The Department of Homeland Security (DHS)
Notice of Funding Opportunity (NOFO)
DHS Science and Technology Directorate (S&T)
Terrorism Prevention and Counterterrorism Research (TPCR) Center of Excellence (COE) – Center Partner

NOTE: If you are going to apply for this funding opportunity and have not obtained a Data Universal Numbering System (DUNS) number and/or are not currently registered in the System for Award Management (SAM), please take immediate action to obtain a DUNS Number, if applicable, and then to register immediately in SAM. It may take 4 weeks or more after you submit your SAM registration before your registration is active in SAM, then an additional 24 hours for Grants.gov to recognize your information. Information on obtaining a DUNS number and registering in SAM is available from Grants.gov at: http://www.grants.gov/web/grants/register.html Detailed information regarding DUNS and SAM is also provided in Section D of this NOFO, subsection, Content and Form of Application Submission.

Table of Contents

A. Notice of Funding Opportunity (NOFO) Description 4

Program Overview, Objectives, and Priorities 4

I. Program Overview 4
II. Priorities and Expectations for a COE 5
III. Objectives & Overarching Vision of the TPCR COE 7
IV. Application Project Narrative 16
V. Research and Workforce Development Themes, Topics, and Questions 20
VI. Performance Metrics 28

B. Federal Award Information 29

Award Amounts, Important Dates, and Extensions 29
Funding Instrument 30

C. Eligibility Information 30

Eligible Applicants 30
Eligibility Criteria 32
Cost Share or Match 32

D. Application and Submission Information 32

Submission Date and Other Key Dates and Times 32
Other Key Dates 33
Address to Request Application Package 33
Informational Webinar 34
Content and Form of Application Submission 34
Optional Forms 36
Other Submission Requirements 36
Unique Entity Identifier and System for Award Management (SAM) 37
Funding Restrictions 41
Indirect (Facilities & Administrative (F&A)) Costs 41

E. Application Review Information 41

Review and Selection Process 41
I. Scientific Quality Review (External Review) 41
II. DHS Relevancy Review (Internal DHS SMEs) 43
Application Evaluation Criteria 44
I. Research Project Evaluation Criteria 45
II. Workforce Development Project Evaluation Criteria: 47
III. Supplemental Financial Integrity Review 50

F. Federal Award Administration Information 51

Notice of Award 51
Work Plan Development Workshop 51
Administrative and National Policy Requirements 51
Reporting 52

G. DHS Awarding Agency Contact Information 52

H. Additional Information 53
Extensions 53
Disclosure 53
APPENDIX A: Terms and Conditions 56
APPENDIX B: Acronyms 95
APPENDIX C: End-to-End Approach 96
APPENDIX D: References for Themes, Topics and Questions 99
APPENDIX E: Checklist for Applicants 101

A. Notice of Funding Opportunity (NOFO) Description

Issued By

U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T)

Assistance Listings Number (formerly Catalog of Federal Domestic Assistance Number)

97.061

Assistance Listings Title (formerly CFDA Title)

Centers for Homeland Security

NOFO Title

DHS S&T Terrorism Prevention and Counterterrorism Research (TPCR) Center of Excellence (COE) - Partner

NOFO Number

DHS-19-ST-061-TPCR

Authorizing Authority for Program

Homeland Security Act of 2002, Section 308, as amended, P.L. 107-296.
Codified at 6 U.S.C. 188

Appropriation Authority for Program

Department of Homeland Security Appropriations Act, P.L. 116-6,

Title IV, Research, Development, Training, and Services.

Program Type

New

Program Overview, Objectives, and Priorities

I. Program Overview

The DHS S&T Office of University Programs (OUP) is requesting applications from accredited U.S. colleges and universities to lead a consortium of universities for a TPCR COE. OUP is also posting a separate NOFO for eligible applicants to submit single project proposals for consideration as a partner to this COE. Please see NOFO

Number DHS-19-ST-061-TPCR-Lead or 97.061 on https://www.grants.gov/ for directions on how to submit single project proposals. DHS will select qualified individual projects from applications received for either the Center Lead NOFO or the Center Partner NOFO, regardless of the institution that is awarded as lead institution. Principal Investigators that are already Partners under a Center Lead application may not submit the same application under this Partner NOFO.

The DHS COEs are university consortia that work closely with DHS Components and their partners to conduct research, develop and transition mission-relevant science and technology, educate the next generation of homeland security technical experts, and train the current workforce in the latest scientific applications. Each COE is led by an accredited U.S. college or university and involves multiple partners for varying lengths of time. COE partners include other academic institutions, commercial industry, DHS Components, Department of Energy National Laboratories and other Federally-Funded Research and Development Centers (FFRDCs), other federal agencies that have homeland security-relevant missions, state, local, tribal, territorial (SLTT) governments, non-profits, and first responder organizations. DHS envisions the COEs as long-term trusted partners that provide an array of resources to help DHS improve operations. OUP maintains both financial assistance and contract mechanisms for DHS to access COE capabilities. The COEs that make up the COE network are listed at https://www.dhs.gov/st-centers-excellence. The new Center will be a fully-integrated component of the COE network and will take advantage of the network's resources to develop mission-critical research, education, and technology transition programs.

Before DHS posts a COE NOFO on grants.gov, DHS subject matter experts (SMEs) identify priority research and workforce development themes, topics, and questions that will be the focus of the COE. Proposals responding to the NOFO are screened for eligibility (see "Eligibility Information"). Ineligible or non-responsive proposals receive no further consideration. Eligible and responsive proposals are reviewed by up to three separate review panels (see "Application Review Information," for a full description of how DHS reviews, rates and selects COE proposals). Each panel focuses on specific proposal characteristics (e.g., scientific quality, mission relevance, management capability) and provides ratings that determine which, if any, proposals are forwarded to the subsequent review panel. DHS may combine elements from several highly-rated proposals to create a new COE.

II. Priorities and Expectations for a COE

It is critical for university applicants to understand the roles and requirements of being a COE lead institution before submitting an application, and to craft a proposal to meet all of the requirements of a DHS COE. The DHS COEs are led by an accredited U.S. based academic institution, with research partners from the commercial sector, national laboratories, and state and local consortia that work closely with each other and with DHS Offices and Components to: conduct research, develop and transition mission-relevant science and technology, educate the next

generation of homeland security technical experts, and train the current workforce in the latest scientific applications. DHS COEs operate using a unique research management approach where researchers work alongside operational and decision-making personnel to find opportunities to use science and technology to enhance homeland security capabilities. The skill sets required to make a COE successful are more extensive than research expertise alone. COEs need to have the ability and commitment to communicate frequently with a variety of actors from federal staff, to attorneys, to university administrators, to the private sector. The COE team must demonstrate their commitment to develop a long-term trust-based partnership between universities and federal agencies; to do that, a range of skills is essential.

In addition to a multidisciplinary research team, COEs should include experts in finance, project management, education, training, outreach and marketing, intellectual property management, technology development, and technology transfer. Applicants should have an understanding of how to translate research to practice including intellectual property issues, licensing, the ability to work with transition partners, and an understanding of federal acquisition.

The COEs are 10-year partners with DHS and priorities will evolve during that period. DHS expects the COE leadership to end non-performing projects as soon as possible using a customer-focused research and development (R&D) framework, and move on to other priority projects within the scope of the portfolio. Managing a COE as an evolving portfolio of projects gives DHS and the COEs the flexibility to fail fast and adjust to fund new efforts with higher marginal benefit for homeland security.

The Center will be expected to construct a plan and schedule, describing the specific business steps needed to build an effective management team, execute subcontracts, identify data needs and sources of such data, establish intellectual property sharing agreements, and engage customers to refine proposals into a work plan. The Center will be required to have these elements in place within 6 months following award.

The DHS COEs are different from many other federally funded university centers, and DHS expects a lot more from them. Each COE lead institution must:

- Work closely with DHS and others on an on-going basis to formulate research projects so that those efforts are aligned with the most critical knowledge and technology gaps.
- Work with research teams to build appropriate stage-gate plans to manage research including literature reviews/technology scouting, test and evaluation; intellectual property, market assessment, etc.
- Place faculty and students (limited to U.S. citizens eligible for clearances) in operational agencies early and often, in order to develop solutions appropriate to complex homeland security problems.
- Build a nation-wide or world-wide network of academic and other SMEs in order to be able to access the best experts for each problem in short order.
- Replace researchers whose projects are not progressing as planned, and

establish a competitive process at regular intervals or as needed to replace projects that have ended.

- Develop detailed plans for transitioning research results into use, including plans to pursue intellectual property protections and to support the transfer of research to those capable of further developing the technology or service, i.e., commercial, government or FFRDC partners.

DHS funds the COEs through cooperative agreements, which provide support for research for general public purposes, yet enable substantial federal agency involvement in COE activities and research. OUP facilitates interactions between researchers, DHS SMEs and customers from the public and private sectors (i.e., homeland security practitioners). The goal of this hands-on management is to develop a trusting, sustained relationship between universities and DHS Components.

The COEs are expected to develop relationships and partnerships with DHS Components and the larger first responder community to provide targeted capabilities and education resources. OUP will work with COE management to formulate each COE's research and education projects, and to develop communication and transition strategies. Interactions commonly include COE-sponsored workshops that bring together diverse SMEs, industry representatives, and federal managers. DHS believes this frequent interaction is the most effective way to get the federal government's research investments into operational use by security, intelligence, and emergency response personnel. Only academic institutions that can embrace this type of close working relationship with industry and government security and intelligence agencies should apply for this funding opportunity.

The DHS mission requires that its operational Components [e.g., U.S. Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), Federal Emergency Management Agency (FEMA), Immigration and Customs Enforcement (ICE), U.S. Coast Guard (USCG), and the U.S. Secret Service (USSS)] be responsive to a wide range of constantly evolving homeland security challenges and threats, both natural and manmade. As a result, DHS priorities and operational challenges may change over the course of a COE's performance period. Therefore, COE research programs should be flexible enough to adapt to new homeland security challenges and priorities, while at the same time maintaining focus on their core research areas. DHS looks to COE leadership to maintain situational awareness of cutting edge research to inform the homeland security enterprise (HSE) of research futures, and to identify potential threats arising from, or to be mitigated by, novel technology.

III. Objectives & Overarching Vision of the TPCR COE

Protecting the American public from terrorism remains the highest mission priority of DHS. To fulfill this mission, DHS must develop and employ approaches to detect, deter, prevent and counter terrorism. DHS must also develop and hone key skillsets such as intelligence collection, analysis, and prevention programs. The TPCR COE will conduct a range of activities including basic and applied research, and education

and training initiatives to support and enhance DHS analytic efforts. DHS seeks research that explores the nature of countering terrorism operations from multiple perspectives including the adversaries' (threat) and that of Homeland security stakeholders (federal, SLTT government and private sector).

Terrorism, both at home and abroad, has great potential to degrade the security, infrastructure, and stability of the U.S. The diverse nature of the terrorist threat continues to evolve with rapid geopolitical, demographic and technological changes. The proliferation of social media and easy access to encrypted technology has created unforeseen opportunities for violent extremist groups and sympathizers that transcend national borders. Former DHS Secretary Kirstjen Nielsen has said, "changes in technology have made it easier for adversaries to plot attacks in general, to inspire and radicalize new followers, and to recruit beyond borders. The problem is compounded by the use of simple, 'do-it-yourself' terror tactics."[1] The widespread use of the internet and accessibility of information has allowed for the transfer of both terrorist resources as well as tactics, from cyber-attacks to simple improvised explosive devices (IEDs).

The terrorist threat globally is becoming more decentralized, and the threat of smaller-scale attacks by Homegrown Violent Extremists (HVEs) are on the rise. According to the U.S. House Homeland Security Committee, "The United States faces its highest Islamist terror threat environment since 9/11, and much of the threat now stems from individuals who have been radicalized at home."[2] We face varying threats of domestic-based "lone offenders" who are inspired by extremist ideologies, both domestic and internationally rooted, to radicalize to violence and commit acts of terrorism against Americans and the Nation. These threats come in multiple forms and, because of the nature of independent actors, may be hardest to detect. We must remain vigilant in detecting and countering these threats. The Nation must respond with innovative approaches to prevent the radicalization to violence and recruitment to terrorism, specifically here in the Homeland.

DHS seeks to counter terrorism by combining prevention, disengagement, and disruption efforts to break the cycle of recruitment, radicalization, and violence. These efforts must include partnerships across federal, SLTT governments, local community organizations, and the private sector. DHS must also anticipate emerging terrorist tactics and provide the HSE workforce with the skills and latest technology to identify vulnerabilities and trends.

The TPCR COE should describe how to integrate technologies and concepts into DHS operations to avoid, prevent, or stop a threatened or actual act of terrorism. Potential approaches include the utilization of innovative technologies (e.g., a new

[1] United States Congress Senate. Committee on the Judiciary. *Hearing on Oversight of the United States DHS. January 16, 2018.* 115th Cong. 2nd sess. Washington. https://www.dhs.gov/news/2018/01/16/written-testimony-dhs-secretary-kirstjen-nielsen-senate-committee-judiciary-hearing. Accessed on July 24, 2018.
[2] "The ISIS Terror Threat in America," Terror Threat Snapshot December 2016, Homeland Security Committee, https://www.hsdl.org/?view&did=797201.

approach to leverage available technology to identify patterns and indicators of terrorist activity among disparate types of data), optimized operational procedures, and a skilled workforce trained in the latest methods to identify and respond to terrorist threats.

Addressing Homeland Security Priorities

Please see Appendix – for the full list of relevant guidance. The following strategic documents guide or partially guide DHS operations and investment:

The proposed center will support part of DHS's primary mission defined in Section 101 of the Homeland Security Act of 2002 as "to prevent terrorist attacks within the United States; to reduce the vulnerability of the United States to terrorism." Key parts of legislation and directives since 2002 develop an increased emphasis on terrorism prevention and information sharing as well as enhanced engagement across all HSE partners.

Congress requires by law DHS review and report on the long term strategy and priorities of the Nation for homeland security every four years in its "quadrennial homeland security review." The *2014 Quadrennial Homeland Security Review (QHSR)*, reaffirms the enduring missions of homeland security as:

- **Prevent Terrorism and Enhance Security:** Protecting the American people from terrorist threats is our founding principle and our highest priority.
- **Secure and Manage Our Borders:** DHS secures the nation's air, land, and sea borders to prevent illegal activity while facilitating lawful travel and trade.
- **Enforce and Administer Our Immigration Laws:** The Department is focused on smart and effective enforcement of U.S. immigration laws while streamlining and facilitating the legal immigration process.
- **Safeguard and Secure Cyberspace:** Department works with industry and state, local, tribal and territorial governments to secure critical infrastructure and information systems. Analyzes and reduces threats and distributes warnings.
- **Strengthen National Preparedness and Resilience:** DHS provides the coordinated, comprehensive federal response in the event of a terrorist attack, natural disaster or other large-scale emergency while working with federal, state, local, and private sector partners to ensure a swift and effective recovery effort.[3]

The TPCR COE will directly align with the first homeland security mission, "Prevent Terrorism and Enhance Security," and will impact four of the five homeland security missions. *The 2014 QHSR* emphasizes securing the nation against the evolving terrorism of threat. This priority includes a strategic shift to focus on countering violent

[3] DHS. *The 2014 QHSR*. June 18, 2014. https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf

extremism (CVE), an increase in deterrence measures, and enhancing data integration and analysis.

In response to the 9/11 Commission, Congress outlined several actions to strengthen terrorism prevention. The *Implementing Recommendations of the 9/11 Commission Act of 2007*created the DHS Office of Intelligence and Analysis (I&A) in its current state and attempts to enhance information sharing across the federal government and with SLTT governments. The focus on strengthening efforts at the state and local level contributed to the development of fusion centers and establishment of grants to assist SLTT governments in terrorism prevention efforts.[4]

In 2011, the Federal Government enacted Presidential Policy Directive Eight (PPD-8): *National Preparedness*. Leveraging the importance of protecting critical infrastructure from terrorism, this directive was aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters.[5]

DHS S&T supports components in their efforts to identify threats, manage risks, and prevent terrorism on multiple levels, including identifying the appropriate resources that can contribute to the mission. In addition to law, DHS's mission is outlined by constantly evolving strategies across DHS and the federal government. Universities provide a unique perspective to terrorism prevention that can buttress the federal government's efforts.

In 2018, the White House issued the *National Strategy for Counterterrorism of the United States of America* that "prioritizes a broader range of non-military capabilities, such as our ability to prevent and intervene in terrorist recruitment, minimize the appeal of terrorist propaganda online, and build on societal resilience to terrorism."[6] Previous national strategies issued by the White House related to terrorism include the *National Strategy for Counterterrorism* issued in June 2011[7] and the *National Strategy for Combating Terrorism* issued in September 2006[8]. Both documents include a "whole-of-government" approach to counterterrorism and stress the importance of information sharing. Federal spending on CVE programs and policy, especially engaging at the local level, has become a focal point in the U.S. counterterrorism strategy.

---

[4] *Implementing Recommendations of the 9/11 Commission Act of 2007*. https://www.congress.gov/110/plaws/publ53/PLAW-110publ53.pdf.
[5] Presidential Policy Directive 8, National Preparedness (2011). https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.
[6] The White House, *National Strategy for Counterterrorism of the United States of America*, October 2018, https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf.
[7] The White House, *National Strategy for Counterterrorism*, June 2011. https://obamawhitehouse.archives.gov/sites/default/files/counterterrorism_strategy.pdf
[8] The White House. *National Strategy for Combating Terrorism.* https://georgewbush-whitehouse.archives.gov/nsc/nsct/2006/

Supporting the HSE

DHS has a central role in the Nation's security. An integrated DHS Intelligence Enterprise (IE) provides a decisive information advantage to the National leadership, DHS components, and our federal, SLTT government, private sector, and international stakeholders. CBP, TSA, I&A, U.S. Citizenship and Immigration Services (USCIS), FEMA, Cybersecurity and Infrastructure Security Agency (CISA) and ICE all have Component Intelligence Programs (CIP) that together form the DHS IE.[9] I&A provides DHS IE with timely intelligence and analysis, delivers intelligence from our SLTT partners to the DHS IE, and provides intelligence to DHS partners across the federal, SLTT governments, public and private sectors, as well as abroad.

DHS seeks R&D to equip DHS IE with intelligence capabilities and information it needs to detect threats and prevent terrorism. These organizations continue to adjust to the ever-changing nature of threats to the Homeland, including but not limited to adversarial communications and social media, threats to cyber infrastructure and identity, increased competencies among terrorists with the evolution of technology, as well as the use of low-tech tactics. DHS also focuses on a strategy of prevention, pursuing efforts to prevent radicalization and to identify vulnerabilities within DHS as well as information and communication approaches needed among DHS, federal government, SLTT and international bodies, and public and private sectors.

DHS and the Nation as a whole depend more and more on SLTT to counter terrorism. For terrorism strategy to work, the intelligence community (IC) must have valuable intelligence products, meaningful community engagement, and effective information sharing. Much of this activity lies in the fusion centers. The TPCR COE will research and develop technologies, protocols and capabilities to support DHS operational components as well as DHS's SLTT and private sector partners. DHS I&A places field personnel throughout the National Network of Fusion Centers. This network of more than 70 centers houses members from across federal agencies and SLTT governments.[10] I&A engages at the center level to gather intelligence as well as to support operations locally to assess, prevent, and/or respond to terrorism. The collaboration across fusion centers will support the DHS IE, IC, SLTT government, and the HSE at large to improve its operational capabilities and contribute to the Nation's layered defense.

DHS's Approach to COEs

Establishing a COE is a major and expensive effort that involves numerous individuals and organizations. There are important elements of standing up and operating a COE that every applicant should understand prior to applying:

[9] DHS Directive 264-01, *DHS IE,* June 28, 2013.
[10] https://www.dhs.gov/state-and-major-urban-area-fusion-centers

1. The overarching research areas that are the focus of all COE NOFOs, are driven by DHS's critical needs and enduring missions.
2. The research topics and questions contained in the NOFO are developed by the DHS Component agencies that have to implement those difficult missions.
3. Proposals for re-branded off-the-shelf research or pet projects will not survive DHS's rigorous review processes. DHS needs use-inspired, results-focused research that generates customized and innovative solutions
4. DHS's expectations for a COE will require university faculty to spend time working with customers in the field to better understand their needs, participate in project teams, execute the work necessary to protect intellectual property, and assess current technology and business markets.
5. DHS expects COE research to make a difference. Universities must actively manage COE research from a sound theoretical base, through methods development, data collection, testing and evaluation to operational use (i.e., End-to-End) in close partnership with DHS.
6. DHS will manage this COE carefully to provide value to operational users.

Research-based solutions generated by this Center must be innovative and well positioned to be transitioned into use by DHS customers. TPCR's research will be based on the HSE needs expressed by HSE practitioners in this NOFO. Research outcomes will include analytical methods, technologies, and knowledge products, e.g., best practices, resource guides, and case studies, which can be transitioned to the HSE workforce. DHS-sponsored researchers will produce new capabilities, and work with partners and stakeholders at all levels to test these capabilities in operational settings, and then take steps to make these solutions available and useful to agencies at all levels.

DHS funds research so that DHS can use the technology or knowledge to accomplish its mission. It is critical for researchers to understand how the Federal government does business. Selected COE Directors and Research Theme leaders must spend 1-3 months in DHS operational environments early in the research life cycle to understand both the technical and business requirements of DHS Components. This emphasizes the intellectual property, sustainability of technologies, security, and other legal requirements that Federal agencies must follow.

The Center will be expected to construct a plan and schedule describing the specific business steps needed to execute subcontracts, identify data needs and the acquisition of such data, establish intellectual property sharing agreements, and engage customers to refine proposals into a work plan. The Center will be required to have these elements in place within 6 months following award.

In order to avoid duplication of existing work, applicants must demonstrate a working knowledge of the scientific landscape, the quantitative methods, policies, and findings relevant to the topics in this NOFO through literature reviews, analysis of alternative approaches, and market-based assessments of related/ emerging technology.

Technology Transfer and Transition

As a mission agency, DHS funds projects with the ultimate goal of making homeland security practitioners more effective and efficient. Therefore, COEs are expected to have concrete objectives for how their research efforts will improve processes (e.g., operations, policies, decision-making), as well as impact homeland security (e.g., protect lives, property, and economies).

Transferring and transitioning research into the market requires a systematic understanding of customer needs, process and product design, and product and service development. The success of COEs depends on the ability to identify the needs of customers and quickly develop products and solutions that meet those needs. Delivering value to the customer is not simply a scientific problem, a design problem, or a market problem; it involves specific attention to each of the three general areas noted above.

DHS OUP utilizes a form of the stage-gate methodology to evaluate the performance of the Center and its projects. The stage-gate methodology, known as the industry and government standard, allows for reviewers to conduct evidence-based decision making that mitigates programmatic risk and enables program managers to monitor progress and make decisions.[11] At each stage, the Center and program managers evaluate the project status and ensure specific criteria such as: strategic fit, technical feasibility, customer acceptance, market opportunity, and financial opportunity are met before proceeding to the next stage of investment. Figure 1 below is a depiction of a generic form of the stage-gate process.

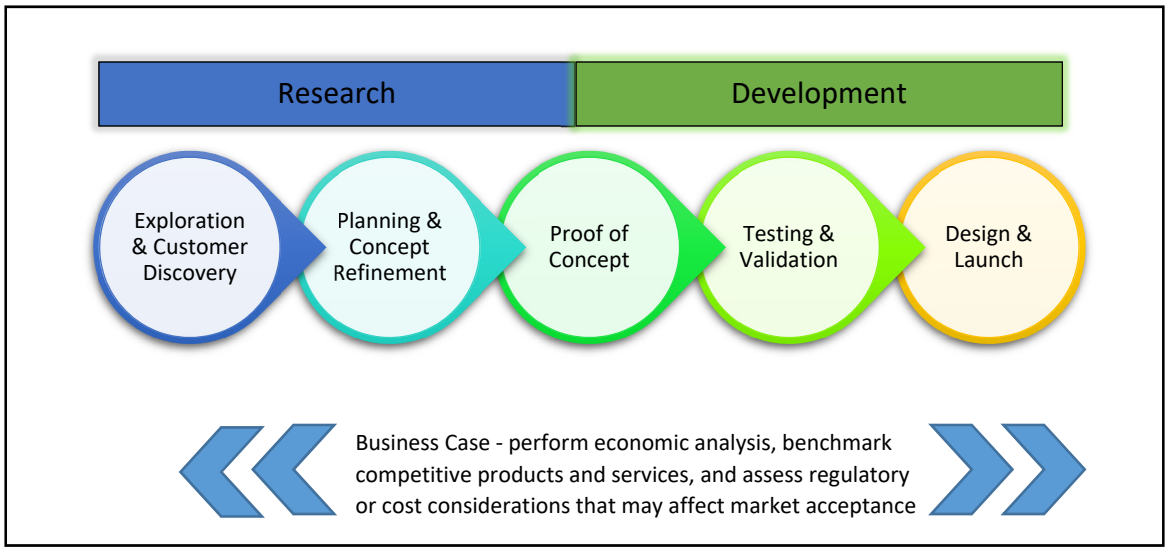


Figure 1: Stage-Gate Process

[11] "Innovation Process". Stage-Gate International. http://www.stage-gate.com/resources_stage-gate.php

The Center's strategy, and each project that is awarded as part of the Center, must propose and adhere to this stage-gate methodology shown in Figure 1, and as described in further detail below. The applicant must use this framework to describe the planning and execution of studies and developmental steps and the corresponding market and business steps necessary to complete the effort and transfer program outcomes into use. As a result of using this framework, each performing institution under the COE should be able to characterize the proposed research as a function of its technical maturity and market readiness at any given time.

Center Partner Applicants are required to submit a detailed proposal addressing the overall purpose of the project, an assessment of the state of the art, a description of the current operational environment, the scientific hypothesis and methodology for the study, data acquisition methods, advanced test and evaluation future needs, intellectual property management approach, and customer involvement in the project. Not all projects will result in commercializable outputs; however, at a minimum, all teams should describe how customers can access the program outputs, how the team will protect intellectual property, and what laws and regulations could impact the use of the program outputs.

Example stages of research are:

a) *Exploration and Customer Discovery*: the stage of research that generates hypotheses or theories through new and refined data analysis, produces observational findings, and creates other sources of research-based information. Efforts to explore customer gaps occurs early in the process. Projects in this stage should describe existing relevant standards, competing approaches, and provide an initial analysis of market conditions.
b) *Planning and Concept Refinement:* the stage of research that narrows project requirements. This includes conducting preliminary market and technical assessments, identifying customer needs and developing initial product specifications. Results from this stage of research may be used to inform the design of a study to test the efficacy of an idea/project. Efforts to define the market and identify and assess market drivers that will affect the transfer or adoption of the project outputs should be initiated.

Example stages of development are:

a) *Proof of Concept*: the stage of development where key technical challenges are initially addressed. Activities may include verifying product requirements and implementing and testing (typically in controlled contexts) approaches to those capability requirements. A technology transfer plan is typically developed that outlines efforts to understand commercialization needs.
b) *Testing and Validation:* the stage of development where a fully-integrated and working prototype is tested. Activities may include iteratively refining the prototype, testing in operational environments, and verifying that all

technical requirements are met. A technology transfer plan is typically ongoing in collaboration with the transfer partner(s). Stage results depict that a product embodiment is realizable.

c) *Final Design and Launch*: the stage of development where the product or service is finalized and made available for customer utilization. This likely requires the development of the corresponding business services that customers will use to buy, license, or otherwise acquire the product or service.

The DHS COEs must form teams of qualified professionals with the complementary skills necessary to transition research results from the research laboratory into the hands of homeland security customers. This includes understanding customer relations, conducting market assessments, managing intellectual property rights, considering commercialization, and assessing life cycle costs and needs (operations and maintenance and training).

The Center Lead Applicants are encouraged to develop proposals that include administrative support for facilitating transition, such as a staff member dedicated to assisting project leads with developing transition plans and the partnerships needed for successful transition, including with customers or the private sector. COEs are encouraged to leverage capabilities and resources offered through their university technology transfer offices in order to protect intellectual property by filing invention disclosures, patents, and licensing agreements. In addition, COEs are expected to participate in workshops, technology demonstrations, conferences, and other events hosted by OUP that may facilitate research and technology transition to customers.

COEs also should have specific objectives for transitioning their education efforts, which should include but are not limited to (1) capacity-building in disciplines relevant to homeland security, including at MSIs, (2) development and training of homeland security professionals for the current and future workforce through executive education programs, and (3) engagement of COE-supported students in research projects in applied or operational settings.

Historically, COEs that have effectively engaged stakeholders early in their activities have had great success. Examples of such engagement include:

- Inviting customers, such as DHS Component representatives or first responders, to work with principal investigators as they develop and implement their research and transition plans
- Conducting projects in coordination with DHS S&T technical divisions
- Inviting customers/stakeholders to participate in program/project reviews
- Holding workshops that bring researchers and homeland security practitioners together
- Partnering with private industry or business to co-develop technologies
- Embedding researchers or students in an operational environment
- Hosting an operational expert to participate in COE activities

Access to Data

Researchers and analysts must be able to obtain access to needed analytical products, relevant data, and open source and publicly available information. They also should anticipate interacting with homeland security partners and stakeholders and other SMEs. **Applicants must discuss any needs for unique or sensitive data, testing, or laboratory facilities that will be required to conduct the research, and how the applicant will ensure its researchers can access necessary data and facilities. See Data Acquisition and Management Plan in Appendix A.**

IV. Application Project Narrative

This section outlines requirements for the Project Narrative portion of the application package.

S&T expects any Partner institution awarded under this NOFO to become a fully integrated component of the COE. Partner applicants must select and clearly identify if their proposed project aligns with the Research Program or the Workforce Development Program. Applicants may only propose 1 project per proposal; however they may submit more than 1 proposal.

Applicants may propose projects lasting up to 2 years, with total budgets up to $500,000. However, Center projects are funded in 1-year increments. Subsequent to the first year, Center and project funding is dependent on successful performance in prior years, the relevance of project outcomes to current homeland security research priorities, and availability of funds. Multi-year project proposals should provide a summary of their long-term vision, timeframe, research and education outcomes, technology transfer or transition pathway, and potential real-world applications.

Applicants must also summarize a results communication and transition plan that outlines how the Partner will implement its project(s) and how they will be transitioned to user groups. Elements of the plan may include: project milestones; career development programs for research staff and students; identification of potential user groups; and a description of how the research results will be transitioned to DHS and other federal and state agencies.

Note: While not all Center projects will result in a final product that transitions to actual use by an end user, even earlier phase or exploratory research should still include a plan for disseminating results to end users/stakeholders in a form that enables end users/stakeholders to understand the potential applicability of the work and leverage outcomes to the maximum extent possible.

The following two sections outline requirements for 1) a Research project or 2) and Workforce and Professional Development project. Please select and clearly identify one area to propose a project.

1. **Research Project (5 pages)**

   Applicants should identify multidisciplinary, comprehensive approaches to address one of the research themes and topics outlined below in Section V "Research and Workforce Development Themes, Topics, and Questions". Applicants should explain why they selected these topics or questions, and describe a proposed method, metrics and outcomes to answer the relevant questions.

   Applicants should consider the maturity and state-of-the-art of the respective theories, technologies, and applications of the proposed areas of study when formulating their research portfolios.

   Applicants must include the following elements for each project:

   - Title
   - Principal investigator (name, title, school/business/non-profit)
   - Other key technical and project personnel supporting intellectual property and administrative tasks (name, title, school/business/non-profit)
   - Specifically identify which theme area and topic the project addresses **-** *if a proposed project falls under multiple themes/topics, identify those as primary, secondary, tertiary, etc.*
   - Project abstract
   - Goals and objectives of the research
   - Significant partners and their roles
   - Technical capability or knowledge gap this project addresses and what DHS Office aligns with the gap
   - How the work builds upon the state-of-the-art of the respective theories, technologies, and applications of the proposed areas of study
   - How the work represents an improvement (incremental or fundamental change) to the current operational posture being used
   - Theoretical approach, hypothesis to be tested
   - Methods for data collection and analysis
   - Methods section including study design
   - Data access plans should data be needed to execute the project
   - Technical technology performance metrics being tested (e.g. specificity, sensitivity, cost, etc.)
   - A year-by-year description of key milestones for the project for the first **two years**
   - Expected outputs and outcomes and how those outputs would be used
   - Transition pathway from lab to field to include identifying the key technical scientific and development steps necessary to transfer the technology to customers or commercialization partners.
   - The stages and gates that will be used to evaluate the technical progress and efforts to frame the business environment that the resulting outputs will effect.

- A year-by-year description of key milestones and the schedule for the project for the first **two years**
- Identification of commercial partners with the necessary complementary assets needed to realize the technology/approaches/concepts
- Total projected costs per year for two years and forecasted costs for up to five years
- Total projected costs per year for two years and forecasted cost for up to five years
- Relevant Citations

2. Workforce and Professional Development Project (5 pages)

The TPCR workforce and professional development program should include innovative initiatives to educate students in both theoretical and methodological underpinnings of the relevant disciplines, as well as practical applications for homeland security operations. As part of this, applicants should describe how they would embed their students and faculty, individually or in teams, with homeland security practitioners to conduct research, and foster opportunities for students to gain practical experience in homeland security-related professions. Applicants should also describe how they would integrate homeland security-related courses of study into existing science, technology, engineering, and mathematics (STEM) degree programs. Additionally, applicants should describe how their Center would provide and enhance technical education and training programs for HSE and DHS professionals, for example, at CBP, I&A, TSA, FEMA, or specific training Centers such as the Federal Law Enforcement Training Center (FLETC), and the Emergency Management Institute.

The overarching goals of a COE's workforce and professional development program are to:

- Build universities' capacity in security focused science, engineering, mathematics and analysis. Analysis includes business administration and policy analysis, as applied to homeland security-related challenges
- Strengthen the science, engineering, and analytical capabilities of the homeland security workforce, both current (professional development) and future (workforce development)
- Diversify the homeland security technical workforce by building homeland security science, engineering, and analysis capacity at Minority Serving Institutions (MSIs)
- Link students and researchers to practitioners in operational settings to develop more robust tools, technologies, and capabilities
- Teach students the business elements of transitioning emerging concepts into the commercial or government markets
- Develop and train existing homeland security professionals in science, engineering, and business administration disciplines for the current and future

workforce. Applicants should be familiar with the current methods by which Federal and State employees receive training.

Applicants must propose a project to align with "Research Theme Areas." DHS encourages proposals that include plans to integrate workforce development initiatives with DHS Components, other federal or state government agencies, and FFRDCs that have homeland security missions.

Education and workforce development program activities include:

- Developing undergraduate, graduate or professional career enhancing programs that support the COE's research program.
- Partnering with the private sector to create internships/co-ops for students in relevant areas to learn the business of managing science and developing products and services.
- Applying existing disciplines to homeland security through development of curricula, concentrations, minors, and certificates within established degree programs.
- Building homeland security capacity at MSIs. Please visit the following link for a list of accredited U.S. post-secondary institutions that meet the statutory criteria for identification as MSIs: http://www2.ed.gov/about/offices/list/ocr/edlite-minorityinst.html.
- Offering continuing education opportunities for first responders and homeland security professionals.
- Offering student internship, scholarship, or fellowship programs that provide homeland security research experience.
- Developing community college partnership programs to attract a diverse population of students and teachers into homeland security science and engineering disciplines.
- Offering homeland security related research opportunities to students.
- Embedding students and faculty in research projects at DHS or other operational agencies within the HSE.

Applicants must include the following elements for each project. Applicants may submit **up to five workforce and professional development projects total**.

- Title
- Principal investigator (name, title, school)
- Specifically identify which theme area and topic the project addresses **-** *if a proposed project falls under multiple themes/topics, identify those as primary, secondary, tertiary, etc.*
- Project abstract
- Goals and objectives of the project
- Significance of the proposed project to homeland security
- Capability or knowledge gap this project addresses

- Significant partners and their roles
- Relevant citations to express workforce needs of DHS
- A description of how the project aligns with and integrates into the Center's research program
- The stages and gates that will be used to evaluate technical and business/programmatic progress - **See "Technology Transfer and Transition" pages 12 - 16 of this NOFO for requirements on how to propose projects using the stage-gate methodology.**
- A description of how the Center would track specific measures of success, i.e., the number of students who graduate with homeland security relevant degrees; the number of students that participated in homeland security-related internships or research activities; the number of students that successfully obtained homeland security-related employment; the number of homeland security-related conference presentations given; the number of homeland security-related papers published; and/or the number of homeland security-related awards or prizes received
- A year-by-year description of key milestones for the project for the first two years
- Total projected costs per year for two years
- Letters of support from organizations agreeing to host interns (this may be included in the appendix of the application)

V. Research and Workforce Development Themes, Topics, and Questions

DHS expects this Center to focus on efforts to prevent terror attacks before they begin, including but not limited to radicalization and mobilization to violence. The *National Prevention Framework, 2nd Edition* issued by DHS in 2016 defines prevention's role in the National Preparedness System as, "The capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism."[12] These capabilities require both an understanding of counterterrorism operations as well as terrorism prevention strategies. DHS's *National Prevention Framework* applies to all levels of government, the private and nonprofit sectors, as well as individuals, and although the COE will engage directly with DHS components, projects may involve stakeholders at any of these levels as all play a role in preventing terrorism.

[12] DHS. *National Prevention Framework, 2nd Ed.* June 2016. https://www.fema.gov/media-library-data/1466017209279-83b72d5959787995794c0874095500b1/National_Prevention_Framework2nd.pdf

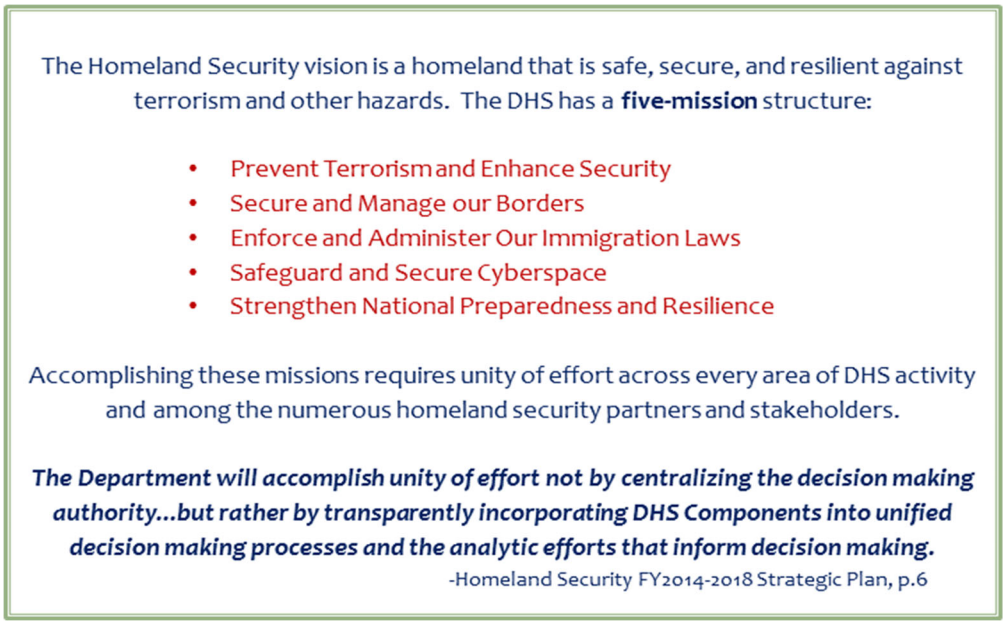


Figure 1: DHS Missions

TPCR shall aim to inculcate analytic rigor throughout the Department to support decision-making (see Figure 2, Prevent Terrorism and Enhance Security, Secure and Manage our Borders, and Safeguard and Secure Cyberspace). DHS also expects that the research outcomes will result in analytic methods, and changes in operations that are derived from statistically significant empirical evidence.

DHS seeks Center projects that include four broad themes within its research portfolio. The matrix below lists the theme areas and associated topics. DHS seeks a portfolio of projects addressing these theme/topic areas. The Center's proposal may include proposed projects focusing on one or more topic areas. These projects are deep dive exploratory research in an academic discipline and shall strive for breakthrough technological advances. The Center proposal shall also include projects that exhibit a combination of themes and topics. DHS encourages this multifaceted approach with a portfolio of projects for TPCR given the complex environment and range of issues included in the DHS mission set.

TPCR COE Themes & Topics	
Themes	**Topics**
(1) Nature of Counterterrorism Operations	1A. Terrorist Tactics, Techniques, and Procedures
	1B. Cyber and Tech Ops
	1C. Data Solutions (Including Big Data)
(2) **Nationwide Suspicious Activity Reporting Initiative**	
	3A. General Research to Practice

(3) Terrorism Prevention	3B. Evaluations of Existing Programs
(4) **Workforce Development**	

Table 1: TPCR COE Themes & Topics

After the Center identifies the DHS gap or challenge, the team should develop initial research questions using insights gained **from discussions with operational personnel**. Figure 3 depicts the TPCR themes in a Venn diagram, to illustrate DHS's recognition of overlap among the themes and topics). The Center should understand the role of each project in terms of its contribution to the Center's portfolio and how that portfolio advances the Center's mission. Understanding how project outputs could be combined to form new capabilities is critical. This requires COE leadership to build teams that contain the skill sets necessary to advance a project through its entire lifecycle where it will either lead to the successful transfer of a technology or knowledge product or will be terminated to allow the Center to move on to another area of investigation.

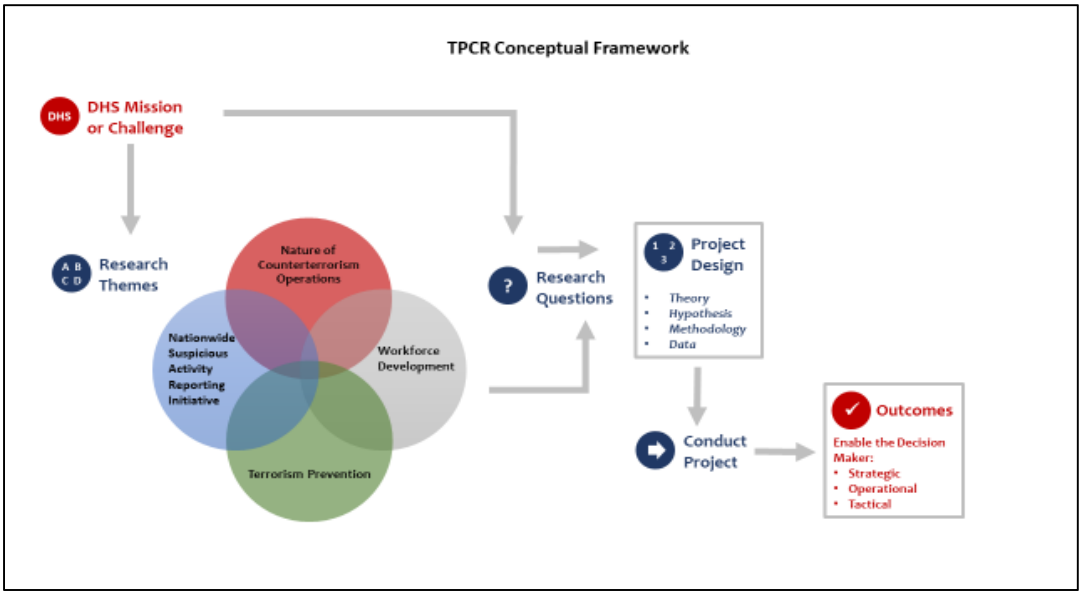


Figure 2: TPCR Conceptual Framework

Successful proposals shall ensure that the link between the anticipated outcomes of the research question will support homeland security decision-makers. Please see the full list of areas to address in the evaluation criteria IV Application Project Narrative of this NOFO. The project plan will outline how the investigators adhere to certain standards and the specific technologies that are being incorporated into the research project. For example, the selection of software tools, IT platforms, or other commercial products to be used in the course of the project.

Research Topics

Theme Area One: Nature of Counterterrorism Operations

DHS seeks research that explores the nature of countering terrorism operations from two perspectives—the adversary (threat) and that of Homeland security stakeholders (federal, state & local government/private sector). Research from the adversary perspective will analyze the terrorist tactics, techniques, and procedures, structures, capabilities and intentions in order to help develop and/or examine government courses of actions to reduce their capabilities to commit an act of terrorism. Research from the government perspective will seek to develop more effective partnerships for terrorism prevention among international, federal, SLTT and private sector entities, in part through after-action analysis of government response to terrorist incidents, including analysis of opportunities for prevention.

Below are representative research questions of interest to DHS by topic (questions not listed in priority order):

Topic 1A. Terrorist Tactics, Techniques, and Procedures (TTP)

- What are the primary factors in US-based terrorists' target selection, and how do we expect their target selection will evolve? What courses of action can the Homeland take to lower target's threat profiles?
- What additional existing or potential tools/assets/technology may further impede future terrorist attacks, without causing a significant financial or resource obligation to SLTT, international and private sector partners?
- What physical and cyber vulnerabilities may increase a target's attractiveness to a terrorist? What courses of action are available to decrease these vulnerabilities? Solutions may range from low tech, low financial, or resource requirements to existing commercial off the shelf products to innovative design solutions.

Topic 1B. Cyber Tech and Operations

- How could terrorists exploit emerging technologies for fundraising or transferring funds to or out of the US? Are terrorists increasing their use of virtual currencies? If not, what could lead them to use virtual currencies more, moving forward? If yes, what is the factual and methodological basis for this conclusion, and are there any deterrents or potential tools for tracking and exploiting these investments?
- How will the evolution of the Internet of Things (IoT) create potential vulnerabilities in terms of terrorist targeting? What can DHS do to mitigate those impacts without adversely impacting IoT development?
- How can we improve methods of lawfully intercepting and thwarting terrorist

communications as communications continue to shift toward end-to-end encryption?
- Regarding adversarial communications and social media, how do we identify and thwart self-propagating malware (bot) activity in or near real-time?

Topic 1C. Data Solutions (Including Big Data)

- How can we leverage AI and/or machine learning in assisting to identify terrorist content, actors, and activities?
- How can analysts fully leverage all available data in its various forms to identify patterns, signatures, and indicators of terrorist activity?
- What tools and competencies can be made available to analysts for fusing and integrating disparate data of interest? Are there any critical gaps that require future development to integrate disparate data?
- What types of data analytics can best support traditional CT analysis?
- What strategies (people, process, technologies) should DHS pursue in conjunction with its partners (SLTT, private sector, IC, and/or international community) for data management to enable machine learning and artificial intelligence capabilities? How do we develop high confidence data for supervised learning approaches and how do we provide sufficient data for unsupervised learning of machine learning algorithms?
- What strategies (people, process, technologies) should DHS pursue to provide analysts, operators and oversight (Office of General Counsel (OGC), Privacy, Office for Civil Rights and Civil Liberties (CRCL)) transparency in terms of how machine learning algorithms work and desired outcomes and compliance mechanisms to ensure that algorithms perform as intended (e.g. compliance)?

Theme Area Two: Nationwide Suspicious Activity Reporting Initiative

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a joint collaborative effort by DHS, the Federal Bureau of Investigation (FBI), and SLTT law enforcement partners. The NSI has concentrated on reporting delivered information that has supported FBI terrorism investigations and watchlisting by the Terrorist Screening Center.

The NSI is a standardized process—including stakeholder outreach, privacy protections, training, and facilitation of technology—for identifying and reporting suspicious activity in jurisdictions across the country and also serves as the unified focal point for sharing SAR information. The COE will support the NSI in the review of existing indicators and behaviors, potential identification of new indicators related to homeland security threats, and later provide validation of those indicators and behaviors.

Examples of COE work that may support this initiative include:

- Develop behavioral indicators for current and future reporting on homeland security topics as determined by NSI stakeholders. Development of these indicators will include interviews/focus groups conducted with DHS I&A Mission Centers and mission partners including federal, SLTT and other partners through engagement with DOJ's Criminal Intelligence Coordinating Council (CICC) and I&A's State and Local Intelligence Council (SLIC). These topics will be developed in an iterative process tied, in part, to the development of the intelligence mission centers.
- Are existing indicators reasonably indicative of pre-operational planning within the criminal activity of interest? If not, what other indicators might be substituted?
- Are the NSI participant organizations able to observe, collect, and report on the indicators for the activity of interest? If not, what other organizations might be added to the NSI to gain reporting on the activity of interest?
- What steps could be taken to increase the quantity and quality of the reporting done against each type of activity of interest and the NSI program overall?

Note: Validation of terrorism indicators and behaviors was done in 2015 by the University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism (START). This START study verified the utility of NSI to provide law enforcement and homeland security agencies with a uniform method for gathering and reporting raw tips, leads, and reports of suspicious activity. The new COE will build on this work.

Topic Area Three: Terrorism Prevention

DHS seeks research projects that directly support its terrorism prevention programs. The goal of terrorism prevention is to render terrorism ineffective as a tactic in the United States by diminishing opportunities for recruitment and inspiration for the support and use of ideologically motivated violence. To accomplish this, prevention programs target radicalization and mobilization to violence. Radicalization to violence is the process by which individuals come to believe that violence is justified to achieve political or social change, while the term "mobilization" is used to denote individuals engaging in crime and/or violence in furtherance of their ideology. For simplicity, these related and sometimes overlapping processes are often shortened and referred to as "radicalization to violence."

Terrorism prevention seeks to address all radicalization paths regardless of ideology and therefore projects should consider all forms of violent extremism and stages of radicalization to violence. Research projects will aim to develop analytic

methods to support threat detection, awareness raising, community engagement, intervention programs and countering the narrative. Unless otherwise identified below, DHS does not seek basic research that improves understanding. Rather, DHS seeks projects that have direct applicability to ongoing or future programs designed to prevent terrorism.

The major questions that DHS seeks the respondent to explore by topic are below:

Topic 3A. General Research to Practice

- What are conditions or factors that enable individuals or communities to increase resiliency to Violent Extremism (VE)? What is the role and influence of higher education in shaping vulnerabilities and responses to VE? What is the most effective role of nongovernmental partners, such as educators and mental health professionals in terrorism prevention?
- What are off-ramps in the radicalization and mobilization processes, including early warning from bystanders? How can technology impact bystanders, especially to motivate them to act on their observations?
- What are the recruitment and radicalization tactics, especially, but not limited to, online or social media campaigns, of domestic terrorists and those who adhere to domestic violent extremist ideologies? Who are the audiences for these tactics and campaigns?
- What are the hallmarks of successful (and failed) counter messaging campaigns?
- To what degree is radicalization and mobilization to violence occurring in state and local jails and correctional facilities? To what degree are federal, state and local agencies, private sector and nongovernmental organizations (NGO) equipped to address rehabilitation and prevention of recidivism post-release?
- What programs increase the likelihood of a convicted terrorist reintegrating successfully into society? What can we learn of the experience of convicted terrorists about their radicalization to violence pathways and possible de-radicalization or disengagement from violent extremist activities?
- To what degree is this similar or different from the reintegration of other incarcerated individuals? Post-release from correctional facilities, do terrorist pose different risks for terrorism recidivism than non-terrorists do for general criminal recidivism?
- What credentials should be required or recommended of someone responsible for treating a convicted terrorist when he or she is released from prison?

Topic 3B. Evaluations of Existing Programs

DHS has a strong interest in promoting best practices in terrorism prevention. To this end, DHS practitioners would work with the performer to identify community-based intervention initiatives for process and impact evaluations and/or demonstration experiments. Examples of programs that DHS would seek to evaluate include the

following types of programs:

- Training and awareness raising programs;
- Engagement programs, including tabletop exercises and roundtables
- Intervention programs working with:
    - individuals radicalizing to violence who have not yet committed a criminal act (i.e. early intervention programs)
    - individuals radicalized to violence that have committed a criminal act (i.e. diversion programs)
    - individuals radicalized to violence incarcerated or released from incarceration (i.e. rehabilitation programs)
- Efforts to combat terrorist use of the Internet, such as:
    - What is the impact of specific counter and alternative narratives currently or recently promoted by various government and non-government actors?
    - How does removal of pro-terrorist content for terms of service violations impact online radicalization? To what extent does the speed with which content is removed or challenged by competing narratives affect its discoverability and resonance?
- How can DHS better improve the efficiency and effectiveness of its communication tools/assets that it leverages to convey Homeland risk concerns with SLTT, private sector, and community partners? How can DHS better leverage SLTT and private sector communication tools/assets, in order to ensure all applicable individuals receive risk information?
- In the context of improving counterterrorism analysis, sentinel events are when prevention fails, such as arrests or attempted / successful attacks. What can researcher-practitioner teams learn from sentinel events to improve current analytic training and anticipate future training needs for counterterrorism analysts?

Topic Area Four: Workforce Development

DHS needs to actively address future workforce requirements and capabilities. Research in this area will include both current and anticipated capabilities and roadmaps to realize them. DHS seeks research projects that directly support its intelligence analyst requirements. The goal is to formalize analyst recruitment, training, and professional development. Research should be conducted into organizations with developed professional analyst career tracks to determine "best in class" programs that DHS will benefit from adopting. Research projects will aim to develop analytic programs to support recruiting, training, and further professionalizing the intelligence analyst profession. Program evaluation should include established U.S. Government analyst programs in addition to private sector offerings both within and outside academia.

The major questions that DHS seeks the respondent to explore are:

- DHS has a strong interest in promoting best practices across DHS Intelligence mission areas and specifically counterterrorism analyst development. DHS seeks to understand and evaluate current programs, programs' significance in development of analysts and leaders, and possible gaps in training. Examples of current programs for evaluation include the following:
    - Entry level analyst training programs offered at the Federal, State, Local or Private entity level:
        - DHS Office of Intelligence & Analysis Junior-Level Intelligence Analyst Comprehensive Training Program
        - DIA Professional Analyst Career Education (PACE) Program
        - International Association of Law Enforcement Intelligence Analysts (IALEIA) Foundations of Intelligence Training
        - DoD Intelligence Training and Education Board (DITEB) analyst certification program
        - Academic institutions offering certifications, bachelors, and advanced degrees in counterterrorism.
        - Leadership Training
    - Mid-career level analyst training programs offered at the Federal, State, Local or Private Sector entity level:
        - Intelligence Community Advanced Analyst Program (ICAAP)
        - The decision to become and Senior Intelligence Officer (SIO) vs. an Intelligence Manager.
        - Leadership Training as part of the developmental track.
    - Senior level analyst training programs offered at the Federal, State, Local or Private Entity level.
    - Specialization training programs relevant to counterterrorism.
- How does DHS professionalize the intelligence analyst career track compare to comparable IC programs? How can DHS better leverage government and non-government programs to enhance career field professionalization?

VI. Performance Metrics

DHS will monitor COE progress through semi-annual and annual performance reports as outlined in the Terms and Conditions. See APPENDIX A: Terms and Conditions for additional details. Reports are emailed to the DHS Grants Office and reviewed as a condition for receiving further annual funding increments.

In addition to these performance reports, on an annual basis COEs will provide DHS S&T the following information regarding COE activities:

- Amount of software developed (Algorithms, prototypes, models, etc.)
- Number of publications produced (Peer reviewed, non-peer reviewed, presentations, congressional testimony)
- Number of education programs developed (Courses, degrees, certificates, internship programs)
- Amount of students enrolled or participating in COE developed education programs (Full/part-time, online/distance learning, DHS professionals, internship enrollees)
- Amount of intellectual property developed (Patents issued, copyrights registered, trademarks registered)
- Number of requests for assistance or advice from DHS
- Number of requests for assistance or advice from other Federal (non-DHS), SLTT entities
- Amount of follow-on funding from other resources (Amount and sources of funding)

This information will allow DHS to track the efficiency and effectiveness of COE programs.

B. Federal Award Information

Award Amounts, Important Dates, and Extensions

Available Funding for the NOFO:	Up to $500,000; total will be distributed over the two year period of performance (Subject to availability of funds and project execution)
Projected number of Awards:	Up to 3; there may be zero awards

DHS may grant up to three awards for Center Partner. DHS reserves the right to add Partner institutions to the successful Center Lead institution, either from those received for the Center Lead NOFO or from the Partner NOFO, provided the applications successfully pass merit and DHS relevancy reviews. A single institution may receive only one Center Partner award under this NOFO.

Period of Performance:	Up to 24 months

DHS anticipates the period of performance of the project to be up to 24 months, encompassing two program years. DHS anticipates each program year will be 12 months. COE annual program years coincide with most academic calendars; i.e., July 1st to June 30th of the following year. The first program year may be more or less than 365 days to allow a new COE's performance periods to be synchronized with this calendar. However, because actual award dates are unknown in advance, applicants should submit proposals for the full year. Each year, annual funding is subject to the availability of appropriated funds, the performance of the Center Partner, and DHS research priorities.

An extension to the period of performance may be permitted. Please refer to **Extensions**, in Section H, for the steps recipients must follow and what information must be included in the justification for such request to be considered.

Projected Period of Performance Start Date(s): 03/23/2020

Projected Period of Performance End Date(s): 03/23/2030

Funding Instrument

Cooperative Agreement

DHS will exercise substantial programmatic involvement through this cooperative agreement. This includes monitoring project progress; providing technical assistance; disapproving and approving sub-projects, work plans or modifications thereto; holding kickoff meetings; conducting biennial reviews; conducting scientific reviews; and, coordinating R&D activities. See APPENDIX A: Terms and Conditions for additional details of substantial programmatic involvement.

Available Funding

There are two funding opportunities associated with the TPCR COE award: (1) one for Center Lead (DHS-19-ST-061-TPCR-Lead) and (2) one for Center Partner (DHS-19-ST-061-TPCR-Partner). Subject to availability of funds, DHS estimates that a ***total*** of up to $3.6 million per year will be available for funding the Center and all direct and indirect costs for the selected Center lead and Partner applications. DHS does not guarantee any total amount of annual or cumulative funding.

DHS reserves the right to select research and/or education projects submitted in response to the Center Lead and/or Partner NOFOs and combine them to create the research and education portfolio for the new Center. DHS awards the cooperative agreement to the Center Lead. Partner projects selected by DHS become part of the Center portfolio and are funded through the cooperative agreement with the Center Lead institution. DHS may allocate up to $250,000 of the $3.6 million per year to each selected Partner applicant, subject to availability of funds. The Center Lead is responsible for administering funding to all DHS-selected projects within the Center's portfolio.

Note: The first year of funding may be less due to startup delays; however, applicants should submit proposals for the full amount.

C. Eligibility Information

Eligible Applicants

The Center Lead designation is restricted to an accredited institution of higher education in the United States, in accordance with 6 U.S.C. 188(b)(2)(A) which specifies: "The

Secretary, acting through the Under Secretary for Science and Technology, shall designate a university-based center or several university-based centers for homeland security."

Partner applicants may be from academia, commercial industry, or non-profit organizations. Proposals must be submitted by an accredited U.S. institution of higher education, commercial industry, or non-profit organizations that, along with its chosen partners, has the ability and capacity to conduct the required research. The applicant institution must be identified as the official lead for proposal submission and subsequent negotiations.

Applicants must submit only 1 project per proposal. Applicants may submit more than 1 proposal. Principal Investigators that are already Partners under a Center Lead application may not submit the same application under this Partner NOFO.

Center lead applicants are strongly encouraged to partner with industry, other academic institutions, including historically black colleges and universities (HBCUs), Hispanic serving institutions (HSIs), and/or other MSIs; institutions in states that are part of the Experimental Program to Stimulate Competitive Research (EPSCoR); public sector institutions, and non-profit organizations, including any organizations that meet the definition of nonprofit in OMB Circular A-122, relocated to 2 CFR Part 230. However, nonprofit organizations described in Section 501(c)(4) of the Internal Revenue Code that engage in lobbying activities as defined in Section 3 of the Lobbying Disclosure Act of 1995 are not eligible to apply. The Center Lead institution will fund partnering institutions through sub-awards.

Center Partner institution partnerships with foreign institutions are permitted, but may require special justification and approval from DHS. The applicant can include team members who are non-U.S. citizens; however, the proposed Center Director must be a U.S. citizen eligible for a security clearance.

FFRDCs or laboratories funded by federal agencies may not apply. FFRDC employees may cooperate or collaborate with eligible applicants within the limits imposed by applicable legislation, regulations, and DHS policies. FFRDC employees are not eligible to serve in a principal leadership role on a grant or cooperative agreement, and may not receive salaries or in other ways augment their agency's appropriations through awards made by this program. National laboratory employees may participate in planning, conducting, and analyzing the research directed by the COE principal investigator, but may not direct projects on behalf of the applicant organization or principal investigator. The principal investigator's institution, organization, or governance may provide funds through its assistance agreement with DHS to an FFRDC for project-specific, non-federal research personnel, supplies, equipment, facilities, data, and other expenses directly related to the research.

Federal agencies may not apply. Federal employees are not eligible to serve in a principal leadership role on a grant or cooperative agreement, and may not receive

salaries or in other ways augment their agency's appropriations through awards made by this program. Nonetheless, federal employees may interact substantively with awardees in the form of cooperation. Cooperation involves consulting on the planning, management, and coordination of COE activities, sharing or comparing samples, equipment, facilities, data, models, or other support during the conduct of the research in which the interaction is substantial and requires the award of a cooperative agreement, rather than a grant. Substantial involvement occurs when the collaboration or cooperation of a federal employee or facility is necessary to achieving the overall goals of the research supported by a cooperative agreement.

Eligibility Criteria

DHS will not consider applications that do not adhere to one or more of the following requirements:

1. **Deadlines.** DHS will not accept late applications. Without exception, applications must be received by Grants.gov on or before the deadline indicated in this announcement or they will not be considered.
2. **Application relevance.** Applications that do not address the purpose of this announcement will not be considered.
3. **Compliance and completeness.** Applications must substantially comply with the application submission instructions and requirements in this announcement or they will not be considered.
4. **Funding limits.** Applications exceeding the funding limits will not be considered.
5. **Project period.** Applications exceeding the project period term will not be considered.

Cost Share or Match

A cost match or a cost share is voluntary. However, the ability to extend the reach of DHS funds for research and education in support of its mission is an important consideration for DHS. In-kind contributions demonstrate a university's commitment to the COE. Identification of university in-kind contributions will result in a higher rating in DHS's overall proposal review.

D. Application and Submission Information

Submission Date and Other Key Dates and Times

Date Posted to Grants.gov:	07/10/2019
Application Submission Deadline:	09/13/2019 at 11:59:59 PM EDT
Anticipated Funding Selection Date:	02/03/2020

Anticipated Award Date: 02/28/2020

NOTE: The application must be received in Grants.gov by the date and time listed above. If an application is received after the deadline, it will not be considered. Applicants will receive a confirmation from Grants.gov once the application is successfully submitted.

All applications are time stamped by the Grants.gov system when submitted and recipients are notified accordingly. The federal office will download all applications that are received by the deadline date and time as indicated on the NOFO.

Other Key Dates

Event	Suggested Deadline For Completion
Informational Webinar	08/6/2019 (3:00PM EDT) See details below
Obtaining DUNS Number	Four weeks before actual submission deadline 08/09/2019
Obtaining a valid EIN	Four weeks before actual submission deadline 08/09/2019
Updating SAM registration	Four weeks before actual submission deadline 08/09/2019
Starting application in Grants.gov	One week before actual submission deadline 08/09/2019

Address to Request Application Package

Application forms and instructions are available at Grants.gov. To access these materials, go to https://www.grants.gov/ , select "Applicants" then "Apply for Grants," read the registration requirements and register if necessary (**Allow up to 7-10 business days after you submit before your registration is active in SAM, then an additional 24 hours for Grants.gov to recognize your information)**. In order to obtain the application package select "Download a Grant Application Package." Enter the CFDA and/or the funding opportunity number located on the cover of this NOFO, select "Download Package," and then follow the prompts to download the application package.

For a hardcopy of the full NOFO, please email request to:

stephanie.dawkins@HQ.DHS.GOV

Applications will be processed through the Grants.gov portal

Informational Webinar

DHS will conduct an informational webinar for interested applicants on August 6, 2019 at 3:00pm [EDT]. During the call, DHS will discuss the NOFO and provide an opportunity for interested applicants to ask questions. The webinar may be accessed by phone (Dial: 855-852-7677, Passcode: 5122121) and computer (https://share.dhs.gov/rwo6kbeg53be/). The webinar will be recorded and posted on www.grants.gov for future reference.

Content and Form of Application Submission

I. SF424 (R & R) Application for Federal Assistance (SF424-V2.0)

Please complete this form in its entirety. If you fill this form out first, other required forms will populate with basic data such as name, address, etc. Signature and date will auto-fill when you submit the application package through Grants.gov.

1. Block 1, Type of Submission – please check "Application"
2. Block 8, Type of Application – please check "New"
3. Block 12, Proposed Project – please provide the start and end dates for your project
4. Block 15, Total Estimated Project Funding – this amount should correspond to your budget justification and the Budget form's total for the requested budget period. ***DHS anticipates the period of performance of the Center to be up to 120 months, encompassing ten program years, however, project budget submission for an application should not exceed the first five years.***
5. Block 16 (E.O. 12372 review question): Please contact your State Single Point of Contact (SPOC) to determine whether you are required to submit this noncompeting continuation application for review, and then check the appropriate box in Block 19. Find your State SPOCs:

   https://www.whitehouse.gov/wp-content/uploads/2019/02/SPOC-February-2019.pdf
6. Regarding Block 17: By submitting this application, your organization is providing certifications and assurances regarding:
   1. Drug-Free Workplace Requirements
   2. Debarment, Suspension, and Other Responsibility Matters—Primary Covered Transactions
   3. Information regarding the certifications on drug-free workplace; and debarment, suspension, and other responsibility matters; is attached for your reference as Attachment A
7. If you are requesting Indirect/Fringe Costs, please attach your indirect cost rate agreement, fringe benefit rate agreement, or a description of how fringe rates are calculated, using the "Add Attachments" button at the end of the 424

II. Budget Information, Non Construction Programs (SF424A-V1.1)

Filling out the Budget Form – please ensure that funds requested on the Budget form correspond to the same items in your budget justification and that the total requested corresponds to Block 15 on the SF 424 form. ***DHS anticipates the period of performance of the Center to be up to 120 months, encompassing ten program years, however, the project budget submission for an application should not exceed the first five years.***

III. Certification Regarding Lobbying (GG_Lobbying Form-V1.1)

Submit this form. It will be electronically signed upon submission to Grants.gov as part of your application. If paragraph two of the certification applies, then complete and submit the SF-LLL Disclosure of Lobbying, which is provided as an optional form in the application package.

IV. Research & Related: Senior/Key Personnel Profile

Applicants must complete a profile for the principal investigator(s) as well as other Senior Key Personnel identified for the project. Provide biographical a sketch for each senior/key person that include education and research activities and accomplishments and each individual's role in the proposed project. Each biographical sketch may not exceed two pages.

V. Research and Related: Other Project Information

Tips: Write for a general audience and avoid use of scientific jargon to the extent possible. Please define any technical terminology that is discipline-specific. Be concise and direct in descriptions.

a. Other Project Information (Items 1-6)

Includes information regarding use of human subjects, use of animal subjects, proprietary information, environmental impacts, historic place designation, and international collaborators.

b. Project Summary/Abstract (Item 7)

The summary is limited to one single-spaced page with 12-point Times New Roman font and one-inch margins. Attach the Summary/Abstract to Item 7 on the Research & Related Other Project Information Form.

The Summary/Abstract is for dissemination to the public and must not include any proprietary or confidential information.

Include the title of the Project and provide a summary of (1) the objectives of the project; (2) the approach to be used; and (3) examples of the potential results and how those results may benefit specific homeland security stakeholders. Applicants must select either a research project or a workforce and professional development project for their proposal. Applicants must clearly identify which they have chosen.

c. Project Narrative (Item 8)

The project narrative is limited to 5 single-spaced pages with 12-point Times New Roman font and one-inch margins. Applicants must adhere

strictly to the page limits. Pages in excess of the page limitations will not be reviewed. Attach the Center Narrative to Item 8 on the Research & Related Other Project Information Form.

Applicants must select either a research project or a workforce development project for their proposal and must clearly identify which they have chosen. Applicants should specifically identify which theme area and topic it has chosen to address.

Applicants must address the requirements as described in Section IV. Application Project Narrative.

d. Bibliography & References Cited (Item 9)

The bibliography and/or references section is limited to 5 single-spaced pages with 12-point font, Times New Roman, and one-inch margins.

e. Facilities and Equipment (Items 10 and 11)

Each applicant must provide a very specific description of any equipment/hardware that it needs to acquire to perform the work. This description should indicate whether or not each particular piece of equipment/hardware will be included as part of a deliverable item under the resulting award. Also, this description should identify the component, nomenclature, and configuration of the equipment/hardware that it proposes to purchase for this effort. The purchase on a direct reimbursement basis of special test equipment or other equipment will be evaluated for allow ability on a case-by-case basis. Maximum use of Government integration, test, and experiment facilities is encouraged. Government research facilities and operational military units are available and should be considered as potential government furnished equipment/facilities. These facilities and resources are of high value and some are in constant demand by multiple programs.

f. Other Attachments (Item 12)

Use this to attach the documents listed under **Other Submission Requirements** (i.e. Consolidated List of Partners and Principal Investigator(s), Consolidated List of Projects, Letter of Support from University Leadership) as well as a bibliography or if you need another place to electronically attach portions of your application.

Optional Forms

SF-LLL Disclosure of Lobbying Activities
Fill out and submit this form ONLY if Condition 2 in the Lobbying Certification applies.

Other Submission Requirements

1. Consolidated List of Partners and Principal Investigator(s)
   Applicants must provide a consolidated list of all Partners and principal investigator(s) to facilitate identification of reviewers that are free of any organizational or personal conflicts of interest.

Unique Entity Identifier and System for Award Management (SAM)

DHS is participating in the Grants.gov initiative that provides the grant community a single site to find and apply for grant funding opportunities; therefore, applicants with electronic access are to submit their applications electronically through http://www.grants.gov/web/grants/applicants/apply-for-grants.html. Before you can apply for a DHS grant at grants.gov, you must have a Data Universal Numbering System (DUNS) number, be registered in SAM, and be approved as an Authorized Organizational Representative (AOR).

Applicants are encouraged to register early. The registration process can take four weeks or more to be completed. Therefore, registration should be done in sufficient time to ensure it does not impact your ability to meet required submission deadlines.

How to Register to Apply through Grants.gov

1. *Instructions:* Read the instructions below about registering to apply for DHS funds. Applicants should read the registration instructions carefully and prepare the information requested before beginning the registration process. Reviewing and assembling the required information before beginning the registration process will alleviate last-minute searches for required information.

   Organizations must have DUNS Number, active SAM registration, and Grants.gov account to apply for grants.

   If individual applicants are eligible to apply for this grant funding opportunity, refer to: https://www.grants.gov/web/grants/applicants/registration.html

   Organization applicants can find complete instructions here: https://www.grants.gov/web/grants/applicants/organization-registration.html

2. *Obtain a DUNS Number*: All entities applying for funding, including renewal funding, must have a DUNS number from Dun & Bradstreet (D&B). Applicants must enter the DUNS number in the data entry field labeled "Organizational DUNS" on the SF-424 form.

   For more detailed instructions for obtaining a DUNS number, refer to: https://www.grants.gov/web/grants/applicants/organization-registration/step-1-obtain-duns-number.html

3. *Register with SAM*: In addition to having a DUNS number, all organizations applying online through Grants.gov must register with the SAM. Failure to register with SAM will prevent your organization from applying through Grants.gov. SAM registration must be renewed annually.

For more detailed instructions for registering with SAM, refer to: https://www.grants.gov/web/grants/applicants/organization-registration/step-2-register-with-sam.html

4. *Create a Grants.gov Account*: The next step in the registration process is to create an account with Grants.gov. Applicants must know their organization's DUNS number to complete this process.

   For more information, follow the on-screen instructions or refer to: https://www.grants.gov/web/grants/applicants/registration.html

5. *Add a Profile to a Grants.gov Account*: A profile in Grants.gov corresponds to a single applicant organization the user represents (i.e., an applicant) or an individual applicant. If you work for or consult with multiple organizations and have a profile for each, you may log in to one Grants.gov account to access all of your grant applications. To add an organizational profile to your Grants.gov account, enter the DUNS Number for the organization in the DUNS field while adding a profile.

   For more detailed instructions about creating a profile on Grants.gov, refer to: https://www.grants.gov/web/grants/applicants/registration/add-profile.html

6. *EBiz POC Authorized Profile Roles*: After you register with Grants.gov and create an Organization Applicant Profile, the organization applicant's request for Grants.gov roles and access is sent to the EBiz POC. The EBiz POC will then log in to Grants.gov and authorize the appropriate roles, which may include the Authorized Organization Representative (AOR) role, thereby giving you permission to complete and submit applications on behalf of the organization. You will be able to submit your application online any time after you have been assigned the AOR role.

   For more detailed instructions about creating a profile on Grants.gov, refer to: https://www.grants.gov/web/grants/applicants/registration/authorize-roles.html

7. *Track Role Status*: To track your role request, refer to: https://www.grants.gov/web/grants/applicants/registration/track-role-status.html

8. *Electronic Signature*: When applications are submitted through Grants.gov, the name of the organization applicant with the AOR role that submitted the application is inserted into the signature line of the application, serving as the electronic signature. The EBiz POC **must** authorize individuals who are able to make legally binding commitments on behalf of the organization as an AOR; **this step is often missed and it is crucial for valid and timely submissions.**

How to Submit an Application to DHS via Grants.gov

Grants.gov applicants can apply online using Workspace. Workspace is a shared, online environment where members of a grant team may simultaneously access and edit different Webforms within an application. For each NOFO, you can create individual instances of a workspace.

Below is an overview of applying on Grants.gov. For access to complete instructions on how to apply for opportunities using Workspace, refer to:

https://www.grants.gov/web/grants/applicants/workspace-overview.html

1. *Create a Workspace*: Creating a workspace allows you to complete it online and route it through your organization for review before submitting.

2. *Complete a Workspace*: Add participants to the workspace to work on the application together, complete all the required forms online or by downloading PDF versions, and check for errors before submission.

3. *Adobe Reader*: If you decide not to apply by filling out webforms you can download individual PDF forms in Workspace so that they will appear similar to other Standard or DHS forms. The individual PDF forms can be downloaded and saved to your local device storage, network drive(s), or external drives, then accessed through Adobe Reader.

   NOTE: Visit the Adobe Software Compatibility page on Grants.gov to download the appropriate version of the software at: https://www.grants.gov/web/grants/applicants/adobe-software-compatibility.html

4. *Mandatory Fields in Forms:* In the forms, you will note fields marked with an asterisk and a different background color. These fields are mandatory fields that must be completed to successfully submit your application.

5. *Complete SF-424 Fields First*: The forms are designed to fill in common required fields across other forms, such as the applicant name, address, and DUNS number. To trigger this feature, an applicant must complete the SF-424 information first. Once it is completed, the information will transfer to the other forms.

6. *Submit a Workspace*: An application may be submitted through workspace by clicking the "Sign and Submit" button on the Manage Workspace page, under the Forms tab. Grants.gov recommends submitting your application package at least 24-48 hours prior to the close date to provide you with time to correct any potential technical issues that may disrupt the application submission.

7. *Track a Workspace*: After successfully submitting a workspace package, a Grants.gov Tracking Number (GRANTXXXXXXXX) is automatically assigned to the application. The number will be listed on the Confirmation page that is generated after submission. Using the tracking number, access the Track My

Application page under the Applicants tab or the Details tab in the submitted workspace.

For additional training resources, including video tutorials, refer to: https://www.grants.gov/web/grants/applicants/applicant-training.html

Applicant Support: Grants.gov provides applicants 24/7 support via the toll-free number 1-800-518-4726 and email at support@grants.gov. For questions related to the specific grant opportunity, contact the number listed in the application package of the grant you are applying for.

If you are experiencing difficulties with your submission, it is best to call the Grants.gov Support Center and get a ticket number. The Support Center ticket number will assist DHS with tracking your issue and understanding background information on the issue.

Timely Receipt Requirements and Proof of Timely Submission

Online Submissions. All applications must be received by **Midnight Eastern Daylight (EDT) Time** on the due date established for each program. Proof of timely submission is automatically recorded by Grants.gov. An electronic date/time stamp is generated within the system when the application is successfully received by Grants.gov. The applicant with the AOR role who submitted the application will receive an acknowledgement of receipt and a tracking number (GRANTXXXXXXXX) from Grants.gov with the successful transmission of their application. This applicant with the AOR role will also receive the official date/time stamp and Grants.gov Tracking number in an email serving as proof of their timely submission.

When DHS successfully retrieves the application from Grants.gov, and acknowledges the download of submissions, Grants.gov will provide an electronic acknowledgment of receipt of the application to the email address of the applicant with the AOR role who submitted the application. Again, proof of timely submission shall be the official date and time that Grants.gov receives your application. Applications received by Grants.gov after the established due date for the program will be considered late and will not be considered for funding by DHS.

Applicants using slow internet, such as dial-up connections, should be aware that transmission can take some time before Grants.gov receives your application. Again, Grants.gov will provide either an error or a successfully received transmission in the form of an email sent to the applicant with the AOR role. The Grants.gov Support Center reports that some applicants end the transmission because they think that nothing is occurring during the transmission process. Please be patient and give the system time to process the application.

Intergovernmental Review

N/A

Funding Restrictions

DHS does not envision any specific funding restrictions at this time. However, DHS substantial programmatic involvement and performance/progress reviews may result in funding restrictions in conjunction with initial and annual continuation awards. Funding restrictions may be issued on activities that require further detail or when corrective actions are needed.

DHS OUP awards Center funding annually. Award amounts are subject to the availability of funding.

Management and Administration

N/A

Indirect (Facilities & Administrative (F&A)) Costs

Indirect Cost (IDC) is allowable by the recipient and sub-recipients. Provide a copy of the negotiated rate approved by the applicant's cognizant agency at the time of application.

E. Application Review Information

Review and Selection Process

DHS S&T will use a two-phase to select the partner institution(s) for a COE. The phases are:

1. External scientific quality review by a panel of peers external to DHS, and
2. Internal relevancy review by a panel of DHS SMEs.

These two evaluation phases are completed in sequence and are scored independently. Only the highest scoring proposals will be referred from the external to the internal review.

Each review phase is rated based upon unique criteria (e.g., scientific quality, relevance to DHS, etc.). A detailed description of each phase and associated criteria is provided below.

Note: All proposals will be the intellectual property of the applicants up until a proposal is approved and an award is made. Additionally, the proposal will be incorporated by reference in the award.

I. Scientific Quality Review (External Review)

This is the first phase in the review process. Applications not meeting the minimum threshold will not advance to the next phase.

DHS will conduct a scientific quality review of proposals by an external review panel of SMEs from academia, non-profit research organizations, industry, and/or federal, state, or local agencies. The panelists will have expertise and/or experience in academic disciplines relevant to intelligence gathering and analysis and terrorism prevention. This includes national security, physical security, computer science, behavioral science, law, public policy, organizational design, education and training, and data science.

The external review panel will consider only evaluation criteria and weightings identified in this NOFO that focus on the quality and influence of the researchers and proposed research and education programs, as well as the appropriateness of research costs.

The OUP Program Manager responsible for the COE serves as chairperson for the external review panel. His/her role is to summarize and convey results (including calculating mean and median ratings) to the Selection Manager (SM) for further consideration, and to answer questions posed by review panelists. The chairperson does not rate the applications. However, the chairperson will serve in an advisory capacity to clarify aspects of the COE program and selection process. In addition, the chairperson maintains order, ensures the absence of conflicts of interest, ensures that all panelists have completed and signed non-disclosure agreements, and ensures proper documentation of the review and rating of the applications. Finally, the chairperson ensures that all documentation is collected from the panel members and all proprietary information is destroyed at the conclusion of the review.

A minimum of three reviewers will review each proposal thoroughly. With the exception of those deemed to have a conflict of interest, all reviewers have access to all proposals, although each reviewer is only assigned a subset of proposals for formal review. Reviewers will rate applications on a set of weighted criteria using numerical ratings of 1 to 5 (poor to excellent). All reviewers will enter their narrative reviews and their preliminary ratings for their assigned proposals into a secure web-based peer review database.

After all of the external reviewers have submitted their reviews through the secure web-based peer review database, the chairperson will organize the resulting scores and documents to identify proposals that meet or exceed the scores necessary to advance to the internal review. DHS does not seek reviewer consensus on a summary review, but rather expects a diversity of opinions. Each primary reviewer must sign off on each summary evaluation form to ensure his or her comments adequately reflect their evaluations.

For each proposal, DHS will calculate the mean and median rating for all reviewers. DHS reserves the right to use either the mean or the median rating as the final rating for applications. A minimum threshold level will be established for referral of applications from the external review phase to the internal review phase. DHS will select the minimum threshold based on the ratings of applications for this funding

opportunity. For example, if DHS receives six applications, three of which have a rating of 4.0 or higher in the external review phase, while the other three are less than 3.5, 4.0 will be the minimum threshold for passing applications to the internal review phase. If the rating—mean or median—is above the threshold established for the external review phase, the application will be considered to be of high scientific quality and will be forwarded for the internal review phase. Under no circumstances will an application be considered if both the mean and the median overall ratings are below 3.0 (Good).

This summary review is critical as it forms a substantive basis for pre-award negotiations with the selected institution(s). The chairperson is responsible for conveying the summary reviews of successful proposals; i.e., those with ratings above the threshold, to the SM for consideration by the internal review panel. The chairperson is also responsible for conveying the summary reviews of the unsuccessful proposals; i.e., those with ratings under the threshold, to the DHS Grants Officer for processing declination letters.

II. DHS Relevancy Review (Internal DHS SMEs)

Applications scoring above the minimum threshold from the external scientific review will advance and be evaluated in the second phase, the internal relevancy review. Scores received in the first phase are not considered in the relevancy evaluation.

As soon as feasible after the external review concludes, the SM convenes an internal review panel of DHS SMEs to review proposals transmitted from the external review phase (those proposals having mean or median ratings at or above the quality threshold). The chairperson of the external review panel will also serve as the chairperson of the internal review panel. His/her role is to summarize and convey results (including calculating mean and median ratings) to the SM for further consideration and to answer substantive questions posed by review panelists. The chairperson does not rate the applications. However, the chairperson will serve in an advisory capacity should questions arise during the review that may require clarification of the COE program or selection process. In addition, the chairperson maintains order, ensures the absence of conflicts of interest, and ensures proper documentation of the review and rating of the applications. Finally, the chairperson ensures that all documentation is collected from the panel members and destroyed at the conclusion of the review.

The internal review panel will focus on the mission relevance of the proposed research; the relation of the proposed research to DHS operations and other research and development in this area; and, the potential for the research results to transition to the user community.

The internal review panel will also describe perceived knowledge gaps in the subject area as a further basis for discussions during the site visit phase and for negotiations with the selected institution(s). This panel can also suggest how elements of different

proposals referred by the external review panel from either the Center Lead NOFO or the Center Partner NOFO could be combined to better serve the research needs of DHS S&T and relevant DHS components. A discussion about DHS's reorganization of research areas or projects will be documented in an Additional Comments section.

With the exception of those deemed to have a conflict of interest, all reviewers have access to all proposals, although they may only be assigned a subset of these proposals for formal review. Reviewers will rate applications on a set of weighted criteria using numerical ratings of 1 to 5 (poor to excellent). Prior to the in-person review meeting, all reviewers will provide their narrative reviews and ratings for their assigned proposals to the chairperson, or if a secure web-based peer review database is used, then they will enter their ratings directly into the on-line database. Narrative comments must support the numerical ratings.

After all internal reviewers have submitted their preliminary reviews to the chairperson, or through the secure web-based peer review database, an in-person internal review panel meeting will take place in Washington, DC. At the in-person meeting, panelists discuss proposals using the selected evaluation criteria described below. Primary reviewers and other panelists who have read the entire proposal may provide ratings for each proposal following these discussions.

For each proposal, DHS will calculate the mean and median rating for all reviewers to determine a final rating. DHS reserves the right to use either the mean or the median rating as the final rating for all applications. A minimum threshold level will be established for referral of applications from the internal review phase to the site visit review phase. DHS will select the minimum threshold based on the ratings of applications for this funding opportunity. For example, if six applications are passed from the external review phase, three of which have a rating of 4.0 or higher in the internal review phase, while the other three are less than 3.5, 4.0 will be the minimum threshold for passing applications to the site visit review phase. If the rating—mean or median—is above the threshold established for the internal review phase, the application demonstrates both scientific quality and relevance. These applications will be forwarded to the site visit review phase. Under no circumstances will an application be considered if both the mean and the median overall ratings are below 3.0. Proposals with ratings above the threshold carry the presumption that the applicant institutions have the capabilities required to establish a successful research and education COE in the relevant topic area.

Application Evaluation Criteria

Prior to making a federal award, the DHS Financial Assistance Office (FAO) is required by 31 U.S.C. § 3321 note, 41 U.S.C. § 2313, and 2 C.F.R. § 200.205 to review information available through any OMB-designated repositories of government wide eligibility qualification or financial integrity information. Therefore, application evaluation criteria may include the following risk based considerations of the applicant:

1. Financial stability.

2. Quality of management systems and ability to meet management standards.
3. History of performance in managing federal award.
4. Reports and findings from audits.
5. Ability to effectively implement statutory, regulatory, or other requirements.

I. Research Project Evaluation Criteria

Each panel or team will be comprised of a set of reviewers and will focus on the evaluation criteria as described in this section. For the external and internal reviews, a minimum of three SMEs will review each proposal and provide comments and ratings based on the relevant criteria. Each phase of the review process is scored separately. The weighting of each criterion is identified under each review phase.

Reviewers will consider the proposals in terms of strengths and weaknesses for evaluation criterion. DHS will rate each criterion using the following scale: 1=Poor, 2=Fair, 3=Good, 4=Very Good and 5=Excellent.

1 (poor):	A proposal where weaknesses far outweigh strengths.
2 (fair):	A proposal with strengths and weaknesses approximately equal.
3 (good):	A proposal where there are more strengths than weaknesses.
4 (very good):	A proposal with many strengths and few weaknesses.
5 (excellent):	A proposal where strengths far outweigh weaknesses.

For each review phase, the specific evaluation criteria, and its assigned scoring weight, is detailed below.

Phase 1: Scientific Quality Review (External): Reviewers will rate how the proposal addresses the following criteria using numerical ratings of 1 to 5 (poor to excellent) and apply the percentage-weighting factor as indicated for an overall rating. A research proposal's final score in this phase will determine eligibility to advance and be evaluated in Phase 2.

A. Originality and/or Innovativeness (45%)

- Is it original (i.e., does the proposed effort challenge and seek to shift current research or paradigms by utilizing novel theoretical concepts, approaches or methodologies)?
- Is it innovative (i.e., is the proposal a novel refinement, improvement, or new application of theoretical concepts, approaches, or methodologies proposed)?
- Does this research have the potential to generate influential peer-reviewed publications in the scientific community or lead to new discoveries or areas of investigation?

- Does the research plan outline appropriate business, legal, and technical considerations necessary to move the proposed research into use by customers?

B. Project Goals and Methodologies (30%)

- Are the research goals clear and based on sound theory?
- Are the proposed goals and methods feasible?
- Are the proposed methods clearly-stated and appropriate for testing the hypotheses?
- Are the data generation or collection approaches appropriate for the research methods?
- Is the proposed timeframe to complete the project(s) appropriate?
- Will the research team have access to the necessary data to execute the project?
- Does the proposal identify the specific gaps being addressed and the steps necessary to test the capabilities in an operational environment?
- If software based, does the proposed research adhere to standards, software requirements specifications, design descriptions, verification and validation plans, configuration management, interoperability, and security standards that are required by potential customers?

C. Qualifications of Personnel and Suitability of Facilities (15%)

- Does the research team have the qualifications – credentials, expertise, and experience – to carry out the proposed research?
- Are the facilities suitable for the proposed research? If so, does the applicant demonstrate a commitment from facility owners to allow researchers to use necessary facilities? Are the facilities currently approved for the work being proposed?
- Does the research proposal demonstrate that the researchers possess a sufficient amount of understanding of regulatory requirements, market conditions, and legal constraints necessary to execute the proposed work?

D. Costs (10%)

- Are the proposed research and education costs appropriate and reasonable?

Phase 2: DHS Relevancy Review (Internal): Reviewers will rate how the proposal addresses the following criteria. Reviewers will rate applications using numerical ratings of 1 to 5 (poor to excellent) and apply the percentage-weighting factor as indicated for an overall rating.

A. Mission Relevance (75%)

- Do proposed projects address the research themes that DHS has identified in the NOFO?
- Do the goals of the research relate to DHS's mission?
- Does the applicant discuss where, in what circumstances, and by whom research results would be used? Are these applications relevant to DHS's mission?
- Are the potential research outcomes and end users of the research well-described?
- Has the applicant demonstrated an understanding of DHS's existing R&D programs, information systems, and databases in relevant areas?
- Does the proposed program address a knowledge gap not addressed by research and development programs sponsored by DHS or others?

B. Transition Strategy (25%)

- Is there an estimated reasonable timeframe for when COE research results would be available in a usable format (such as web-based platforms that are compatible with most servers, applications (available on desktop or mobile app store) assays, etc.)? How will intellectual property be handled for COE outputs? How effective are the proposed approaches to address sustainability and access concerns?
- Does the transition plan propose a process to identify and engage customers throughout the entire duration of the project?
- Has the program developed a compelling strategy for research management oversight to include a phased stage gate process?
- Does the applicant provide key performance parameters and metrics to capture project performance?
- If software based, does the proposed research adhere to standards, software requirements specifications, design descriptions, verification and validation plans, configuration management, interoperability, and security standards that are required by potential customers?
- Does the applicant have a university resource (e.g., technology transition office) to provide business and legal services necessary to make efficient decisions to support technology transfer?

II. Workforce Development Project Evaluation Criteria:

Scientific Merit Review (External): Reviewers will rate how the proposal addresses the following criteria using numerical ratings of 1 to 5 (poor to excellent) and apply the percentage-weighting factor as indicated for an overall rating. A workforce development proposal's final score in this phase will determine eligibility to advance and be evaluated in phase two.

A. Project Goals, Approaches, and Methodologies (60%)

- Is the approach needs-based or market-driven? Will it establish significant courses or content relevant to professionals working in homeland security?
- Does the proposed program coursework have the potential to be far-reaching, transferrable, and accessible by a diverse audience?
- Does the proposal describe university/industry/government partnerships that could potentially provide internship experiences, employment opportunities, or career mentorships for the Center's students?
- Does the proposal describe initiatives for tracking career development of the Center's students post-graduation?
- Is there a viable plan for a successful transition of students (undergraduates to graduate school or HSE workforce: Graduate students and professionals to the HS workforce)?
- Is the approach for evaluating and reporting on program and student performance and success sound?

B. Integration and Partnerships (15%)

- Does the application incorporate external public and private partners who can provide guidance and or potentially provide employment for supported participants?

C. Qualifications of Personnel and Suitability of Facilities (15%)

- Does the application incorporate qualified personnel – credentials, expertise, and experience – who can enrich and teach the proposed content?
- Are the facilities suitable for the proposed education? If so, does the applicant demonstrate a commitment from facility owners to allow the team to use necessary facilities?

D. Costs (10%)

- Are the proposed costs appropriate and reasonable?

Relevancy Review: Reviewers will rate how the proposal addresses the following criteria. Reviewers will rate applications using numerical ratings of 1 to 5 (poor to excellent) and apply the percentage-weighting factor as indicated for an overall rating.

A. Mission Relevance (100%)

- Is the proposed program relevant to the priority areas within DHS?
- Does the proposed program have the potential to enhance or improve the HSE workforce over the long term?
- Does it incorporate relevant case studies or content linked to homeland security-related science and technology issues and challenges?

- Does the plan incorporate information on the current workforce needs within the relevant HSE sectors?

Example Evaluation

Each reviewer's overall rating for a proposal will be calculated by first multiplying the weight for each criterion by its rating, then adding the weighted scores together for an overall proposal rating.

The charts below provide examples of how one reviewer's overall rating for a proposal would be calculated for each review phase.

Research Project Example

Scientific Quality Review (External – Research):

Evaluation Criteria	**Reviewer Score**	**Weight (%)**	**Weighted Score**
Originality and/or Innovativeness	4	45%	1.00
Project Goals, Approaches, and Methodologies	5	30%	1.25
Qualifications of Personnel and Suitability of Facilities	5	15%	0.75
Costs	4	10%	0.40
External Review Rating			**4.15**

Only those applications meeting the threshold rating for the external review phase will be forwarded to the internal review phase.

DHS Relevancy Review (Internal - Research):

Evaluation Criteria	**Reviewer Score**	**Weight (%)**	**Weighted Score**
Mission Relevance	5	75%	3.75
Transition Strategy	2	25%	0.5
Internal Review Rating			**4.25**

Workforce Development Project Example

Scientific Quality Review (External – Workforce Development):

Evaluation Criteria	**Reviewer Score**	**Weight (%)**	**Weighted Score**

Project Goals, Approaches, and Methodologies	5	60%	3.00
Integration and Partnerships	3	15%	0.45
Qualifications of Personnel and Suitability of Facilities	5	15%	0.75
Costs	4	10%	0.40
External Review Rating			**4.60**

Only those applications meeting the threshold rating for the external review phase will be forwarded to the internal review phase.

DHS Relevancy Review (Internal - Workforce Development):

Evaluation Criteria	**Reviewer Score**	**Weight (%)**	**Weighted Score**
Workforce Development	5	100%	5
Internal Review Rating			**5**

For each proposal, DHS will calculate the mean and median rating for all reviewers to determine a final rating. DHS reserves the right to use either the mean or the median rating as the final rating for all applications.

III. Supplemental Financial Integrity Review

If the anticipated federal share of a federal award will be greater than the simplified acquisition threshold, currently $250,000 (see Section 805 of the National Defense Authorization Act for Fiscal year 2008, Pub. L. No. 115-91, OMB Memorandum M-18-18 at https://www.whitehouse.gov/wp-content/uploads/2018/06/M-18-18.pdf):

A. Prior to making a federal award with a total amount of federal share greater than the simplified acquisition threshold, DHS is required to review and consider any information about the applicant that is in the designated integrity and performance system accessible through SAM (currently FAPIIS).
B. An applicant, at its option, may review information in the designated integrity and performance systems accessible through SAM and comment on any information about itself that a federal awarding agency previously entered and is currently in the designated integrity and performance system accessible through SAM.
C. DHS will consider any comments by the applicant, in addition to the other information in the designated integrity and performance system, in making a judgment about the applicant's integrity, business ethics, and record of performance under federal awards when completing the review of risk posed by applicants as described in 2 C.F.R. § 200.205 federal awarding agency review of risk posed by applicants.

F. Federal Award Administration Information

Notice of Award

Customarily, applicants are notified about evaluation decisions within six months of the application closing date. A summary statement of the scientific review by the peer panel will be provided to each applicant with an award or declination letter. DHS also requires successful applicants to provide responses to comments or suggestions offered by the peer reviewers and revise and resubmit their proposal accordingly. Successful applicants may also be requested to submit a revised budget. DHS will contact the applicant to obtain these materials. Before or after an award, applicants may be required to provide additional quality assurance documentation. A cooperative agreement award will be executed by a DHS Grants Officer authorized to obligate DHS funding. The successful applicant will receive the award and cover letter by e-mail. The successful applicant will have the option to request an original by mail.

Work Plan Development Workshop

After award and subject to agreement from the DHS Program Manager, the selected Center Lead will hold a work plan development workshop with Center Partners and homeland security practitioners to refine the originally proposed work selected as part of this funding opportunity. Project proposals will receive an initial year of funding once DHS has approved a project work plan. Additional funding beyond the first year will depend upon performance and availability of funds. DHS expects this workshop to occur within 60 days of the award.

Administrative and National Policy Requirements

All successful applicants for all DHS grant and cooperative agreements are required to comply with DHS Standard Administrative Terms and Conditions, which are available online at:

DHS Standard Terms and Conditions

The applicable DHS Standard Administrative Terms and Conditions will be for the last year specified at that URL, unless the application is to continue an award first awarded in an earlier year. In that event, the terms and conditions that apply will be those in effect for the year in which the award was originally made.

In addition, successful applicants of this NOFO must accept all conditions of the Terms and Conditions that apply specifically to this COE Award as administered by the DHS Grants and Financial Assistance Division (GFAD) (APPENDIX A: Terms and Conditions).

Before accepting the award, the authorized official should carefully read the award package for instructions on administering the grant award and the terms and conditions associated with responsibilities under Federal Awards. Recipients must accept all conditions in this NOFO as well as any Special Terms and Conditions in the Notice of Award to receive an award under this program.

Reporting

See APPENDIX A: Terms and Conditions for the reporting requirements (financial and performance) successful applicants must comply with during the award's period of performance.

Federal Financial Reporting Requirements

See APPENDIX A: Terms and Conditions

The Federal Financial Reporting Form (FFR) is available here:

SF-425 *OMB #4040-0014*

Program Performance Reporting Requirements

See APPENDIX A: Terms and Conditions

Close Out Reporting Requirements

Within 90 days after the end of the period of performance, or after an amendment has been issued to close out a grant, whichever comes first, recipients must submit a final FFR and final progress report detailing all accomplishments and a qualitative summary of the impact of those accomplishments throughout the period of performance.

If applicable, an inventory of all construction projects that used funds from this program must be reported with the final progress report.

After these reports have been reviewed and approved by DHS FAO, a closeout notice will be completed to close out the grant. The notice will indicate the period of performance as closed, list any remaining funds that will be deobligated, and address the requirement of maintaining the grant records for three years from the date of the final FFR.

The recipient is responsible for returning any funds that have been drawn down but remain as unliquidated on recipient financial records.

Disclosing Information per 2 C.F.R. § 180.335

This reporting requirement pertains to disclosing information related to government-wide suspension and debarment requirements. Before a recipient enters into a grant award with a federal agency, the recipient must notify the federal agency if it knows if any of the recipient's principals under the award fall under one or more of the four criteria listed at 2 C.F.R. § 180.335. At any time after accepting the award, if the recipient learns that any of its principals falls under one or more of the criteria listed at 2 C.F.R. § 180.335, the recipient must provide immediate written notice to the federal agency in accordance with 2 C.F.R. § 180.350.

G. DHS Awarding Agency Contact Information

Contact and Resource Information

1. **Grants Officer**

The Grants Officer is the DHS official that has the full authority to negotiate, administer and execute all terms and conditions of this Award in concurrence with the Program Officer.

Name: Stephanie Dawkins

Email: stephanie.dawkins@HQ.DHS.GOV

2. **Program Manager**

The Program Manager shall be the DHS staff member responsible for monitoring the completion of work and technical performance of the projects or activities described in the Program Narrative statement.

Name: Jeffrey Brownsweiger

Email: Jeffrey.Brownsweiger@HQ.DHS.GOV

3. **Office of University Programs Mailing Address**

S&T Stop 0205

Department of Homeland Security

245 Murray Lane, SW

Washington, DC 20528-0217

H. Additional Information

Extensions

Extensions to this program are allowed. DHS will base extension approvals on the availability of funds, acceptable performance, and the reason(s) for the requested extension. DHS will not provide extensions solely to enable universities to expend unspent funds.

Disclosure

Risk Assessment Evaluation

DHS staff will evaluate the risks to the program posed by each applicant, including conducting due diligence to ensure an applicant's ability to manage federal funds. This evaluation is in addition to the evaluation of the applicant's eligibility and the quality of its application on the basis of the Selection Criteria, and results from this evaluation may assist funding decisions. If an award is made, DHS may apply special conditions that correspond to the degree of risk of the award.

In evaluating risks, DHS may consider the following:

- Financial stability;
- Quality of management systems and ability to meet the management standards prescribed in applicable OMB Guidance;
- Applicant's record in managing previous DHS awards, cooperative agreements, or procurement awards, including:

    1. Timeliness of compliance with applicable reporting requirements
    2. Accuracy of data reported
    3. Conformance to the terms and conditions of previous federal awards
    4. If applicable, the extent to which any previously awarded amounts will be expended prior to future awards
    5. Information available through OMB-designated repositories of government-wide eligibility qualification or financial integrity information, such as: Federal Awardee Performance and Integrity Information System (FAPIIS), Duns and SAM
    6. Reports and findings from single audits performed under Subpart F – Audit Requirements, 2 C.F.R. Part 200 and findings and reports of any other available audits
    7. Applicant organization's annual report
    8. Publicly available information, including information from the applicant organization's website
    9. Applicant's ability to effectively implement statutory, regulatory, or other requirements imposed on award recipients.

In addition, organizations who have not received prior DHS GFAD awards may be required to complete a risk assessment questionnaire as part of the pre-award financial and administrative review.

Applicant Disclosure of High Risk Status

Applicants are to disclose if they are currently designated as high risk by a federal awarding agency. This includes, but is not limited to, any status requiring additional oversight by a federal awarding agency due to past programmatic, administrative or financial concerns. If an applicant is designated as high risk by a federal awarding agency, it should provide an explanation with the application package and include the following information:

- The federal awarding agency that assigned the high risk status;
- The federal awarding agency's point of contact for the risk status, including name, phone number and email address;
- Date of the risk status designation;
- Reason(s) for the risk status.

DHS seeks this information to ensure appropriate federal oversight of all grant awards. The disclosure of an organization's risk status does not disqualify it from receiving an award; however additional grant oversight may be required. If necessary, this information will be provided in the award documentation. Failure to disclose high risk status may result in award termination or other remedies.

APPENDIX A: Terms and Conditions

In addition to the DHS Standard Administrative Terms and Conditions, which are available online at: http://www.dhs.gov/publication/fy15-dhs-standard-terms-and-conditions, the following Terms and Conditions apply specifically to this COE Award as administered by the DHS Grants and Financial Assistance Division (GFAD):

CENTER OF EXCELLENCE (COE)

COOPERATIVE AGREEMENT TERMS AND CONDITIONS

GRANTS AND FINANCIAL ASSISTANCE DIVISION (GFAD)

In addition to the Department of Homeland Security (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 GFAD:

ARTICLE I. ADMINISTRATIVE TERMS AND CONDITIONS

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

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

2. Recipient shall compete fully and fairly, to the maximum extent practicable, all projects funded under this Award unless DHS has approved otherwise.

3. 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 communication and transition activities;

        iii. Summary of Center management efforts including management decision making apparatus;

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

            - Objective/Purpose
            - Baseline
            - Methodology

- Project milestones
- Performance metrics used to evaluate progress & assessments of current concept of operations and baselines/state of the art in use
- Transition plans to include development steps, intellectual property management plans, & market specific considerations
- Stakeholder engagement
- Potential programmatic risks to completion; and,
- Project outcomes and outputs, including information on how project outcomes will advance or impact current policies, procedures, technologies or capabilities.

v. Budget information categorized by both object class and project, including budget justification. DHS requires Centers to submit a budget that maps to the key competencies and activities necessary for a Center to deliver useful technologies and knowledge products to the Department. The competency areas also align to the criteria DHS utilizes to evaluate its Centers of Excellence Program. Centers should allocate resources in the following categories: Administration & Execution, Research & Development, Education & Training, Customer Outreach & Communication, and Transition. The following categories should be included in the budget request. Centers should work with PM's to identify minimum expenditures in each category necessary to address Biennial Evaluation Criteria:

1. Administration and Execution (labor)
    a. Director
    b. Executive Director
    c. Professional Project Management Staff & Financial Staff
    d. Travel to sub-contractor sites
2. R&D
    a. Principal Investigator & supporting investigators (labor)
    b. Data acquisition (licenses, fees, etc.)

c. Materials

d. Supplies

e. Equipment

f. Facilities

g. Project travel (consistent with iv. Customer outreach)

3. Education and Training

a. Staff (labor)

b. Scholarships

c. Fellowships

d. Internships

e. Workforce development classes/webinars/seminars

f. Course & curriculum development (labor)

g. Summer workshops (labor, facilities, materials)

h. MSI program support (labor)

4. Customer Outreach and Communication

a. Professional Strategic Communications Expert (labor)

b. Communications support staff (labor)

c. Travel for all Center functions to DHS customers including project level travel

d. Communication services, products, materials

e. Annual meeting and outreach events – not including travel (technical and customer engagements)

5. Transition

a. Technology development professional (labor)

b. IP due diligence costs (labor legal)

c. Business planning evaluations – financial modeling to support stage gate decisions (labor business)

d. IP submission costs e.g. trademark, copyright expenses

e. Market assessments (labor)

f. Licensing costs for background IP

g. Initial operations and maintenance costs (vendor services)

h. Unit testing and evaluation – (labor , facilities, supplies/equipment/materials)

i. Concept or technology integration costs (in customer environments or to meet final customer requirements, e.g. FISMA accreditation)

4. 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.

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

6. 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.

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

8. DHS has an interest in publications generated from DHS-funded research for program awareness. Recipient shall forward publications to the DHS Program Officer as follows:

    a. On a quarterly basis one electronic and one hard copy of all publications generated under this Award; and

b. Prior to publication, one electronic copy of any near-final pre-publication draft.

Please refer to Article II. Section L for information on Enhancing Public Access to Publications.

9. 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.

10. Data Acquisition and Management Plan

    a. Within thirty (30) days of 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's Technology, Security, Privacy, and/or Information offices, as appropriate, prior to submission to DHS. The Recipient shall submit its plan to the DHS Program Officer for review and comment within thirty (30) days of 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 (see 11e for data definitions):

        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.

11. Information Protection Plan: The Parties agree that all research conducted under this Award is intended to have publicly releasable results. Accordingly, no research under this Award should involve, use, or generate sensitive information, which includes PII, and/or classified information (see Item d of this section for Definitions). As a condition of access to this COE, DHS agrees not to provide the Recipient any data or information that is sensitive or classified, i.e., information or data that would not be released completely in response to a request under the Freedom of Information Act, 5 U.S.C. § 552. Should the Recipient receive any data or information from DHS that the Recipient has reason to believe may be sensitive or classified, within 24 hours, the Recipient shall (1) notify the DHS Grants Management Specialist named in the award documents; (2) shall send such data or information to the Grants Management Specialist, unless otherwise directed by DHS; (3) shall erase or otherwise destroy any vestige of such data or information in its records and computer systems; and (4) shall notify the Grants Management Specialist of the means and time of such destruction.

    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.

    a. 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.

    b. 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.

c. 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.

d. 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.

e. 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 DHS (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.

12. Information Technology Security

a. As a condition of access to this COE, DHS agrees not to provide the Recipient any data or information that is sensitive or i.e., information or data that would not be released completely in response to a request under the Freedom of Information Act, 5 U.S.C. § 552. Should the Recipient receive any data or information from DHS that the Recipient has reason to believe may be sensitive or classified, within 24 hours, the Recipient shall (1) notify the DHS Grants Management Specialist named in the award documents; (2) shall send such data or information to the Grants Management Specialist, unless otherwise directed by DHS; (3) shall erase or otherwise destroy any vestige of such data or information in its records and computer systems; and (4) shall notify the Grants Management Specialist of the means and time of such destruction.

13. 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.

14. 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 SMEs 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.

15. Public Communication: The Recipient shall input and update all required project information into relevant webpage(s) hosted on the www.hsuniversityprograms.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.

16. COE Science and Engineering Workforce Development:

Should the COE work with DHS through this initiative, the recipient shall follow the below terms and conditions:

a. DHS must ensure that U.S. citizens are trained in homeland security-related science and engineering disciplines in order to maintain U.S. leadership in science and technology, as required by the Homeland Security Act of 2002. Only U.S. citizens can work with federal, state and local agencies in the agencies' secure offices and operating environments, and can obtain security clearances and access to sensitive information needed to conduct research into homeland security issues.

b. Under this initiative, each COE may use COE Science and Engineering Workforce Development tuition assistance and stipends to support U.S. students studying the topics of, and working on homeland security research projects of their COEs.

Ninety-two percent (92%) of funds must go directly to support undergraduates, graduates, or a combination of undergraduate and graduate, students who are U.S. citizens working in the recipient COE's research area.

c. All students supported by COE Workforce Development funds shall report directly to COE faculty or staff, and shall work primarily on COE projects. Student participation in COE activities must take precedence to other research or employment for students to be eligible for COE support. COE activities include but are not limited to the following: supporting COE management activities, working on COE research projects, teaching, and experiential learning related to COE research topics.

d. Grants may be used to complement existing funding sources for students that are selected as participants, but may not supplant or be used in lieu of other COE funds. ***DHS expects a net increase in the number of students supported in COE programs funded through this section. These funds must be awarded only to newly supported students.***

e. All COEs working with DHS on this initiative must develop and submit a Workforce Development work plan to DHS Program Manager 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.

   The work plan shall include:

   i. A description of the COE's established or proposed science and engineering research and coursework including how research experiences will be incorporated in to the program.

   ii. Details of an application and award process for selecting recipients. This process must include input from external SMEs. Qualified students must meet the following minimum standards:

      1. Must be U.S. citizens.

      2. Must achieve and maintain a cumulative GPA of 3.30 or higher on a 4.00 scale, averaged over all academic terms.

      3. Must major in priority science and engineering-related discipline associated with the COE research areas. ***These funds may not be used to support the completion of professional degrees (law school, medical school, etc.)***

      4. NOTE: Many positions in the homeland security field require a background check. Therefore, the student selection process and

program experiences should include plans to address these requirements.

5. A commitment to facilitate student attendance at a professional conference within a science and engineering-related field of study.

6. A description of how the COE will assign qualified academic mentors for each recipient from the student's field of study.

7. A plan to make awards within one year of receipt of funds. Recipient institutions must award tuition assistance and stipends to students attending COE-affiliated institutions and working on COE research, development or technology transition projects. The students must be supported for up to 2 years for undergraduates and 3 years for graduate students or for the duration of their studies whichever is less. COEs may adjust this amount to account for other monetary awards to individual students.

8. For undergraduates, awards shall cover up to 100% but not less than 50% of tuition and mandatory fees (or equivalent), plus a stipend of no more than $1,200 per month for twelve months. Stipends can be less than $1,200 per month if appropriate for the geographic region or if paid summer internships can be secured.

9. For graduate students, awards shall cover up to 100% but not less than 50% of tuition and mandatory fees (or equivalent), plus a stipend of no more than $2,700 per month for twelve months. Stipends can be less than $2,700 per month if appropriate for the geographic region or if paid internships can be secured.

iii. A plan for identifying and placing students in the two required ten week internships that complement DHS COE approved research or are operational venues that work in the COE field of study. Internships should take place away from the student's home institution. Students must receive a stipend and travel/lodging support to an internship location during summer months for 2 summers if paid internships cannot be secured. Funds budgeted for stipends during summer months may be re-budgeted if paid internships are secured.

iv. Details of a strategy to ensure supported students proactively seek and obtain paid employment within the HSE (DHS, SLTT government, etc.) for at least one year after graduation.

1. Employment requirement will be waived for those entering the military /military school, or with a commitment to teach Science and Engineering at the elementary or secondary level.

2. Undergraduate students will be allowed a deferment of the one year service requirement if they have been accepted into a Science and Engineering related graduate program. Include a plan for managing and tracking this type of deferment.

v. An approach to evaluating student success

vi. A plan to monitor the activity of individual students to assure compliance with program requirements; develop a mitigation strategy; and establish procedures to ensure funds are used appropriately.

vii. A plan to monitor student's homeland security employment placement for up to six years after graduation from the program.

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 work plan 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 HSE 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 SMEs 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 R&D 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 will be subject to DHS's publications approval process prior to dissemination of the publication as required under Item 9, in Section A.

8. DHS shall review and provide comments on the Recipient's Information Protection Plan as required under Item 11 in Section A.

9. DHS shall review and provide comments on the Recipient's Research Safety Plan as required under Item 14, in Section A.

10. DHS may create a Board of Directors that provides guidance and direction to the DHS Program Officer regarding the Recipient's research plan.

11. DHS may invite subject matter experts, customers, or stakeholders to assist in evaluating the Center's annual work plan, 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 REVISION

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. 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.

2. 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 sixty (60) 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

1. 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 written 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.

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

G. PERFORMANCE REPORTS

1. Performance Reports. The Recipient shall submit semiannual performance reports to the DHS Grants Officer for review and acceptance by DHS as a condition for receiving further annual funding increments. Semi-Annual performance reports are due 6 months after the start of each budget year and no later than sixty (60) 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 the DHS Grants Office and 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 based on the activities discussed in the corresponding work plan. These reports should map work plan activities (activities planned) to those activities performed during the year to include:

    i. Summary reports on the Center's strategic vision and support justification

    ii. Summary of Center communication and transition activities;

    iii. Summary of Center management efforts including decision making apparatus;

    iv. Performance reports on each Center Project should include:

        - Explanation of any changes from the initially approved work plan
        - Objective/Purpose
        - Baseline
        - Methodology
        - Project milestones
        - Performance metrics used to evaluate progress & assessments of current concept of operations and baselines/state of the art in use
        - Transition plans to include development steps, intellectual property management plans, & market specific considerations
        - Stakeholder engagement
        - Potential programmatic risks to completion; and,
        - Progress against each milestone outcomes and outputs and explanation of why any items were not reached
        - Unanticipated problems and plans for addressing them; and
        - Information supported by data on how project outcomes will advance or impact current technologies or capabilities.

    v. Budget information and expenditure (narrative and figures) categorized by both object class and project as described in Article 1, Item A.3.

vi. If applicable, include a certification that no patentable inventions were created during the budget period.

vii. 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. Annual COE Science and Engineering Workforce Development Report. COEs working with DHS through the COE science and engineering workforce development initiative will submit a separate Science and Engineering Workforce Development Annual Performance Report to the DHS Grants Officer.

a. The report shall compare actual accomplishments to the approved project objectives and shall include:

i. A program overview section on the goals, objectives and accomplishments to date; total number of students supported; total number of students graduated; total number of students still enrolled; number of graduate students supported; number of undergraduate students supported; total number of students currently employed full time in a Homeland Security related position

ii. A student report for each supported student including: student name; current status of student (graduated/enrolled); degree (masters, bachelors, PhD); major; dates of funding; total funding amount; description of complete internship/research experiences; workshops/conference attended; publications, presentations, poster sessions; other relevant accomplishments/success stories; copy of student resume

3. 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

4. The Final COE Science and Engineering Workforce Development Performance Report. COEs working with DHS through the COE science and engineering workforce development initiative will submit final reports within ninety (90) days after the expiration date of the performance period of this initiative to the DHS Grants Officer.

    a. The Final COE Science and Engineering Workforce Development Performance Report shall include:

        i. Post completion employment plans for each student scholar/fellow or an explanation for student leaving the program.

        ii. Summary of research accomplishments and contributions, post-award activity and post-graduation placement, new skills or knowledge acquired

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 10 years, unless extensions are approved. All COEs' annual performance periods shall run from July 1 to July 30 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 D), 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 12 months, from July 1, through June 30 of the following year.

    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 unless otherwise notified by DHS Grants and Financial Assistance Officers) 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 and a revised Center budget consistent with Article A. Item 3

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.

iii. 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

iv. COE Science and Engineering Workforce Development annual workplan and budget justification: COEs retain the ability to balance financial support as appropriate if students have or will receive other sources of funding. Should the COE work with DHS through this initiative, the recipient will submit an annual workplan described in Article A, Item 16.

I. PRIOR APPROVAL REQUIRED

1. 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 AND RETENTION 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 AND EXPORT CONTROLS GROUP 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 CAPM. Additional guidance regarding the review process is provided in the following sections, along with contact information. 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, testing, evaluation, 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 review of all such projects, including classified projects; projects involving biological and/or chemical agents, surrogates, or simulants; and non-laboratory activities related to biological and/or chemical agents (e.g., literature reviews, simulations, and/or modeling activities) to be systematically evaluated for compliance at inception, prior to funding approval, whenever there are any project changes, 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 biological and/or chemical defense-related effort (including non-laboratory activities related to biological and/or chemical agents) 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) and a Statement of Work.

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 project modification and/or whenever in the course of project execution an issue potentially raises a compliance concern**: an updated TCF and an updated Statement of Work detailing the proposed modification (updates should be highlighted to assist with timely reviews). The proposed project modification must receive written approval from CAPO prior to initiation. Examples of project modifications include – but are not limited to—the addition of agents, a change in performer, modifications to the scope of work, and changes to the technical approach.

   The Recipient should contact the CAPO regarding treaty compliance issues at treatycompliance@hq.dhs.gov to: obtain the TCF, submit the completed TCF, and/or request additional guidance regarding treaty compliance documentation and review requirements, as applicable to (1) new biological and/or chemical defense- related efforts, or (2) modifications to previously approved efforts. The CAPO will review all submitted materials and provide written confirmation of approval 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, prior to 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*,* Rev 01, *Biosafety*; DHS Instruction 066-02-001, *Biosafety;* and any local institutional policies that may apply for Recipient institution facilities performing work under this Award. The CAPO 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 CAPO at STregulatorycompliance@hq.dhs.gov for guidance on the requirements, and then submit all required documentation based on CAPO 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 or synthetic nucleic acid molecules; (2) Biological Select Agents and Toxins or 'BSAT'; or (3) biological agents, toxins, or other biological materials that are not recombinant, synthetic, or 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 CAPO 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 five (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 or Synthetic Nucleic Acid Molecules. Laboratory activities involving recombinant or synthetic nucleic acid molecules research are defined by the *NIH Guidelines for Research Involving Recombinant or Synthetic Nucleic Acid Molecules, "NIH Guidelines"*. Each Recipient and any Recipient institution shall conduct all such work in compliance with the NIH Guidelines. In addition to the documentation referenced above, **each facility conducting research activities involving recombinant or synthetic nucleic acid molecules under this Award must submit copies of the following documentation to the CAPO 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 recombinant or synthetic nucleic acid molecules research protocol(s); and

d. Documentation of final IBC approval for each recombinant or synthetic nucleic acid molecules 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 CAPO 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, Rev 01, *Safeguarding Select Agents and Toxins*; and DHS Instruction 026-03-001, *Safeguarding Select Agents and Toxins.* **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 CAPO for review prior to the initiation of such activities:**

   a. Current APHIS/CDC Certificate of Registration;

   b. Current versions of the Biosafety, Security, and Incident Response Plans required and reviewed under the Select Agent Regulations; and

   c. 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 CAPO at STregulatorycompliance@hq.dhs.gov to obtain the CAPO Documentation Request Checklist, submit documentation, or request more information regarding the DHS CAPO documentation and compliance review requirements. The CAPO will provide written confirmation of receipt of all required documentation to the designated Point(s) of Contact. The CAPO 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 CAPO will review all submitted materials and provide written confirmation to the Recipient once all requirements have been met.

CAPO 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 CAPO 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 CAPO, 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 the CAPO with documentation sufficient to illustrate this compliance. The CAPO 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 CAPO's formal written approval.

E. REGULATORY REQUIREMENTS FOR 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; any additional requirements set forth in the DHS Directive 026-01, Rev 01, *Care, Use, and Transportation of Animals in Research;* and DHS Instruction 026-01-001*, Care, Use, and Transportation of Animals in Research.* **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 CAPO 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) accreditation letter 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 CAPO at STregulatorycompliance@hq.dhs.gov. Additional documentation may be required in some cases and must be submitted upon request. The CAPO 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 CAPO. **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 CAPO.**

The Recipient, as well as any Recipient institution and partner institutions conducting animal research under this Award, shall also comply with ongoing CAPO 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 CAPO 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 accreditation letter, as applicable.

The Recipient must promptly report the following to the CAPO, 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.

3. 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 DHS approval for work involving animals. All entities involved in activities under this Award must comply with their own applicable national and regional/local regulations, standards and guidelines. The Recipient must provide CAPO documentation sufficient to illustrate this compliance. The CAPO 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 CAPO.

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

The Recipient and any Recipient institutions shall conduct all research involving agents and toxins identified in sections III.1 and 6.2.1 of the *USG Policy for Oversight of Dual Use Research of Concern and USG Policy for the Institutional Oversight of Dual Use Research of Concern*, respectively, in accordance with both policies referenced above and in accordance with any additional requirements set forth in related DHS policies and instructions. Under this award, each Recipient and any Recipient institutions planning to perform research involving agents and toxins identified in sections III.1 and 6.2.1 of the USG DURC policies, regardless of the funding source, must submit the following documentation outlined in this section for CAPO review. Institutions were required to implement the policy on or by September 24, 2015.

1. Requirements for Research Using DURC Agents and Toxins. To ensure compliance with the USG DURC Policies, each facility conducting research involving the agents and toxins identified in sections III.1 and 6.2.1 of the USG DURC Policies, regardless of funding source, must submit the following documentation for compliance review by CAPO prior to the initiation of such activities:

    a. Institutional Review Entity (IRE) charter, and/or other available documentation of IRE policies and procedures, to include the contact information for the Institutional Contact for DURC (ICDUR);

    b. Institution's project-specific risk mitigation plan, as applicable;

    c. DURC training or education program description;

d. Formal annual assurance of compliance with the USG Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern;

e. A completed iDURC form and a Statement of Work.

2. Required Notifications to DHS:

   a. Within 30 calendar days of initial and periodic reviews of institutional review of research with DURC potential, notify CAPO of the results, including whether the research does or does not meet the DURC definition.

   b. Report, in writing, any instances of noncompliance and mitigation measures to correct and prevent future instances of noncompliance within 30 calendar days to CAPO.

3. Flowdown Requirements: The Recipient shall include the substance of this section in all sub-awards/contracts at any tier where the sub-Recipient is performing work with agents or toxins identified in sections III.1 of the *USG Policy for Oversight of Dual Use Research of Concern and 6.2.1 of the USG Policy for the Institutional Oversight of Dual Use Research of Concern.*

   The Recipient should contact CAPO at STregulatorycompliance@hq.dhs.gov to submit documentation or to request more information regarding the DHS regulatory documentation and compliance review requirements. CAPO will provide written confirmation of receipt of all required documentation to the designated Points of Contact. CAPO will evaluate the submitted materials. Additional documentation may be required in some cases and must be submitted upon request. CAPO will review all submitted materials and provide written confirmation to the Recipient once all requirements have been met. Upon receipt of this written confirmation, the Recipient may initiate approved projects under this award.

   In order to meet the reporting requirements set forth in section IV.2 of the *2012 USG Policy for Oversight of Life Sciences Dual Use Research of Concern* (the biannual DURC Data Call), the Recipient and any Recipient institution shall submit documentation regarding all active, planned or recently completed (within twelve months of the submission) unclassified intramural or extramural activities on Federally-funded or conducted life science research projects biannually on the first Monday in May and November. The Recipient should contact CAPO at STregulatorycompliance@hq.dhs.gov to submit documentation. Documentation should include an update on all listed activities, including status, all agents or toxins incorporated by strain or surrogate name, performers, contract information, and sites of activities. Documentation should also include any changes to existing or completed projects since the most recent submission, including—but not limited to—the addition of agents, a change in performer, modifications to the scope of work, and/or changes to the technical approach. A

supplemental report detailing all work involving low pathogenic avian influenza virus H7N9 (LPAI H7N9) and Middle East Respiratory Syndrome Coronavirus (MERS-CoV).

4. 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 the iDURC policy. The Recipient must provide CAPO documentation sufficient to illustrate this compliance. CAPO 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 CAPO's formal written approval.

G. REGULATORY REQUIREMENTS FOR 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 6 C.F.R. § 46, Subparts A, and 45 C.F.R. § 46, Subparts B-D, DHS Directive 026-04, Rev 01, *Protection of Human Subjects*, and DHS Instruction 026-04-001, *Ensuring Human Subjects Research Compliance*, 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 CAPO 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 CAPO. Each Recipient must submit the following documentation to the CAPO 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 CAPO. Exemption determinations made by an OHRP-registered IRB, or equivalent, should be submitted to the CAPO 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 CAPO review. DHS Program Officers (or institutions conducting human subjects' research under this Award) seeking an exemption determination from the CAPO 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 CAPO at STregulatorycompliance@hq.dhs.gov. The submitted documentation will be retained by the CAPO 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 CAPO before a certification letter is issued and participant enrollment can begin under this Award. The CAPO 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 CAPO, 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 CAPO 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 CAPO 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 CAPO.

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 CAPO 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, PATENT, AND DATA 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 contributed in the 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 **{insert Award Number as outlined in Item #5 on Notice of Award cover page}**

    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 and DHS S&T Logo.

    Recipient shall not use the DHS seal. Recipient shall acquire DHS's approval prior to using the DHS S&T logo.

3. Enhancing Public Access to Publications: Per Article I. Section A. DHS requires that the Recipient shall forward one electronic (PDF) copy of all publications generated under this award to the Program Officer at the time of publication. The Program Officer will make all publications publically available by posting on www.hsuniversityprograms.org in a manner consistent with copyright law no later than 12 months after the official date of publication. 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 200.339.

O. TRAVEL

Travel required in the performance 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 May, 2015

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. Application and Assurances dated May, 2015

R. CLASSIFIED SECURITY CONDITION

1. "Classified national security information," as defined in Executive Order (EO) 12958, as amended, means information that has been determined pursuant to EO 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

2. No funding under this award shall be used to support a contract, sub-award, or other agreement for goods or services that will include access to classified national security information if the award recipient itself has not been approved for and has access to such information.

3. Where an award recipient has been approved for and has access to classified national security information, no funding under this award shall be used to support a contract, sub-award, or other agreement for goods or services that will include access to classified national security information by the contractor, sub-awardee or other entity without prior written approval from the DBS Office of Security, Industrial Security Program Branch (ISPB), or, an appropriate official within the Federal department or agency with whom the classified effort will be performed.

4. Such contracts, sub-awards, or other agreements shall be processed and administered in accordance with the DHS "Standard Operating Procedures, Classified Contracting by State and Local Entities," dated July 7, 2008; EOs 12829, 12958, 12968, as amended; the National Industrial Security Program Operating Manual (NISPOM); and/or other applicable implementing directives or instructions.

5. Immediately upon determination by the award recipient that funding under this award will be used to support such a contract, sub-award, or other agreement, and prior to execution of any actions to facilitate the acquisition of such a contract, sub-award, or other agreement, the award recipient shall contact ISPB, or the applicable Federal department or agency, for approval and processing instructions.

   DHS Office of Security ISPB contact information:

   Telephone: 202-447-5346

   Email: DD254AdministrativeSecurity@hq.dhs.gov

   Mail: Department of Homeland Security

Office of the Chief Security Officer

ATTN: ASD/Industrial Security Program Branch

Washington, D.C. 20528

APPENDIX B: Acronyms

List of commonly used acronyms in this NOFO:

AOR:	Authorized Organization Representative
CAPO:	Compliance Assurance Program Office
CBP:	Customs and Border Protection
CFDA:	Catalogue of Federal Domestic Assistance
CIP:	Component Intelligence Programs
CIS:	Citizenship and Immigration Services
CISA:	Cybersecurity and Infrastructure Security Agency
COE:	Center of Excellence
DHS:	U.S. Department of Homeland Security
DUNS:	Data Universal Numbering System
E2E:	End-to-End
ECG:	Export Control Group
FEMA:	Federal Emergency Management Agency
FLETC:	Federal Law Enforcement Training Center
FFRDC:	Federally Funded Research and Development Center
GFAD:	Grants and Financial Assistance Division
HSE:	Homeland Security Enterprise
I&A:	Office of Intelligence and Analysis
IC:	Intelligence Community
ICE:	Immigration and Customs Enforcement
IE:	Intelligence Enterprise
MC:	Mission Centers
MSI:	Minority Serving Institution
NOFO:	Notice of Funding Opportunity
OUP:	Office of University Programs
PPD:	Presidential Policy Directive
QHSR:	Quadrennial Homeland Security Review
R&D:	Research and Development
SAM:	System for Award Management
S&T:	Science and Technology Directorate
SLTT:	State, Local, Tribal and Territorial (Government)
SME:	Subject Matter Expert
STEM:	Science, Technology, Engineering and Mathematics
TPCR:	Terrorism Prevention and Counter Terrorism Research
TSA:	Transportation Security Administration
USCG:	U.S. Coast Guard
USSS:	U.S. Secret Service

APPENDIX C: End-to-End Approach

The End-to-End (E2E) approach blends concepts from various management models to deliver university created technologies that meet the needs of DHS and other HSE customers. The approach supports the development of relevant knowledge, technologies, and capabilities using a milestone-driven approach to transfer and transition efforts from the Centers to appropriate partners or customers. The E2E initiative includes phased-milestone reviews, continual market research, early and ongoing customer involvement, intellectual property management, test and evaluation exercises, and strategic partnering (Figure 4).

After every two years of operation, OUP and the COE leadership will conduct a Biennial Review to review each project within the COE portfolio. Low-scoring projects will be eliminated and funding will be reallocated to new or existing projects. At the conclusion of the first Biennial Review, the COE must identify high-scoring project(s) that will utilize the E2E approach, and then form a supporting project team. This team of people must represent all phases of the technology creation-transition-adoption continuum, from early stages of research to use in practice. Using the E2E approach will focus the project team on proposed research goals, data collection, analytical approaches, performance metrics, outcomes and outputs, market assessments, potential transition paths, test and evaluation plans, intellectual property issues, legal and privacy issues, practical barriers to technology adoption, and development of comprehensive case studies.

The E2E approach involves much more hands-on management, planning, and engagement with outside parties by a COE Director or management team than is common in most academic research. The E2E approach can encompass a single larger research project, or it can integrate several related projects under the direction of a single management team that works closely with the researchers, project advisors, commercial partners, HSE customers, and SMEs. There may be significant uncertainty in assessing potential outcomes for early stage E2E initiatives. Some uncertainty will be eliminated by conducting a thorough market assessment for the technologies being developed. Most importantly, COE lead applicants must demonstrate a willingness to partner with customers to facilitate transition of their research into use, and describe how they would accomplish this. Note: DHS does not expect all team members of principal investigators to have a complete understanding of transition issues, but to be able to identify and recruit people that do for as long as needed.

The following are key characteristics of the E2E approach:

- A multi-year timeframe (3-5 years)
- A multi-disciplinary approach
- A formal commitment, (e.g., Memorandum of Understanding (MOU), by the intended customers to work directly with the COE throughout the life of the project) [Note: an MOU is not required at the application stage].
- Clear understanding and deadlines
- Exchange opportunities for students, researchers, and homeland security practitioners to foster mutual understanding of academic research and real-life experience in operational environments, and

- A transition plan that addresses the following questions:
    - What is the customer need?
    - What is the gap in knowledge, capabilities, or technology?
    - How would the proposed project significantly advance existing customer capabilities? (i.e., how will the research make the Nation more secure or make homeland security operations more cost-effective)?
    - Who are the key partners to enable effective transition?
    - How would the COE address intellectual property (IP) challenges, and how would the COE share IP among team members?
    - What is the potential market for the technology or other research results? (e.g., recipients will conduct both a technology "horizon scan" and a market assessment at the appropriate times)
    - Who would be responsible for post-transition management, repair, updates, training, and operations and maintenance?
    - At what point would the research product(s) be handed off to a customer? (e.g., will the output become part of an official government system, remain a service offering within the university complex, or be delivered (sold, licensed) to a commercial interest)?
    - How would the Center work with customers to identify testing, evaluation, or standards needed for customers to incorporate outputs into their operations?
    - What training curricula or materials would be needed to support successful transition?
    - What are the metrics for measuring the ongoing progress and success of the effort?

To recap, a successful E2E project will capture the life-cycle of a research effort starting with an idea and ending with a working product in the hands of a customer. In addition, E2E should support education and training opportunities in real-world venues for new and existing faculty, research staff, and students. The site visit presentation to DHS leadership should provide an overview of how the prospective COE leadership team would expect the E2E project to reach fruition.

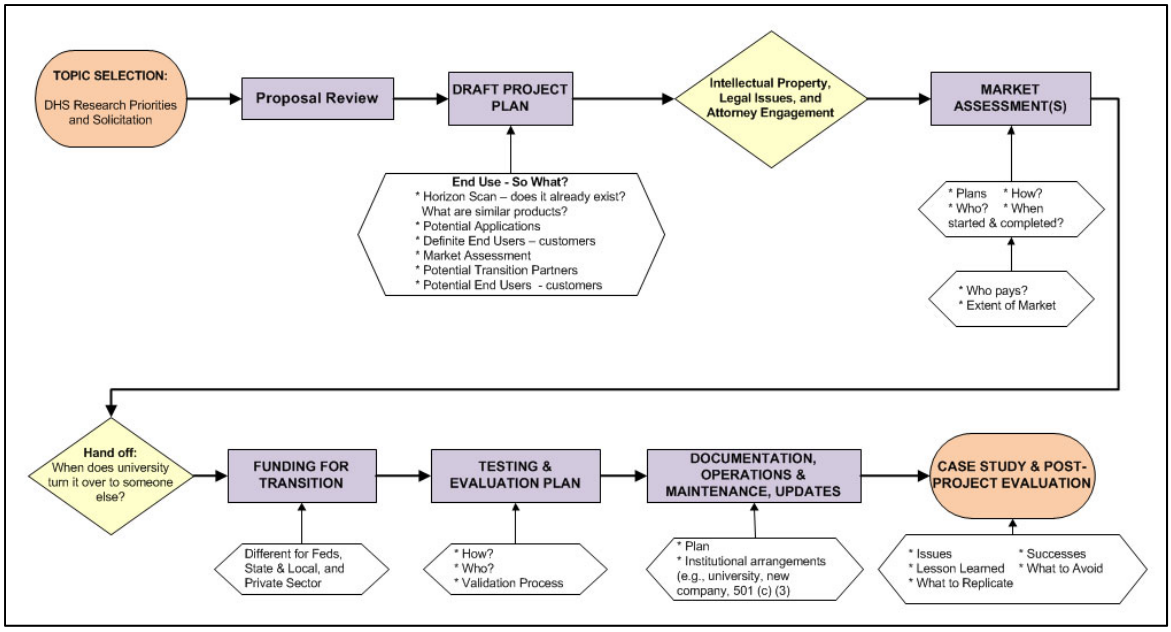


Figure 3: E2E Approach

APPENDIX D: References for Themes, Topics and Questions

The following list of publications is provided as a resource for applicants. While this list is not exhaustive, it does represent key policy documents and reports used in the development of this NOFO. Applicants are expected to be aware of the diversity of available studies, policy documents, and findings relevant to this NOFO.

National Strategic Documents

- 2012 National Strategy for Information Sharing and Safeguarding: https://obamawhitehouse.archives.gov/sites/default/files/docs/2012sharingstrategy_1.pdf
- Quadrennial Homeland Security Review (QHSR): http://www.dhs.gov/quadrennial-homeland-security-review
- DHS Strategic Plan FY2014 – 2018: http://www.dhs.gov/sites/default/files/publications/FY14-18%20Strategic%20Plan.PDF
- DHS Office of I&A Strategy: Fiscal Year 2011 – 2018: https://www.dhs.gov/xlibrary/assets/ia-fy2011-fy2018-strategic-plan.pdf
- National Strategy for Information Sharing and Safeguarding 2012: https://obamawhitehouse.archives.gov/sites/default/files/docs/2012sharingstrategy_1.pdf
- DHS Strategy for Countering Violent Extremism 2016 https://www.dhs.gov/sites/default/files/publications/16_1028_S1_CVE_strategy.pdf
- *National Strategy for Counterterrorism of the United States of America*, October 2018, https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf
- *National Strategy for Counterterrorism*, June 2011. https://obamawhitehouse.archives.gov/sites/default/files/counterterrorism_strategy.pdf
- *National Strategy for Combating Terrorism.* https://georgewbush-whitehouse.archives.gov/nsc/nsct/2006/
- HSPD-8 *National Preparedness*- set forth in 2011, this directive establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities.[13]
- National Intelligence Strategy of the United States of America 2014 https://www.dni.gov/files/documents/2014_NIS_Publication.pdf
- U.S. Public Law 107–296, *Homeland Security Act of 2002*- Created DHS to prevent terrorist attacks, reduce U.S. vulnerability to terrorist attacks, and minimize damage and assist in recovery from terrorist attacks that occur in the United States.
- U.S. Public Law 110-53, *Implementing Recommendations of the 9/11 Commission Act of 2007*- Enacted wide-ranging legislation with many components including replacing the

[13] "HSPD-8 National Preparedness". Government Publishing Office. Weekly Compilation of Presidential Documents (December 22, 2003), v.39 n.51, p.1822-1826 https://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1745.pdf

DHS Directorate of Information Analysis and Infrastructure Protection with I&A and a separate Office of Infrastructure Protection as one step to improve information.

- U.S. Public Law 108-458, *Intelligence Reform and Terrorism Prevention Act (IRTPA)*. – reformed the IC and information sharing practices, including establishing the Director of National Intelligence (DNI) and National Counterterrorism Center (NCTC) in response to the 9/11 Commission Report. The Office of DNI (ODNI) integrates intelligence from foreign, military and domestic sources and is considered the head of the IC.
- U.S. Public Law 111-352, *Government Performance and Results Act (GPRA) Modernization of 2010*- required all federal agencies to collaborate on everything from information sharing to operations.
- Critical infrastructure and key resources provide the essential services that underpin American society. The Nation possesses numerous key resources, whose exploitation by terrorists, or destruction by catastrophic disruptions, could cause severe health effects or mass casualties comparable to those from the use of a weapon of mass destruction. In addition, some critical infrastructure is so vital that its incapacitation, exploitation, or destruction by terrorists would have a debilitating effect on U.S. security and economic well-being.[14] To help mitigate this risk, in 2003, the White House issued Homeland Security Presidential Directive Seven (HSPD-7): *Critical Infrastructure Identification, Prioritization, and Protection*. This directive institutes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.[15]

[14] DHS. https://www.dhs.gov/homeland-security-presidential-directive-7

[15] "Homeland Security Presidential Directive7: Full Text". DHS. December 17, 2003. https://www.dhs.gov/homeland-security-presidential-directive-7

APPENDIX E: Checklist for Applicants

This checklist is meant to provide applicants with a starting place in developing and submitting a responsive proposal. Applicants will be evaluated against the criteria outlined in the NOFO, **not** this checklist.

Did you:

- ☐ Read entire NOFO
- ☐ Ensure you are eligible to apply (Section C. Eligibility Information)
- ☐ Familiarize yourself with past and current research at the current COE Network at https://www.dhs.gov/st-centers-excellence
- ☐ Respond to all required sections described in in the NOFO. Areas to consider may include:
  - ☐ How you will build your team to cover the necessary skills in program management, intellectual property, technology test and evaluation, finance, and scientific expertise
  - ☐ How you communicate your knowledge of DHS CBP, TSA, FEMA, I&A, ICE, USSS, CISA, and S&T operations and technical needs
  - ☐ How you would address the major theme areas
  - ☐ Topics you propose to address for each theme area
  - ☐ Two example End-to-End (E2E) projects in different theme areas
  - ☐ How your research program is original and/or innovative
  - ☐ Project goals, approaches, and methodologies
  - ☐ Relevance to the homeland security mission for every project you propose
  - ☐ How project results would be transitioned to customers
  - ☐ How your program will be integrated with both internal and external partners
  - ☐ Qualifications of personnel and suitability of facilities
  - ☐ How you will manage the Center
  - ☐ How you will work closely with DHS Component agencies and other homeland security practitioners to identify priority research
  - ☐ How education programs will complement the research to increase homeland security community workforce development, for both current and future workforce.
- ☐ Submit all forms listed in the "Content and Form of Application Submission section " section
- ☐ Funding requested does not exceed the available funding for the NOFO
- ☐ Project period requested does not exceed the NOFO
- ☐ Submit application by Deadline: September 13th, 2019 at 11:59:59 PM EDT
- ☐ Mark your calendar for the Informational Webinar for interested applicants on August 6th at 3:00 PM EDT.