct safe research.

17. Public Communication: The Recipient shall input and update all required project information into relevant webpage(s) hosted on the www.hsuniveristyprograms.org. Posting and updating Center and project level information is a condition for receiving further annual funding increments. This website is one of the primary mechanisms used to communicate COE information to the public. Project updates follow pre-determined categories of information that must be populated at least annually. The DHS Office of University Programs maintains the right to edit and post submissions to www.hsuniversityprograms.org, as needed.

B. DHS PROGRAMMATIC INVOLVEMENT

In addition to the usual monitoring and technical assistance, the following identifies DHS responsibilities under this Award:

1. DHS shall determine if a kickoff meeting is required for proposed projects or proposed continuations of existing projects. DHS shall coordinate with appropriate DHS staff, Center staff and Center researchers prior to project initiation.

2. DHS shall approve or disapprove annual work plans and any modifications to the work plans for this Award (See Article 1. A.).

3. DHS shall conduct ongoing monitoring of the activities of Recipient's workplan and activities funded through this Award through face-to-face and/or telephone meetings and review of progress reports.

4. DHS shall coordinate biennial reviews in cooperation with the Recipient during the Project Period to provide guidance on how the research and education programs need to evolve to align with the needs of the Homeland Security Enterprise consistent with the COE mission. The biennial review evaluates the Center's long-term strategy, relevance of the research and education to DHS mission needs and technology gaps, stakeholder engagement, research quality, outreach efforts and management of the activities funded under this Award. The DHS Program Officer will select a review panel of subject matter experts representing government, industry and academia for the biennial review.

5. DHS coordination with the Recipient will include, but is not limited to:
   a. Providing strategic input as necessary on an ongoing basis;
   b. Coordinating research and development activities that support the national research agenda; and
   c. Creating awareness and visibility for this program.

6. DHS may modify this Award to support additional research projects funded by DHS or other sources provided that these projects meet three conditions:
   a. Are research for a public purpose that addresses homeland security research priorities;
   b. Fall within scope of the grant or cooperative agreement; and
   c. Conform to federal assistance agreements (grant and cooperative agreement) guidelines.

7. DHS employees may co-author publications with COE researchers. Any publication co-authored by DHS staff shall be subject to DHS's publications approval process prior to dissemination of the publication as required under Item 12 in Section A.

8. DHS shall review and provide comments on the Recipient's Information Protection Plan as required under Item 14 in Section A.

9. DHS shall review and provide comments on the Recipient's Research Safety Plan as required under Item 16 in Section A.

10. DHS may create a Federal Coordinating Committee that provides guidance and direction to the DHS Program Officer regarding the Recipient's research plan.

11. DHS may invite subject matter experts, end users, or stakeholders to assist in evaluating the Center's annual workplan, annual meetings, or other events for the purpose of reviewing project quality and/or providing relevant operational perspectives.

12. DHS shall facilitate initial engagement with Homeland Security Enterprise stakeholders, but recipient is expected to maintain ongoing engagement for research areas of interest to the stakeholders.

C. AMENDMENTS AND REVISIONS

1. Budget Revisions.

a. Transfers of funds between direct cost categories in the approved budget when such cumulative transfers among those direct cost categories exceed ten percent of the total budget approved in this Award require prior written approval by the DHS Grants Officer.

b. The Recipient shall obtain prior written approval from the DHS Grants Officer for any budget revision that would result in the need for additional resources/funds.

c. The Recipient is not authorized at any time to transfer amounts budgeted for direct costs to the indirect costs line item or vice versa, without prior written approval of the DHS Grants Officer.

2. Extension Request.

a. Extensions to the Period of Performance can only be authorized in writing by the DHS Grants Officer.

b. The extension request shall be submitted to the DHS Grants Officer sixty (60) days prior to the expiration date of the performance period.

c. Requests for time extensions to the Period of Performance will be considered, but will not be granted automatically, and must be supported by adequate justification to be processed. The justification is a written explanation of the reason or reasons for the delay; an outline of remaining resources/funds available to support the extended Period of Performance; and a description of performance measures necessary to complete the project. Without performance and financial status reports current and justification submitted, extension requests shall not be processed.

d. DHS has no obligation to provide additional resources/funding as a result of an extension.

D. EQUIPMENT

1. Title to equipment acquired by the Recipient with federal funds provided under this Award shall vest in the Recipient, subject to the conditions pertaining to equipment in the 2 C.F.R. Part 200.

2. Prior to the purchase of Equipment in the amount of $5,000 or more per unit cost, the recipient must obtain the written approval from DHS.

3. For equipment purchased with Award funds having a $5,000 or more per unit cost, the Recipient shall submit an inventory that will include a description of the property; manufacturer model number, serial number or other identification number; the source of property; name on title; acquisition date; and cost of the unit; the address of use; operational condition of the property; and, disposition data, if applicable. This report will be due with the Final Progress Report 90 days after the expiration of the project period, and emailed to DHS-GrantReports@hq.dhs.gov.

E. FINANCIAL REPORTS

1. (Annual) Federal Financial Reports. The Recipient shall submit a Federal Financial Report (SF425) to the DHS Grants Officer no later than ninety (90) days after the end of the budget period end date. The report shall be emailed to DHS-GrantReports@hq.dhs.gov and include the grant program name and number in the subject line.

2. Final Federal Financial Report. The Recipient shall submit the final Federal Financial Report (SF425) to the DHS Grants Officer no later than ninety (90) days after the end of the Project Period end date. The report shall be emailed to DHS-GrantReports@hq.dhs.gov and include the grant program name and number in the subject line.

3. Quarterly Federal Financial Reports (Cash Transaction). The Recipient shall submit the Federal Financial Report (SF425) Cash Transaction Report to the Department of Health and Human Services, Payment Management System. Quarterly Cash Transaction reports shall be submitted no later than 1/30, 4/30, 7/30, and 10/30.

F. PAYMENT

The Recipient shall be paid in advance using the U.S. Department of Health and Human Services/Payment Management System, provided it maintains or demonstrates the willingness and ability to maintain procedures to minimize the time elapsing between the transfer of the funds from the DHS and expenditure disbursement by the Recipient. When these requirements are not met, the Recipient will be required to be on a reimbursement for costs incurred method.

Any overpayment of funds must be coordinated with the U.S. Department of Health and Human Services/Payment Management System.

G. PERFORMANCE REPORTS

1. Annual Performance Reports. The Recipient shall submit annual performance reports to the DHS Grants Officer for review and acceptance by DHS as a condition for receiving further annual funding increments. Annual performance reports are due no later than ninety (90) days after the end of the Center's budget period of each year. Annual reports must provide a summary of the activities conducted during the prior budget year. The report shall be emailed to DHS-GrantReports@hq.dhs.gov and include the grant program name and number in the subject line.

a. Performance reports must provide information on the overall progress of the Center. These reports shall include:

i. Summary reports on the Center's strategic vision and activities;

ii. Budget information categorized by both object class and project.
iii. Performance reports on each Center Project to include:
- o Explanation of any changes from the initially approved workplan
- o Progress against each milestone and explanation of why milestones were not reached
- o Unanticipated problems and plans for addressing them; and
- o Information on how project outcomes will advance or impact current technologies or capabilities.

iv. Budget information categorized by both object class and project.
v. If applicable, include a certification that no patentable inventions were created during the budget period.
vi. Updates to the Center's Information Protection Plan and Researcher Safety Plan as needed.

b. If the performance report contains any information that is deemed proprietary, the Recipient will denote the beginning and ending of such information with the following heading:
******PROPRIETARY INFORMATION******

2. Final Performance Report. The Recipient shall submit the Final COE Performance Report to the DHS Grants Officer and DHS Program Officer no later than ninety (90) days after the expiration of the Project Period (See Section H). The report shall be emailed to DHS-GrantReports@hq.dhs.gov and include the grant program name and number in the subject line.

a. The Final COE Performance Report shall include:
i. An executive summary and final summary abstracts for each sub-project across all years of the period of performance.
ii. Address the areas identified above in the annual report section.

H. PERIOD OF PERFORMANCE

The Period of Performance is the Project Period approved for the supported activity and is comprised of one or more Budget Periods as reflected on the Notice of Award cover page.

1. Project Period. The Project Period shall be for approximately 5 years from July 1, 20XX through June 30, 20XX of the following year. An exception is made for the first performance period, which will run from the date of award to June 30 of the following year. Subsequent years' funding is contingent on acceptable performance, as determined by the Department of Homeland Security's (DHS's), acceptance and approval of each non-competing continuation application, and the availability of the next year's annual DHS appropriations. The Recipient shall only incur costs or obligate funds within the Project Period for approved activities.

2. Budget Period. The Budget Period shall be for a period of twelve months, from July 1, 20XX through June 30, 20XX.

a. Additional funding will be provided for subsequent Budget Periods of the project, contingent on all of the following:
i. Acceptable performance of the project as determined by the DHS under this Award;
ii. Acceptance and approval by the DHS of each noncompeting continuation application;
iii. Acceptance and approval by the DHS of each previous Annual Performance Report and
iv. Subject to the availability of appropriated funds.

3. Non-Competing Continuation Requirements.

a. Ninety (90) days prior to the expiration date of each budget period, the Grants Officer will request submission of the annual incremental funding request details via Grants.gov website. The Recipient shall submit a non-competing continuation application to request the next Budget Period's incremental funding and a separate request for any possible carryover of prior year funds.

The non-competing continuation application shall include:

i. An annual project work plan as described in Article A, Item 3

ii. Carryover of Funds. Recipients are required to submit a separate Carryover Application for the unobligated balances remaining from funds awarded in one budget period to be carried over to the next succeeding budget period. This submission is due to the DHS Grants Officer and DHS Program Manager 90 days prior to budget period expiration (e.g., March 31) and is a best estimate at the budget period expiration from the recipient (lead university and all sub-recipients). The Program Officer will review the Carryover justification, in consultation with the DHS Grants Officer, and provide input to the Grants Officer that the justification is reasonable and the carryover funds should be used to complete any objectives which remain unmet from the prior budget period. Requests for carryover of funds from one Budget Period to the next Budget Period shall be submitted separately via email to the DHS Grants Officer with an SF 424 (R&R) face page and shall include:

1. A brief description of the projects or activities and milestones to be carried forward,
2. The amount of funds to be carried over,
3. The reason the projects or activities were not completed in accordance with the project time line, and
4. The impact on any future funding for the projects or activities.

The DHS Program Officer will review the continuation application submission and provide input to the Grants Officer as to whether the Continuation Application is consistent with the approved work plan.

I. PRIOR APPROVAL REQUIRED

The Recipient shall not, without the prior written approval of the DHS, request reimbursement, incur costs or obligate funds for any purpose pertaining to the operation of the project, program, or activities prior to the approved Budget Period.

ARTICLE II. GENERAL TERMS AND CONDITIONS

A. ACCESS TO RECORDS.

The Recipient shall retain financial records, supporting documents, statistical records, and all other records pertinent to this Award for a period of 3 years from the date of submission of the final expenditure report. The only exceptions to the aforementioned record retention requirements are the following:

1. If any litigation, dispute, or audit is started before the expiration of the 3-year period, the records shall be retained until all litigation, dispute or audit findings involving the records have been resolved and final action taken.
2. Records for real property and equipment acquired with federal funds shall be retained for 3 years after final disposition.
3. The DHS Grants Officer may direct the Recipient to transfer certain records to DHS custody when he or she determines that the records possess long term retention value. However, in order to avoid duplicate recordkeeping, the DHS Grants Officer may make arrangements for the Recipient to retain any records that are continuously needed for joint use.

DHS, the Inspector General, Comptroller General of the United States, or any of their duly authorized representatives, have the right of timely and unrestricted access to any books, documents, papers, or other records of the Recipient that are pertinent to this Award, in order to make audits, examinations, excerpts, transcripts and copies of such documents. This right also includes timely and reasonable access to Recipient's personnel for the purpose of interview and discussion related to such documents. The rights of access in this award term are not limited to the required retention period, but shall last as long as records are retained.

With respect to sub-recipients, DHS shall retain the right to conduct a financial review, require an audit, or otherwise ensure adequate accountability of organizations expending DHS funds. Recipient agrees to include in any sub-award made under this Agreement the requirements of this award term (Access to Records).

B. COMPLIANCE ASSURANCE PROGRAM OFFICE TERMS AND CONDITIONS

The Compliance Assurance Program Office (CAPO) is comprised of the DHS Treaty Compliance Office (TCO), Export Control Group (ECG), and the DHS Regulatory Compliance Office (RCO). The Compliance Assurance Program Manager (CAPM) is the DHS official responsible for overseeing CAPO and implementing procedures to ensure that the Recipient and any Recipient institutions/collaborators under this Award comply with international treaties, federal regulations, and DHS policies for Arms Control Agreements, Biosafety, Select Agent and Toxin Security, Animal Care and Use, the Protection of Human Subjects, Life Sciences Dual Use Research of Concern, and Export Controls.

CAPO collects and reviews relevant documentation pertaining to this Award on behalf of the Compliance Assurance Program Manager. Additional guidance regarding the review process is provided in the following sections, along with contact information for the TCO, RCO, and ECG. This guidance applies to the Recipient and any/all Recipient institutions involved in the performance of work under this Award. The Recipient is responsible for ensuring that any/all Recipient institutions and collaborators comply with all requirements and submit relevant documentation, as outlined in sections C – G below, for work being performed under this Award.

C. TREATY COMPLIANCE FOR BIOLOGICAL AND CHEMICAL DEFENSE EFFORTS

The Recipient and any Recipient institution shall conduct all biological and chemical defense research, development, and acquisition projects in compliance with all arms control agreements of the U.S., including the Chemical Weapons Convention (CWC) and the Biological Weapons Convention (BWC). DHS Directive 041-01, *Compliance With, and Implementation of, Arms Control Agreements* , requires all such projects to be systematically evaluated for compliance at inception, prior to funding approval, whenever there is significant project change, and whenever in the course of project execution an issue potentially raises a compliance concern.

1. Requirements for Initial Treaty Compliance Review. To ensure compliance with DHS Directive 041-01, for each new biological and/or chemical defense-related effort (including paper and modeling studies) to be conducted under this Award, the Recipient must submit the following documentation for compliance review and certification prior to funding approval: a completed Treaty Compliance Form (TCF), which includes a Project Summary; a BWC Checklist; and/or a CWC Checklist.

2. Requirements for Ongoing Treaty Compliance Review. To ensure ongoing treaty compliance for approved biological and/or chemical defense-related efforts funded through this Award, the Recipient must submit the following documentation for review and approval prior to any significant project change and/or whenever in the course of project execution an issue potentially raises a compliance concern: a detailed description of the proposed modification, and written request for approval.

The Recipient should contact the Treaty Compliance Office (TCO) at treatycompliance@hq.dhs.gov to obtain the TCF template, submit the completed Form, or request additional guidance regarding TCO documentation and review requirements, as applicable to (1) new biological and/or chemical defense-related efforts, or (2) modifications to previously approved efforts. The TCO will review all submitted materials and provide written confirmation of approval to initiate work to the Recipient once the treaty compliance certification process is complete. The Recipient and any Recipient institution shall not initiate any new activities, or execute modifications to approved activities, until receipt of this written confirmation.

D. REGULATORY COMPLIANCE FOR BIOLOGICAL LABORATORY WORK

The Recipient and any Recipient institution shall conduct all biological laboratory work in compliance with applicable federal regulations; the latest edition of the CDC/NIH Biosafety in Microbiological and Biomedical Laboratories; DHS Directive 066-02, Biosafety; and any local institutional policies that may apply for Recipient institution facilities performing work under this Award. The Regulatory Compliance Office (RCO) will review the submitted Treaty Compliance Form (TCF) for planned work under this Award to determine the applicability of the requirements outlined in this section. The Recipient must contact the RCO at STregulatorycompliance@hq.dhs.gov for guidance on the requirements, and then submit all required documentation based on RCO guidance, prior to the initiation of any biological laboratory work under this Award.

1. Requirements for All Biological Laboratory Work. Biological laboratory work includes laboratory activities involving: (1) recombinant DNA or 'rDNA'; (2) Biological Select Agents and Toxins or 'BSAT'; or (3) biological agents, toxins, or other biological materials that are non-rDNA and non-BSAT. Each Recipient and any Recipient institution to be conducting biological laboratory work under this Award must submit copies of the following documentation, as required by the RCO after review of the TCF(s), for review prior to the initiation of such work:

a. Research protocol(s), research or project plan(s), or other detailed description of the biological laboratory work to be conducted;
b. Documentation of project-specific biosafety review for biological laboratory work subject to such review in accordance with institutional policy;
c. Institutional or laboratory biosafety manual (may be a related plan or program manual) for each facility/laboratory to be involved in the biological laboratory work;
d. Biosafety training program description (should be provided as available in existing policies, plans, and/or manuals for all relevant facilities/laboratories where work is conducted;

e. Documentation of the most recent safety/biosafety inspection(s) for each facility/laboratory where the biological laboratory work will be conducted;
f. Exposure Control Plan, as applicable;
g. Documentation from the most recent Occupational Safety and Health Administration (OSHA) or State Occupational Safety and Health Agency inspection report; a copy of the OSHA Form 300 *Summary of Work Related Injuries and Illnesses* or equivalent, for the most recent calendar year; and documentation of any OSHA citations or notices of violation received in the past 5 years; and
h. Documentation from the most recent U.S. Department of Transportation (DOT) inspection report; and documentation of any DOT citations or notices of violation received in the past 5 years.

2. Requirements for Research Involving Recombinant DNA (rDNA). Laboratory activities involving rDNA research are defined by the *NIH Guidelines for Research Involving Recombinant DNA Molecules, "NIH Guidelines"* . Each Recipient and any Recipient institution shall conduct all rDNA work in compliance with the NIH Guidelines. In addition to the documentation referenced in Section B.1 above, each facility conducting research activities involving rDNA under this Award must submit copies of the following documentation to the RCO for review prior to the initiation of such activities:

a. Institutional Biosafety Committee (IBC) Charter, and/or other available documentation of IBC policies and procedures;
b. Most recent Office of Biotechnology Activities (OBA) acknowledgement letter of the annual IBC Report;
c. IBC-approved rDNA research protocol(s); and
d. Documentation of final IBC approval for each rDNA research protocol and all subsequent renewals and amendments as they occur

3. Requirements for Activities Involving Biological Select Agents and Toxins (BSAT). Planned activities involving the possession transfer, and/or use of BSAT must be reviewed by the RCO prior to initiation. This requirement also applies to activities involving select toxins that fall below the Permissible Toxin Limits, both at facilities registered with the National Select Agent Program and at unregistered facilities. Each Recipient and any Recipient institution shall conduct all BSAT work in compliance with all applicable regulations, including 42 C.F.R. § 73, 7 C.F.R. § 331, and 9 C.F.R. § 121, related entity- and laboratory-specific policies and procedures, and DHS Directive 026-03, *Select Agent and Toxin Security* . In addition to the documentation referenced in Section B.1 above, each facility conducting activities involving BSAT under this Award must submit copies of the following documentation to the RCO for review prior to the initiation of such activities:

a. Current APHIS/CDC Certificate of Registration;
b. Most recent APHIS/CDC inspection report(s), response(s), and attachment(s);
c. Current versions of the Biosafety, Security, and Incident Response Plans required and reviewed under the Select Agent Regulations; and
d. Documentation of the most recent annual BSAT facility inspection, as required of the Responsible Official under the Select Agent Regulations.

The Recipient should contact the RCO at STregulatorycompliance@hq.dhs.gov to obtain the RCO Documentation Request Checklist, submit documentation, or request more information regarding the DHS RCO documentation and compliance review requirements. The RCO will provide written confirmation of receipt of all required documentation to the designated Point(s) of Contact. The RCO will evaluate the submitted materials, along with available documentation from any previous reviews for related work at the Recipient and Recipient institution. Additional documentation may be required in some cases and must be submitted upon request. The RCO will review all submitted materials and provide written confirmation to the Recipient once all requirements have been met.

RCO review of submitted materials may determine the need for further compliance review requirements, which may include documentation-based and on-site components. The Recipient, and any Recipient institutions conducting biological laboratory work under this Award, must also comply with ongoing RCO compliance assurance and review requirements, which may include but are not limited to initial and periodic documentation requests, program reviews, site visits, and facility inspections.

The Recipient must promptly report the following to the RCO, along with any corrective actions taken: (1) any serious or continuing biosafety or BSAT program issues as identified by the APHIS/CDC National Select Agent Program, other compliance oversight authorities, or institutional-level reviews (e.g., IBC or equivalent, laboratory safety/biosafety inspections); (2) any suspension or revocation of the APHIS/CDC Certificate of Registration; and (3) any for-cause suspension or termination of biological, rDNA, or BSAT activities at the laboratories/facilities where DHS-sponsored work is conducted.

Foreign Contractors/Collaborators and U.S. Institutions with Foreign Subcomponents. Foreign organizations (including direct Contractors, Subcontractors, Grant Recipients, Sub-recipients, and subcomponents or collaborating partners to U.S. Recipients) are subject to applicable DHS requirements for biological laboratory activities. All entities involved in activities under this Award must comply with applicable national and regional/local regulations, and standards and guidelines equivalent to those described for U.S. institutions (e.g., *BMBL* and *NIH Guidelines*). The Recipient must provide RCO documentation sufficient to illustrate this compliance. The RCO will evaluate compliance measures for these institutions on a case-by-case basis. The Recipient must not initiate work nor provide funds for the conduct of biological laboratory work under this Award without RCO's formal written approval.

E. RESEARCH INVOLVING ANIMALS

The Recipient and any Recipient institution shall conduct all research involving animals under this Award in compliance with the requirements set forth in the Animal Welfare Act of 1966 (P.L. 89-544), as amended, and the associated regulations in 9 C.F.R., Chapter 1, Subchapter A; the Public Health Service (PHS) Policy on Humane Care and Use of Laboratory Animals (which adopts the "U.S. Government Principles for the Utilization and Care of Vertebrate Animals used in Testing, Research, and Training", 50 FR 20864, May 20, 1985); the National Research Council (NRC) Guide for the Care and Use of Laboratory Animals; the Federation of Animal Science Societies (FASS) Guide for the Care and Use of Agricultural Animals in Agricultural Research and Teaching; and any additional requirements set forth in the DHS Directive for the Care and Use of Animals in Research (026-01). Each Recipient and any Recipient institution planning to perform research involving animals under this Award must comply with the requirements and submit the documentation outlined in this section.

1. Requirements for Initial Review of Research Involving Animals. Research Involving Animals includes any research, experimentation, biological testing, and other related activities involving live, vertebrate animals, including any training for such activities. Each facility conducting research involving animals under this Award must submit copies of the following documentation to the RCO for review **prior to the initiation of such research**:

a. Institutional Animal Care and Use Committee (IACUC)-approved animal research protocol(s), including documentation of IACUC approval, any protocol amendments, and related approval notifications;

b. Public Health Service (PHS) Animal Welfare Assurance, including any programmatic amendments, and the most recent NIH Office of Laboratory Animal Welfare (OLAW) approval letter for each Recipient and Recipient institution; OR DHS Animal Welfare Assurance, if the Recipient is not funded by the PHS and does not have a PHS Assurance on file with OLAW. Any affiliated IACUCs must be established under the same requirements as set forth in the PHS Policy;

c. Most recent IACUC semiannual program review and facility inspection reports covering all relevant facilities/laboratories involved in DHS-funded work; and

d. Most recent Association for Assessment and Accreditation of Laboratory Animal Care (AAALAC) inspection report(s) for AAALAC-accredited institution(s) housing and/or performing work involving animals under this Award.

All documentation, as well as any questions or concerns regarding the requirements referenced above, should be submitted to the RCO at STregulatorycompliance@hq.dhs.gov. Additional documentation may be required in some cases and must be submitted upon request. The RCO will review all submitted materials and provide written confirmation to the Recipient once all documentation requirements have been met. Upon receipt of this written confirmation, the Recipient may initiate approved animal research projects under this Award, but must address any potential compliance issues or concerns identified by the RCO. Research involving the use of nonhuman primates or international collaborations involving animal research will require more extensive review prior to approval, and must not begin under this Award without first obtaining a formal certification letter from the RCO.

The Recipient, as well as any Recipient institution and partner institutions conducting animal research under this Award, shall also comply with ongoing RCO compliance assurance functions, which may include but are not limited to periodic site visits, program reviews, and facility inspections.

2. Requirements for Ongoing Review of Research Involving Animals. For ongoing animal research activities, each Recipient and any Recipient institutions must submit updates to the RCO regarding any amendments or changes to (including expiration, renewal, or completion of) ongoing animal protocols as they occur, and may be required to submit annual updates regarding the ACU program at Recipient and Recipient institutions. Annual updates may include, but are not limited to, the IACUC semiannual (program review and facility inspection) reports, the USDA inspection report, and the most recent AAALAC inspection report, as applicable.

The Recipient must promptly report the following to the RCO, along with any corrective actions taken: (1) any serious or continuing noncompliance with animal care and use regulations and policies adopted by DHS (as referenced above); (2) any change in AAALAC accreditation status; (3) any USDA Notice of Violation; and (4) IACUC suspension of any animal research activity conducted under this Award.

Foreign Contractors/Collaborators and U.S. Institutions with Foreign Subcomponents. Foreign organizations (including direct Contractors, Subcontractors, Grant Recipients, Sub-recipients, and subcomponents or collaborating partners to U.S. Recipients) are subject to all DHS requirements for work involving animals. All entities involved in activities under this Award must comply with applicable national and regional/local regulations, and standards and guidelines equivalent to those described for U.S. institutions (e.g., Title 9, C.F.R, Chapter 1, Subchapter A; Public Health Service Policy on Humane Care and Use of Laboratory Animals; the Guide for the Care and Use of Laboratory Animals; and the Guide for the Care and Use of Agricultural Animals in Agricultural Research and Teaching). The Recipient must provide RCO documentation sufficient to illustrate this compliance. The RCO will evaluate compliance measures for these institutions on a case-by-case basis to determine their sufficiency. The Recipient must not initiate nor provide funds for the conduct of work involving animals at foreign institutions under this Award without formal written approval from the RCO.

F. LIFE SCIENCES DUAL USE RESEARCH OF CONCERN (DURC)

The Recipient and any Recipient institutions shall identify, report, and conduct any research involving life sciences dual use research of concern (as defined by the United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern) in compliance with federal regulations, DHS Directive 026-08, *Oversight of Life Sciences Dual Use Research of Concern* , as well as any additional requirements set forth in related DHS policies and instructions.

G. RESEARCH INVOLVING HUMAN SUBJECTS

The Recipient and any Recipient institutions shall conduct all Research Involving Human Subjects in compliance with the requirements set forth in 45 C.F.R. § 46, Subparts A-D, DHS Directive 026-04, *Protection of Human Subjects* , and any related DHS policies and instructions prior to initiating any work with human subjects under this Award. Each Recipient and any Recipient institutions planning to perform research involving human subjects under this Award must submit the documentation outlined in this section for RCO review.

1. Requirements for Research Involving Human Subjects. Each facility conducting work involving human subjects under this Award is required to have a project-specific Certification of Compliance letter issued by the RCO. Each Recipient must submit the following documentation to the RCO for compliance review and certification prior to initiating research involving human subjects under this Award:

a. Research protocol, as approved by an Institutional Review Board (IRB), for any human subjects research work to be conducted under this Award;
b. IRB approval letter or notification of exemption (see additional information below on exemption determinations), for any human subjects research work to be conducted under this Award;

c. IRB-approved informed consent document(s) (templates) or IRB waiver of informed consent for projects involving human subjects research under this Award; and
d. Federal-wide Assurance (FWA) number from the HHS Office for Human Research Protections (OHRP), or documentation of other relevant assurance, for all Recipient institutions (including Sub-recipients) involved in human subjects research under this Award.

2. Exemptions for Research Involving Human Subjects. Exemption determinations for human subject research to be conducted under this Award should only be made by authorized representatives of (1) an OHRP-registered IRB, or equivalent, or (2) the RCO. Exemption determinations made by an OHRP-registered IRB, or equivalent, should be submitted to the RCO for review and record-keeping. Program Officers, principal investigators, research staff, and other DHS or institutional personnel should not independently make exemption determinations in the absence of an IRB or RCO review. DHS Program Officers (or institutions conducting human subjects' research under this Award) seeking an exemption determination from the RCO should submit a request to STregulatorycompliance@hq.dhs.gov that includes the following:

a. Research protocol or detailed description of planned activities to be conducted under this Award.

b. Identification of the exemption category that applies to the project(s) to be conducted under this Award and explanation of why the proposed research meets the requirements for that category of exemption.

All documentation, as well as any questions or concerns regarding the requirements referenced above, should be submitted to the RCO at STregulatorycompliance@hq.dhs.gov. The submitted documentation will be retained by the RCO and used to conduct a regulatory compliance assessment. Additional documentation may be required in some cases to complete this assessment. The Recipient must provide this documentation upon request, and address in writing any compliance issues or concerns raised by the RCO before a certification letter is issued and participant enrollment can begin under this Award. The RCO will review all submitted materials and provide written confirmation to the Recipient once all documentation requirements have been met.

The Recipient and any Recipient institution shall submit updated documentation regarding ongoing research involving human subjects, as available and prior to the expiration of previous approvals. Such documentation includes protocol modifications, IRB renewals for ongoing research protocols ("Continuing Reviews"), and notifications of study completion.

The Recipient must promptly report the following to the RCO, along with any corrective actions taken: (1) any serious or continuing noncompliance with human subjects research regulations and policies adopted by DHS (as referenced above); and (2) suspension, termination, or revocation of IRB approval of any human subjects research activities conducted under this Award.

Foreign Contractors/Collaborators and U.S. Institutions with Foreign Subcomponents. Foreign organizations (including direct Contractors, Subcontractors, Grant Recipients, Sub-recipients, and subcomponents or collaborating partners to U.S. Recipients) are subject to all DHS and RCO requirements for research involving human subjects. All entities involved in activities under this Award must comply with applicable national and regional/local regulations, and standards and guidelines equivalent to those described for U.S. institutions (e.g., 45 C.F.R. § 46, including all Subparts, as relevant). The RCO will evaluate compliance measures for these institutions on a case-by-case basis to determine their sufficiency. The Recipient must not initiate nor provide funds for the conduct of work involving human subjects at foreign institutions under this Contract without formal written approval from the RCO.

H. COMPLIANCE WITH U.S. EXPORT CONTROLS

Activities performed by the Recipient and any Recipient institution under this Award may or may not be subject to U.S. export control regulations. The Recipient and any Recipient institution shall conduct all such activities, to include any and all DHS-funded research and development, acquisitions, and collaborations in full compliance with U.S. export controls—to include the Export Administration Regulations (EAR), the International Traffic in Arms Regulations (ITAR), and the Office of Foreign Assets Control (OFAC) Regulations. The Recipient and any Recipient institution will ensure that all legal requirements for compliance with U.S. export controls are met prior to transferring commodities, technologies, technical data, or other controlled information to a non-U.S. person or entity. Upon DHS request, the Recipient and any Recipient institution must provide to CAPO documentation and any other information necessary to determine satisfaction of this requirement.

All documentation, as well as any questions or concerns regarding export controls, should be submitted to the RCO at exportcontrols@hq.dhs.gov.

I. CONTROLLED UNCLASSIFIED INFORMATION

The parties understand that information and materials provided pursuant to or resulting from this Award may be export controlled, sensitive, for official use only, or otherwise protected by law, executive order or regulation. The Recipient is responsible for compliance with all applicable laws and regulations. Nothing in this Award shall be construed to permit any disclosure in violation of those restrictions.

J. INTELLECTUAL PROPERTY RIGHTS

Patent rights.

The Recipient is subject to applicable regulations governing patents and inventions, including government-wide regulations issued by the Department of Commerce at 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements." The clause at 37 CFR 401.14 is incorporated by reference herein. All reports of subject inventions made under this Award should be submitted to DHS using the Interagency Edison system website at http://www.iedison.gov.

Data rights.

1. General Requirements. The Recipient grants the Government a royalty free, nonexclusive and irrevocable license to reproduce, display, distribute copies, perform, disseminate, or prepare derivative works, and to authorize others to do so, for Government purposes in:

a. Any data that is first produced under this Award and provided to the Government;

b. Any data owned by third parties that is incorporated in data provided to the Government under this Award; or

c. Any data requested in paragraph 2 below, if incorporated in the Award.

"Data" means recorded information, regardless of form or the media on which it may be recorded.

2. Additional requirement for this Award.

a. Requirement: If the Government believes that it needs additional research data that was produced under this Award, the Government may request the research data and the Recipient agrees to provide the research data within a reasonable time.

b. Applicability: The requirement in paragraph 2.a of this section applies to any research data that are:

i. Produced under this Award, either as a Recipient or sub-recipient;

ii. Used by the Government in developing an agency action that has the force and effect of law; and

iii. Published, which occurs either when:

1) The research data is published in a peer-reviewed scientific or technical journal; or

2) DHS publicly and officially cites the research data in support of an agency action that has the force and effect of law

c. Definition of "research data:" For the purposes of this section, "research data:"

i. Means the recorded factual material (excluding physical objects, such as laboratory samples) commonly accepted in the scientific community as necessary to validate research findings.

ii. Excludes:

1) Preliminary analyses;
2) Drafts of scientific papers;
3) Plans for future research;
4) Peer reviews;
5) Communications with colleagues;
6) Trade secrets;
7) Commercial information;
8) Materials necessary that a researcher must hold confidential until they are published, or similar information which is protected under law; and
9) Personnel and medical information and similar information the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, such as information that could be used to identify a particular person in a research study.

d. Requirements for sub-awards: The Recipient agrees to include in any sub-award made under this Agreement the requirements of this award term (Patent Rights and Data Rights) and **DHS Standard Terms and Conditions** award term (Copyright).

K. PROGRAM INCOME

Post-award program income:

In the event program income becomes available to the recipient post-award, it is the recipient's responsibility to notify the DHS Grants Officer to explain how that development occurred, as part of their request for guidance and/or approval. The Grants Officer will review approval requests for program income on a case-by-case basis; approval is not automatic. Consistent with the policy and processes outlined in 2 C.F.R. Part 200, pertinent guidance and options, as determined by the type of recipient and circumstances involved, may be approved by the Grant Officer.

If approval is granted, an award modification will be issued with an explanatory note in the remarks section of the face page, concerning guidance and/or options pertaining to the recipient's approved request. All instances of program income shall be listed in the progress and financial reports.

L. PUBLICATIONS.

1. Publications. All publications produced as a result of this funding which are submitted for publication in any magazine, journal, or trade paper shall carry the following:

a. Acknowledgement. "This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number, 2015-ST-061-CIRC01."

b. Disclaimer. "The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security."

Recipient agrees to include in any sub-award made under this Agreement the requirements of this award term (Publications).

2. Use of DHS Seal. Recipient shall acquire DHS's approval prior to using the DHS seal.

3. Enhancing Public Access to Publications. DHS requires that investigators submit their final, peer-reviewed, pre-publication manuscript upon acceptance for publication, to the DHS Program Officer, to be made publically available no later than 12 months after the official date of publication. Final, peer-reviewed manuscripts should be emailed to the DHS Program Officer in pdf format and will be publically posted to www.hsuniversityprograms.org in a manner consistent with copyright law. DHS Policy explicitly recognizes and upholds the principles of copyright. Authors and journals can continue to assert copyright in publications that include research findings from DHS-funded activities, in accordance with current practice. While individual copyright arrangements can take many forms, DHS encourages investigators to sign agreements that specifically allow the manuscript or software to be deposited with DHS for U.S. Government use after journal publication. Institutions and investigators may wish to develop particular contract terms in consultation with their own legal counsel, as appropriate. But, as an example, the kind of language that an author or institution might add to a copyright agreement includes the following: "Journal (or Software recipient) acknowledges that the Author retains the right to provide a final copy of the final manuscript or software application to DHS upon acceptance for Journal publication or thereafter, for public access purposes through DHS's websites or for public archiving purposes."

M. SITE VISITS

The DHS, through authorized representatives, has the right, at all reasonable times, to make site visits to review project accomplishments and management control systems and to provide such technical assistance as may be required. If any site visit is made by the DHS on the premises of the Recipient, or a contractor under this Award, the Recipient shall provide and shall require its contractors to provide all reasonable facilities and assistance for the safety and convenience of the Government representatives in the performance of their duties. All site visits and evaluations shall be performed in such a manner that will not unduly delay the work.

N. TERMINATION

Either the Recipient or the DHS may terminate this Award by giving written notice to the other party at least thirty (30) calendar days prior to the effective date of the termination. Failure to adhere to the terms and conditions may result in award termination. All notices are to be transmitted to the DHS Grants Officer via registered or certified mail, return receipt requested. The Recipient's authority to incur new costs will be terminated upon arrival of the date of receipt of the letter or the date set forth in the notice. Any costs incurred up to the earlier of the date of the receipt of the notice or the date of termination set forth in the notice will be negotiated for final payment. Closeout of this Award will be commenced and processed pursuant to 2 C.F.R. Part 200.

O. TRAVEL

Travel required in the performance of the duties approved in this Award must comply with 2 C.F.R. Part 200.

Foreign travel must be approved by DHS in advance and in writing. Requests for foreign travel identifying the traveler, the purpose, the destination, and the estimated travel costs must be submitted to the DHS Grants Officer 60 days prior to the commencement of travel.

P. GOVERNING PROVISIONS

The following are incorporated into this Award by this reference:

31 CFR 205	Rules and Procedures for Funds Transfers
2 C.F.R. Part 200	Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards
Application	Grant Application and Assurances dated 9/26/2014, as revised

Q. ORDER OF PRECEDENCE

1. 2 C.F.R. Part 200, “Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards.”

2. The terms and conditions of this Award

3. The Funding Opportunity, DHS-14-ST-061-COE-CIRC-001A, Critical Infrastructure Resilience

4. Application and Assurances dated 9/26/2014, as revised