The Department of Homeland Security (DHS)
Notice of Funding Opportunity (NOFO)
DHS Science and Technology Directorate (S&T) Center of Excellence (COE)
Center for Cross-Border Threat Screening and Supply Chain Defense – 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. Application Project Narrative 20
III. Research and Workforce and Professional Development Themes, Topics, and Questions 24

B. Federal Award Information 34

Award Amounts, Important Dates, and Extensions 34

C. Eligibility Information 36

Eligible Applicants 36
Eligibility Criteria 37
Cost Share or Match 38

D. Application and Submission Information 38

Submission Date and Other Key Dates and Times 38
Address to Request Application Package 39
Informational Webinar 39
Optional Forms 42
Other Submission Requirements 42
Funding Restrictions 44
Indirect (Facilities & Administrative (F&A)) Costs 44

E. Application Review Information 44

Review and Selection Process 44

I. Scientific Quality Review (External Review) 45
II. DHS Relevancy Review (Internal DHS SMEs) 47

Application Evaluation Criteria 48

I. Evaluation Criteria 48

F. Federal Award Administration Information 55

Notice of Award 55

I. Work Plan Development Workshop 55

Administrative and National Policy Requirements 55
Reporting 56

See Error! Bookmark not defined.

See Error! Bookmark not defined.

See Error! Bookmark not defined.

G. DHS Awarding Agency Contact Information 57

Contact and Resource Information 57

H. Additional Information 57

Extensions 57
APPENDIX A: Terms and Conditions 58
APPENDIX B: Acronyms 59
APPENDIX C: References for Themes, Topics and Questions 92

A. Notice of Funding Opportunity (NOFO) Description

Issued By

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

Catalog of Federal Domestic Assistance (CFDA) Number

97.061

CFDA Title

Centers for Homeland Security

Notice of Funding Opportunity Title

DHS S&T Center of Excellence for Cross-Border Threat Screening and Supply Chain Defense – Center Partner

NOFO Number

DHS-16-ST-061-CBTS-Partner

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. 114-4,
Title IV, Science and Technology, Research, Development, Acquisition and Operations.

Program Type

New

Program Overview, Objectives, and Priorities

I. Program Overview

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Office of University Programs (OUP) is requesting applications from U.S. colleges and universities to serve as a partner institution for the Center for Cross-Border Threat Screening and Supply Chain Defense (CBTS). OUP is also posting a separate NOFO for eligible applicants to submit lead proposals for consideration. Please see NOFO Number DHS-16-ST-061-CBTS-Lead or 97.061 on https://www.grants.gov/ for directions on how to submit Lead

proposal. 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 a U.S. college or university and involves multiple partners for varying lengths of time. COE partners include other academic institutions, 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 governments, non-profits, and first responder organizations. DHS envisions the COEs as long-term trusted academic partners that provide an array of resources to help DHS and its partners achieve their missions, and improve their 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.

Process for Establishing a New COE

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 three separate review panels (see "E. Application **Review Information**," for a full description of how COE applicants are reviewed, rated and selected). Each panel 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.

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. The DHS COEs are university consortia that work closely with each other and with DHS Offices and 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. DHS COEs operate using a unique research management approach where researchers work alongside operational and decision-making personnel to explore opportunities to use science and technology to enhance capabilities in line with DHS' mission. 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. COE teams should include experts in finance, project management, education, training, outreach and marketing, intellectual property management, technology development, and technology transfer. Applicants should also have an understanding of how to translate research to practice including licensing, the ability to work with transition partners, and an understanding of federal acquisition. The COE team must demonstrate their commitment to develop a long-term trust-based partnership between universities and federal agencies; to do that, this wide range of skills is essential.

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 workplan. **The Center will be required to have these elements in place within 6 months following award.**

The DHS COEs are different than 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 to identify the most critical knowledge and technology gaps that a COE can address, on an on-going basis
- Place faculty and students (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 subject matter experts in order to be able to access the best experts for each problem in short order
- Develop plans for replacing researchers whose projects are not progressing as planned, and a process to hold competitions to replace projects that have ended
- Work with DHS and other operational customers to identify projects with a high potential of generating usable knowledge or technologies, and developing a plan to implement operationally
- Develop detailed plans for transitioning research results into end uses, including plans to pursue intellectual property protections and execute those decisions to support the transfer of research to those capable of further developing the technology or service.

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 (for details on the agreement, please refer to **Error! Reference source not found.**, Programmatic Involvement. On a regular basis, 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 homeland security operational agencies.

The COEs are expected to develop relationships and partnerships with DHS Components and the larger first responder community to provide targeted research and education resources. OUP will work with COE management to formulate the 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 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), 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.

Overarching Vision of the Cross Border Threat Screening and Supply Chain Defense Center of Excellence

The Cross Border Threat Screening and Supply Chain Defense Center of Excellence will research and develop solutions, protocols, and capabilities to enhance the ability of DHS and its partners to detect, assess, and respond to known and unknown biological threats and hazards that could adversely impact the Nation's people, agriculture, and economy. There are numerous organizations across the public and private sector that have a role in detecting threats and mitigating consequences. This Center will support DHS improve its operational capabilities that contribute the Nation's layered defense.

New biological threats and hazards have the potential tosignificantly affect the health and well-being of DHS personnel. These threats may also spread to people, animals, plants, and negatively affect the Nation's economy and critical infrastructure. Persistent and emerging threats exist such as invasive species, novel biological agents and materials, infectious human and zoonotic diseases, and counterfeit goods that could cause significant harm to health and economic stability. Biological and chemical threats can affect our infrastructures directly; halt their productivity, or utilize those systems to promulgate across nodes within supply chains.

Capabilities in biotechnology will advance, including ready access to component hardware, precursor chemicals and materials; likewise, the knowledge and expertise in creating modified or novel organisms will advance. Traditional and non-traditional actors and adversaries will explore new toxins, live agents, and bioregulators that will in turn require new integrated systematic techniques and technology systems to detect, prevent, and treat these broad threats. Biology and biological processes are becoming programmable and scalable, providing tremendous advances in healthcare, but are also lowering barriers for malicious actors to leverage these technologies for nefarious purposes. The inherently dual-use nature of many biological technologies and infrastructure means that anticipating such threats and hazards and monitoring their emergence on the global scene, especially the potential for their dispersal (intentional or natural) through the other noted trends in globalization, will be increasingly difficult .

The biodefense enterprise must approach the future with flexibility to prevent, detect and respond to biological threats andhazards in order to both avoid surprise by adversaries who would seek to employ biological means against the U.S. and its allies and the inadvertent releaseof biological hazard within the U.S. Current biosecurity and biosafety policies struggle with the pace of advancement and diffusion of technology, and the emergence of new capabilities that result from the convergence of traditional biological disciplines with engineering, bioinformatics, and information technology. Similarly, supply chains are becoming more complex, adaptable, which can support markets but potentially introduce the opportunity for malicious activities or new physical threats that affect health and the economy.

The DHS 2014 Quadrennial Homeland Security Review posits a future environment characterized by several persistent trends related to globalization, including increased trade; accessible and increased world-wide travel to a growing number of the earth's population; and improved accessibility to, and proliferation of, life-sciences knowledge. [1] DHS seeks to understand alternative approaches to reduce risks posed by new biological threats encountered at

[1] "The 2014 Quadrennial Homeland Security Review. The Department of Homeland Security. June 18, 2014. https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf

borders, ports of entry (POEs), and within the global supply chain in which DHS has responsibility. DHS is most concerned with transnational agro- and bio-terrorism, pandemics, transboundary animal diseases, and other unknown biothreats. Faced with ever-increasing volumes of trade and travelers, border security and immigration managers need technological innovations and better management of information.

COEs should describe how technologies and concepts could be integrated into DHS operations to enhance screening and bio-threat identification, assessment, and prevention. Potential approaches include the utilization of innovative technologies (e.g., screening physical cargo and passengers and data analysis to identify potential conditions that warrant greater scrutiny), optimized operational procedures, and a skilled workforce trained in latest methods to identify and respond to biological threats and their corresponding impact on health and the economy.

DHS Operational Environment

Since 2001, the U.S. Government has worked with numerous public and private sector agencies and entities in efforts to enhance resiliency against natural and manmade disasters. In 2002, The Department of Homeland Security (DHS) was established to prevent terrorism and enhance security, secure and manage our borders, enforce and administer immigration laws, safeguard and secure cyberspace, and ensure resiliency to disasters. DHS has a diverse role in supporting federal, state, and local agencies prepare for, protect against, respond to, and recover from catastrophic incidents that may affect our citizens' health and impact the Nation's infrastructures.

DHS has a central role in the Nation's security. Its seven operational Components have a diverse set of missions and operations, all focused on making the U.S. more secure and resilient. The Components are present across the country at ports of entry including land borders, air and sea ports, and international cargo ports. A significant part of the Components' missions are to maintain the continuity of the nation's trade and economic activities.

It is critical for DHS Customs and Border Protection (CBP), Office of Health Affairs (OHA), Federal Emergency Management Agency (FEMA), Transportation Security Agency (TSA) and their partners in United States Department of Agriculture (USDA), Health and Human Services (HHS), and industry to know in advance about emerging and imminent biological threats, have the capability to detect these threats, and to understand how such threats could be introduced and moved throughout our infrastructure and supply chain systems. DHS is not the lead sector specific agency for the Food and Agriculture

Sector or the Public Health Sector, but it has a substantial role in coordinating and sharing information with federal, state, local, tribal, territorial and industry partners.

U.S. Customs and Border Protection (CBP) is the principal agency responsible for securing the borders, enabling safe and secure commerce, and protecting our citizens and economy from foreign-sourced threats. This mission is supported in varying ways by the DHS Office of Health Affairs (OHA), the Transportation Security Agency (TSA), the National Protection and Programs Directorate (NPPD), and the Federal Emergency Management Agency (FEMA). Collectively, the DHS enterprise and its federal partners work to understand how best to support the safety and security of the Nation's citizens, infrastructures, and the economy.

DHS seeks research and development to assist CBP field personnel prepare for and respond to biological threats, or known hazards could impact border security, public health, trade, and travel. Ports of Entry (POEs) are Federal inspection facilities where travelers and goods are processed by immigration and customs officials. POEs also serve as gateways to flows of people and goods throughout the global community. CBP inspection operations involve multilayered screening processes to identify, target, and inspect high-risk entries in cargo, international mail, and passenger pathways.

OHA is DHS's principal authority for all medical and public health issues. OHA's five divisions guide DHS leaders on medical and public health issues related to national security and long-term policies. OHA supports DHS Components and public health communities nationwide to plan for, respond to, and recover from crises. OHA monitors the environment for dangerous biological agents, analyzes data for early signs of chemical and biological threats, and plans responses to pandemics. OHA works closely with DHS professionals on the frontlines, like CBP and TSA officers, to keep them healthy and safe. OHA also helps DHS officials coordinate medical resources and understand health and medical risks during incidents[2].

FEMA's mission is to help citizens and first responders build, sustain and improve the Nation's capability for preventing, mitigating, responding to, and recovering from all domestic disasters, whether natural or man-made, including acts of terror. FEMA's efforts at the national and regional levels are led by individuals with a broad range of hands-on emergency management, fire, rescue, emergency medical services, law enforcement, military and private sector experience. [3] Timely and accurate information on biological and chemical threats is essential to develop an effective FEMA response.

[2] Department of Homeland Security Office of Health Affairs. Accessed on 8/30/2016. https://www.dhs.gov/office-health-affairs

[3] The Federal Emergency Management Agency (FEMA). Accessed on 8/30/2016. www.fema.gov

TSA was established after the events of September 11, 2001, by the Aviation and Transportation Security Act. This act charged TSA with the responsibilities for enforcing security-related regulations and requirements. This includes: identifying and undertaking research and development (R&D) activities necessary to enhance transportation security; inspecting, maintaining, and testing security facilities, equipment, and systems; ensuring the adequacy of security measures for the transportation of cargo; overseeing implementation efforts, and; ensuring the adequacy of security measures at airports and other transportation facilities [4]

The scope of DHS operations necessary to support efficient and secure trade is immense. CBP and TSA are critical agencies within this layered defensive structure. Each year, more than 11 million maritime containers arrive at the Nation's seaports. At land borders, another 11 million arrive by truck and 2.7 million by rail.[5] The CBP antiterrorism mission is not limited to the physical examination of cargo when it arrives in U.S. POEs. CBP uses intelligence from a number of sources to identify high-risk shipments in order to concentrate its inspection resources.

In addition to its own regulations, CBP enforces over 400 laws on behalf of over 40 other U.S. Government agencies.[6] A large number of these import rules were designed to protect American agriculture and citizens from health risks, and dangerous, illegal, or counterfeit goods. CBP has a number of initiatives including use of non-intrusive inspectional technology to examine cargo effectively with little disruption in the flow of trade and inconvenience to travelers. Similarly, TSA works with federal and international partners to secure the global supply chain that drives the Nation's domestic critical infrastructures. TSA is utilizing a multi-layered, risk-based approach to air cargo security focused on emerging and next generation threats. In 2015, TSA screened more than 432 million checked bags, more than 1.6 billion carry-on bags, 708 million passengers, and 12.9 million airport employees.[7] Today, nearly 51,000 officers screen passengers and their belongings to ensure the safety of aviation security and to protect against introduced threats.[8]

[4] "Aviation and Transportation Security Act". Transportation Security Administration (TSA). November 19, 2001. https://www.tsa.gov/sites/default/files/aviation_and_transportation_security_act_atsa_public_law_107_1771.pdf

[5] "Cargo Security and Examinations". United States Customs and Border Protection. https://www.cbp.gov/border-security/ports-entry/cargo-security

[6] "Cargo Examination". United States Customs and Border Protection. https://www.cbp.gov/border-security/ports-entry/cargo-security/examination

[7] "National Press Release: TSA 2015 Statistics". Transportation Security Aviation. January 21, 2016. https://www.tsa.gov/news/releases/2016/01/21/tsa-releases-2015-statistics

[8] United State Department of Homeland Security, Aviation Security. September 23, 2015. Available at: https://www.dhs.gov/aviation-security

The increase number and efficiency of transportation networks and supply chains can increase the chances to introduce new strains of diseases, pathogens, hazardous substances, and invasive species, all of which can adversely impact human and animal health and the economy (Figure 1). According to the United States Department of Agriculture (USDA) Economic Research Service (ERS), the value of U.S. agricultural exports increased from $85 billion in 1995 to over $144 billion in 2013. [9] Agriculture and agriculture-related industries contributed $835 billion to the U.S. gross domestic product (GDP) in 2014. [10] If a disease outbreak were to occur in the U.S., agricultural exports to other countries would be curtailed, with severe impacts to the economy.

Seventy five percent of new diseases affecting humans are zoonotic, while twenty well-known diseases--including tuberculosis (TB), malaria, and cholera--have reemerged or spread geographically since 1973, often in more virulent and drug-resistant forms. At least 30 previously unknown disease agents have been identified since 1973, including HIV, Ebola, hepatitis C, and Nipah virus, for which no cures are available. [11]

The global food supply chain is a network of producers, processors, distributors, consumers, and government/non-governmental regulators. Technological advances enable the food supply chain to increase to meet demand, which increases the likelihood of accidental or deliberate contamination by counterfeit products, chemicals, pests, pathogenic diseases, or invasive species. Globalization of the food supply has led to the rapid and widespread international distribution of foods and anything those foods may be contaminated with.

[9] United States Department of Agriculture Economic Research Service. "The Evolution of U.S. Agriculture Exports". https://www.ers.usda.gov/topics/international-markets-trade/us-agricultural-trade/

[10] United States Department of Agriculture Economic Research Service. "Ag and Food Sectors and the Economy". https://www.ers.usda.gov/data-products/ag-and-food-statistics-charting-the-essentials/ag-and-food-sectors-and- the-economy.aspx

[11] World Health Organization. "Veterinary Public Health". http://www.who.int/zoonoses/vph/en/



Figure 1

Strategic Guidance and Legal Authorities Relevant to this COE

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

CBP's mission is to prevent terrorists and weapons of terrorism from entering the United States by eliminating potential threats before they arrive at our borders and ports. The United States Coast Guard and Customs and Border protection secure the waterways and land borders. Homeland Security Presidential Directive thirteen (HSPD-13) underscores the importance of securing the Maritime Domain, defined as *"All areas and things of, on ,under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities ,infrastructure, people, cargo, and vessels and other conveyance."* [12]

Agriculture, food, and people are all susceptible to exposure to biological threats and hazards. In 2004, HSPD-9 *Defense of United States Agriculture and Food* established a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.[13] The U.S. food supply system is comprised of thousands of potential targets for terrorist attacks or naturally occurring diseases, pests, or toxins.

[12] "National Plan to Achieve Maritime Domain Awareness". The Department of Homeland Security Digital Library. October 20005. https://www.dhs.gov/sites/default/files/publications/HSPD_MDAPlan_0.pdf

[13] "Homeland Security Presidential Directive 13: Maritime Security Policy". Department of Homeland Security. 2005. https://www.hsdl.org/?abstract&did=451035

HSPD-10 *Biodefense for the 21st Century* was enacted four months after HSPD-9. This directive states that "the United States will use all means necessary to prevent, protect against, and mitigate biological weapons attacks perpetrated against our homeland and our global interests."[14] HSPD-10 also sets forth four pillars of U.S. biodefense: threat awareness; prevention and protection; surveillance and detection; and, response and recovery. The HSPD-10 requires collaboration and synergistic efforts among various federal agencies (i.e. DHS, DoD, HHS, and USDA).

The Security and Accountability For Every Port Act of 2006 (SAFE Port Act) requires the Secretary of Homeland Security to develop and implement a strategic plan to enhance the security of the international supply chain, in consultation with appropriate Federal, State, local and tribal government agencies, the private sector, and the international community.[15]

To strengthen global supply chains and encourage actions to increase resilience, the U.S. created the *National Strategy for Global Supply Chain Security* in 2012[16]. A key attribute of our public health and economic stability is the ability to identify and mitigate threats to our supply chains. The global supply chain that serves the U.S. can be targeted by malicious actors, or disrupted by infectious diseases, natural disasters, or other catastrophes.

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.

[14] "Biodefense for the 21st Century". The White House, Office of the Press Secretary. April 28, 2004. https://www.hsdl.org/?view&did=784400

[15] "Security Safe Port Act". Congress. October, 13, 2006. https://www.congress.gov/109/plaws/publ347/PLAW-109publ347.pdf

[16] "National Strategy for Global Supply Chain Security". The White House, Office of the Press Secretary. January 25, 2012. https://obamawhitehouse.archives.gov/the-press-office/2012/01/25/fact-sheet-national-strategy-global-supply-chain-security

DHS's Approach to COEs

Establishing a COE is a major and expensive effort that involves a lot of actors on both the federal and university sides. There are important elements of standing up and operating a COE that every applicant should understand prior to applying:

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. CBTS's research will be based on the HSE needs expressed by HSE practitioners in this NOFO. Research outcomes will include analytical tools, 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 envisions that multi-disciplinary research teams working closely with DHS and other subject matter experts will develop successful innovations to confront future homeland security challenges. The teams will need various combinations of academic disciplines, including operations research, social sciences, engineering, biological and physical sciences, and mathematics. This COE will focus on major and cross-cutting DHS mission areas in ways that previous COEs have not addressed. For more information about DHS S&T and its organizational structure, visit http://www.dhs.gov/st-organization. For more information about the COEs, visit: http://www.hsuniversityprograms.org.

This COE will support a portfolio of projects that range in technical maturity, potential impact, and that address different elements of the complex challenges associated with integrating information relevant to protecting the Nation against next generation biological threats. Centers are required to develop and adhere to a systematic framework that guides project teams through appropriate developmental steps, addresses critical regulatory, market, and other business factors that will impact the likelihood that the outcome will be used by customers.

CBTS researchers, faculty and students must work closely with DHS Components and other federal, state local, territorial, and tribal law enforcement and emergency management partners to develop and deploy tools and methods to support homeland security decision makers.

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.

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.[17] 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 2 below is a depiction of a generic form of the stage-gate process.

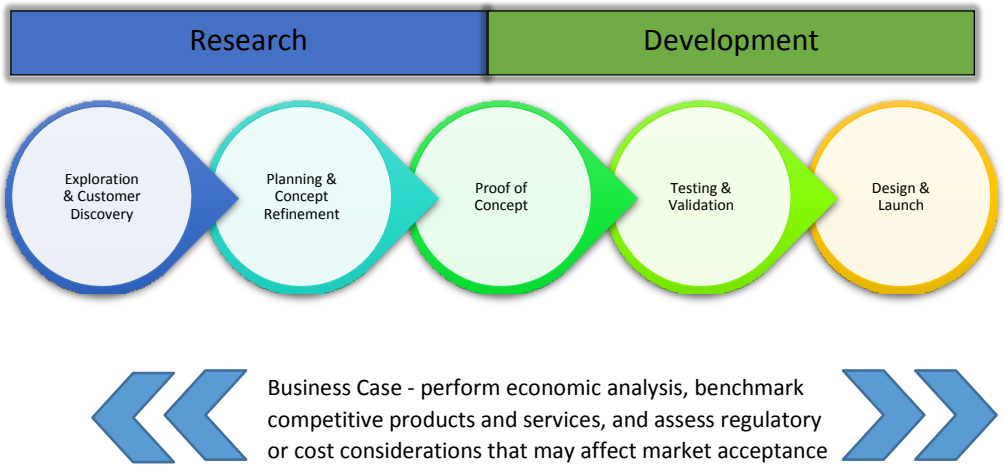


Figure 2

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 2, 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

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

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 subject matter experts. **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 Other Submission Requirements in Appendix A.

II. 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 VIII "Research Theme Areas". 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 CBTS workforce and professional development program should include innovative initiatives to educate or train 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. Applicants should describe how their Center would provide and enhance technical education and training programs for HSE and DHS professionals, for example, at the Federal Law Enforcement Training Center, the Emergency Management Institute or other federal training centers.

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

- Build universities' capacity in 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 and technologies

- 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.

Prescribed education program activities include:

- Developing undergraduate, graduate or professional career enhancing programs that support the COE's research program
- Offering continuing education opportunities for first responders and homeland security professionals
- Offering student internship, scholarship, or fellowship programs that provide homeland security research experience
- 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
- Developing community college partnership programs to attract a diverse population of students and teachers into homeland security
- Offering homeland security related research opportunities to students
- Embedding students and faculty in research projects at DHS or other operational agencies within the homeland security enterprise.

Applicants must include the following elements for each project:

- 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 "Transition" p 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)

III. Research and Workforce and Professional Development Themes, Topics, and Questions

The CBTS Center shall work with DHS S&T, CBP, OHA, FEMA, TSA and their partners in USDA, HHS, and industry to understand how to detect next generation biological threats and how such threats could move throughout our infrastructure systems. There are numerous efforts underway to develop sensors, technologies, and techniques for biological detection, data integration, and analytics. DHS is interested in analyzing, integrating, and testing broad spectrum technical approaches and procedures that could be used to establish next generation multiplexed screening capabilities in the field. CBTS shall aim to inculcate analytic rigor throughout the Department to support decision-making (see Figure 2 Prevent Terrorism and Enhance Security and Secure and Manage our Borders).

The Homeland Security vision is a homeland that is safe, secure, and resilient against terrorism and other hazards. The DHS has a **five-mission** structure:

- Prevent Terrorism and Enhance Security
- Secure and Manage our Borders
- Enforce and Administer Our Immigration Laws
- Safeguard and Secure Cyberspace
- Strengthen National Preparedness and Resilience

Accomplishing these missions requires unity of effort across every area of DHS activity and among the numerous homeland security partners and stakeholders.

The Department will accomplish unity of effort not by centralizing the decision making authority…but rather by transparently incorporating DHS Components into unified decision making processes and the analytic efforts that inform decision making.

-Homeland Security FY2014-2018 Strategic Plan, p.6

Figure 2

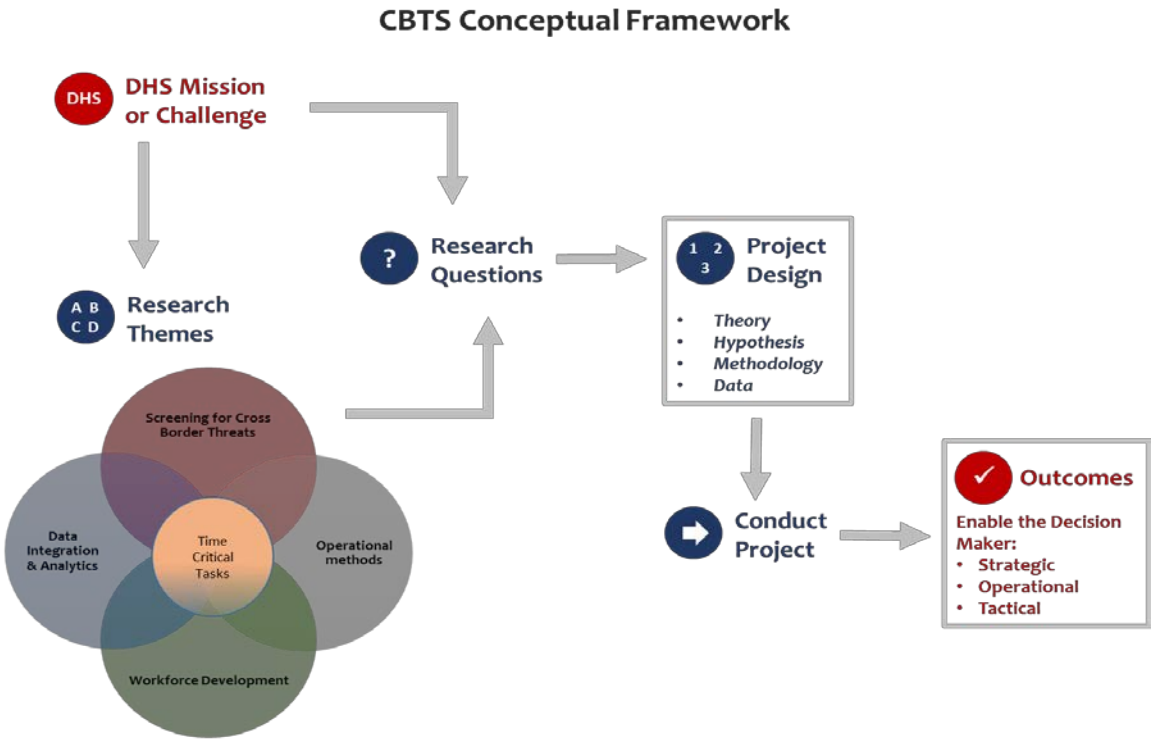


Figure 3

After the Applicant 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 CBTS themes in a Venn diagram, to illustrate DHS's recognition of overlap among the themes and topics). Applicants 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 ended to allow the Center to move on to another area of investigation.

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 II 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, selection of software tools, IT platforms, or other commercial products to be used in the course of the project.

Research Topics

Topic Area One: Detecting Threats and Disruptions to People and Global Supply Chains:

DHS maintains core capabilities at ports of entry, preclearance stations situated abroad, and other transportation nodes where CBP and TSA officials screen people and goods before entering the US. Timely and accurate detection of biological threats, malicious activities, invasive species, and other hazardous materials at inspection points and prior to inspection points is critical to securing the legitimate flow of goods and people. To promote the efficient and secure movement of goods and people, DHS must work with partners to reduce illegal commerce and interdict those that look to exploit the supply chain for nefarious purposes.

Detecting threats early in the process will strengthen the security and resilience of the global supply chain system. Numerous research teams across the academic and commercial sector are working to develop biological sensors and laboratory approaches, but these efforts can be too narrow to support field operations. DHS needs simplified, cost effective, interoperable, and broad spectrum approaches to screen for biological threats. Next generation capabilities will be able to analyze samples against a multitude of known and unknown pathogens simultaneously, will not require cold chain, provide useful feedback to the customer, and be deployed with limited technical skills. In addition, DHS seeks to better understand how to use data to inform operational based processes and procedures, provide timely decision making, promote safe trade and travel, and protect the health of its workforce.

Representative research questions of interest to DHS (not listed in priority order):

- ☐ How can biological screening and data fusion capabilities work across domains (human, animal, food, supply chain, and environmental) to quickly and accurately triage:
  - Imminent biothreats and pathways of entry into the US; and,
  - High-risk trade entities and people hidden behind legitimate trade and travel
  - Data needs to provide scientifically defensible, actionable information
- ☐ What techniques exist to accurately discriminate legitimate from fraudulent, or deceptive entries in cargo and traveler ports of entry environments?
- ☐ What capabilities exist to rapidly determine if the biothreat landscape is changing? What are the current limitations and what leap ahead opportunities exist to identify changes across domains?
- ☐ What detection technologies offer open architecture approaches that allow the diverse institutions and organizations that are part of the homeland security enterprise to contribute data and analytics to support bio-threat identification?
- ☐ How do different supply chains work and where are the critical nodes within a supply chain where opportunities exist for mitigating risk posed by hazardous threats? Are there alternative supplies, suppliers, or supply chains that are likely to emerge or enter the market during disasters? What stresses will be on these supply chains and how can DHS identify conditions that would warrant rapid inspection?
- ☐ How can new advances in molecular, cellular, and imaging technologies be used to support existing DHS screening approaches for known and emerging, high consequence diseases and pathogens? How can technology support the identification and origin of agricultural and biological imports accurately and quickly at Ports of Entry?
- ☐ What is the state of the art in cost-effective and sustainable fixed-laboratory and field-portable instruments and assays that detect biological materials and hazardous substances? What are the cost benefit characteristics of these technologies?
- ☐ How can public and private enterprises establish effective detection-based deployment schemas that balance cost, capability, and flexibility?
- ☐ How can scientific developments in synthetic biology provide definitive awareness of biothreat releases?
- ☐ What material and non-material approaches can improve the speed and accuracy of identification and characterization of a potential biothreat, including whether an agent has been genetically modified? How can synthetic biology improve diagnostic capabilities for detecting biothreat agents in complex matrices, such as food, water, cargo, and other materials?

- ☐ Are there legal implications of identifying high consequence diseases and pathogens (natural and intentionally designed) in people and cargo? What are appropriate legal and technology-based methods to protect individual privacy while still providing data to those institutions that need to take action to prevent the spread or misuse of those biological threats?
- ☐ Historically, commercial entities and government researchers have looked to the Federal government as the primary market for funding the development and procurement of detection tools for high consequence, low probability pathogens and diseases - human, animal, and zoonotic. The way the Federal, state, and local agencies are organized and receive appropriations/funds creates real challenges in determining and encouraging the development of a market: who pays for sustainability for these detection tools, what is the market for these tools, and what incentives, policies, and laws would support the adoption of methods and technologies to reduce the impact of biological incidents?
- ☐ How can DHS better leverage international partnerships to coordinate resources and enhance its ability to detect and interdict biological threats and hazards prior to entering the United States?

Topic Area Two: Data Integration and Analytics

The rapid proliferation of technologies and knowledge provide tremendous opportunities for growth but also introduces new vulnerabilities that could be exploited for nefarious purposes. As the capabilities diffuse to those that intend to do harm, DHS and its partners must prepare for the corresponding increasing risk to our Nation. Many public and private sector organizations will be involved in the mitigation of threats. The tools and communications between those entities must be secure and structured to protect the interests of the response and recovery efforts. Information sharing must bring value to those providing the data. To effectively assess situations and make sense of data, DHS must provide value back to data owners. This can be legally and technically challenging.

DHS CBP, OHA, FEMA, TSA, and Intelligence and Analysis (I&A) serve as critical partners within the supply chain, providing screening, interdiction, and protection of goods and people. In this context, understanding how data can be combined, how analysts can make sense of the information, and how the information can impact operations is a key step in the early identification of a hazardous incident. Much of the data that will be used by analysts may belong to the private sector or may belong to public institutions that follow different authorities. This creates uncertainty on how data will be used, how liability will be addressed, and what value is created by participating in data sharing partnerships. DHS in interested in exploring how to encourage data sharing in this environment.

Accurate and timely information is essential to being able to mitigate, predict, prepare, and respond to biological threats and or hazards. The ability to extract, analyze, and visualize data on the most essential information sources is key. DHS seeks to improve decision analysis in the field by developing innovative tools, methodologies and processes to support DHS and its partners. Interoperable field deployable software tools that integrate data from multiple data sources such as sensors, health records, import/exports, supply chains, private industry, and government partners may support the decision making.

Representative research questions of interest to DHS (not listed in priority order):

- ☐ How can the value of supply chain, environmental, health, social media, financial, and intelligence data sets be assessed quantitatively for inclusion in tools focused on providing insights into the health status of our Nation? How effective are current predictive analytics in identifying potential incidents or conditions that warrant further investigation?
- ☐ How can the homeland security enterprise use data to discern relationships, detect anomalies, and display trends that might mitigate terrorist actions, threats public safety, pandemics, and potential natural or manmade disasters?
- ☐ How can DHS integrate existing surveillance data streams for animal (wild, domestic, and companion), plant and human health to develop a more holistic view of situations? What legal or information policies would encourage data owners to share data, at what level of granularity, and under what legal protection?
- ☐ How do organizations best handle fatigue generated from responding to multiple requests for data pertaining to public, environmental, and animal health?
- ☐ What are possible methods to establish data linkages across the multiple systems utilized at various ports of entry environments (e.g., cargo, passenger, express consignments, and international mail)?
- How can analytical capabilities in epidemiology be included into existing event-based biosurveillance systems capable of providing spatiotemporal patterns of spread of infectious biological agents across hosts and environmental conditions? Can these analytics accept data feeds on agriculture, wildlife trade, and international travel from CBP's data warehouses to establish footprint and origin, and provide probabilistic spatiotemporal movement of the biothreat across the globe and into the US? What legal agreements would be necessary to share this data in real time?
- Data science offers tremendous potential in the fields of biomedical research, bioinformatics, and computational biology. How can advances in these fields be applied to adaptable detection platforms capable of supporting DHS's evolving needs to identify and detect new and emerging high consequence diseases, pathogens, and synthetic bio materials?
- ☐ What is the state of the art in predicting geospatial, temporal, and directional movement of biological agents, persistent and emerging pests, and pathogenic

high consequence diseases of animals, humans, and plants, through trade, travel, and/or natural atmospheric circulation pattern?

- ☐ How can specific information pertaining to location, classification of material, certification documentation, and threat assessment be easily referenced during the non-intrusive inspection process of goods?
- ☐ How can documentation on products that are seized, re-exported, or destroyed be improved? How can the aggregation of this data then be used in training or trend analysis?
- ☐ What emerging high consequence diseases pose national and health security threats based on the migration of people and animals due to climate change?
- ☐ How can decision makers be informed of the impact of different policies that optimize trade and/or economic benefits?
- ☐ What are some appropriate methods to analyze unintended side effects of innovative policies pertaining to preparing for, responding to, and recovering from biological attacks?
- ☐ What is the state of the art in alerting capabilities for predictors/indicators of future biological risks? What are the limitations of these approaches?
- ☐ What is the best way to display data and information to the various organizations that are part of the supply chain for biological products, food and agriculture products, or that regulate or inspect those products? How should confidentiality concerns be addressed to encourage data sharing and partnership?
- ☐ Evidence of tampering with microorganisms may provide insight into perpetrators of biocrime. How can techniques to discover and understand intentional genetic manipulation be used to attribute a biological attack to a specific person, location, or laboratory?
- ☐ What applications of synthetic biology could enable scientists to distinguish efforts that represent dual use research of concern?

Topic Area Three: Novel Operational Methods to Use Emerging Tools to Reduce Risk

The homeland security enterprise is composed of a complex collection of federal, state, local, tribal and territorial (FSLTT) government and private resources, programs and initiatives designed for a variety of purposes and dedicated to mitigating risks. These groups operate in shared spaces, operate in unique operational environments, and have different authorities, missions, and capabilities. However, these groups must be able to work together to provide the risk-based, layered approach necessary to protect the Nation.

Respective research questions of interest to DHS (not listed in priority order):

- ☐ What biological screening approached will support the identification of counterfeit goods, are contaminated with biological threats, are not declared, are prohibited or could be otherwise compromised while in transit through the global supply chain?
- ☐ How effective are current incentive-based programs in protecting cargo from biological threats? How would program effectiveness be measured?
- Are industry's current risk management principles sufficient in restoring the movement of food and animal products following catastrophic disruptions?
- ☐ How can DHS assist in providing critical information to support the coordinated restoration of a supply chain following a biological attack or catastrophic disruption? What policies are needed and what data and information is needed to expedite this restoration?
- ☐ As diseases emerge globally and with increasing frequency, new quantitative techniques to digitally detect outbreaks of new, unknown, and emerging diseases are required. How can DHS implement new quantitative techniques such as use of Electronic Health Records to develop long term capabilities to better detect unusual disease outbreaks?
- ☐ How can screening processes for people and cargo be optimized to balance cost, performance, and sustainability?
- ☐ How can CBP officers and DHS analysts detect relevant patterns in biological and supply chain data? Are there existing computational techniques or big data algorithms that can visualize hidden illegitimate relationships from legitimate entries?
- ☐ How can the government and commercial sector work together to integrate security and processes into supply chain operations to support the identification of threats as early as possible, while protecting confidential business information?
- ☐ How can applications of perceived R&D technologies (e.g., computational techniques, modeling and predictive analysis etc.) be operationalized at the field level?
- DHS must protect the Department's workforce from accidental, deliberate, or naturally occurring biological threats and/or hazards. Are current PPE used by the CBP, TSA, and other DHS Components adequate to ensure their safety on the job? How can these wearable PPE technologies be used to protect field officers from biological threats while not raising panic to the public?
- ☐ What are the performance characteristics of existing portable field biosensors to priority biological agents and toxins? What advantages and disadvantages exist in these systems when deployed in operational settings such as POEs or in other operational environments including sea ship inspections?
- ☐ What are the most promising incentives to encourage private and public entities to share data that is critical to making risk informed decisions necessary to prepare for, respond to, and recover from an intentional biological attack?
- ☐ How can this data be securely accessed or shared to support actionable decision making that will affect DHS operations?

- ☐ CBP maintains information on trade and travel entries, legitimate or otherwise; including disposition of those entries under regulatory domains of other Federal agencies. Yet, this information has not been fully utilized by current risk assessments. This information, combined with event biosurveillance data available in open source or curated by international and/or concerned organizations, can provide insights that support the prediction of imminent threats. What legal mechanisms would assist DHS in partnering with other FSLTT and private sector partners in identifying data to share? What concerns must be addressed in order to facilitate discussions with data owners?
- ☐ What are the most effective ways for businesses and public sector organizations to determine when conditions warrant increased screening of people and cargo for bio-threats or other hazardous conditions?
- ☐ How might synthetic biology be used to render dangerous biothreat agents harmless in an effective and timely way?
- ☐ How might synthetic biology be used to detect and remove environmental contaminates?
- ☐ How might existing regulatory frameworks be adapted, or what new frameworks might be created, to reduce the combination of biosafety and biosecurity concerns raised through the application of synthetic biology techniques, without adversely impairing scientific progress?
- ☐ What are the limitations of current biological agent dispersion models? How can this be improved? Could these models be incorporated into simulation training for DHS operational components?

Topic Area Four: Workforce Development

Ensuring the DHS workforce is adequately trained and educated to perform the required operations is essential. DHS's workforce needs to be prepared for current and emerging threats to health and the economy. DHS encourages educational institutions to utilize internships, co-operative initiatives, and other programs to provide opportunities for students to develop cross-functional skills necessary to thrive in the technology, operator, and business environments. These educational programs must be formal and flexible to provide all levels of operators the guidance necessary to understand evolving global threats.

Representative research questions of interest to DHS (not listed in priority order):

- ☐ What partnership opportunities exist to link students with commercial entities that develop products and offer services in the fields of data science, supply chains, biology, synthetic biology, diagnostics, materials sciences, engineering, risk assessments, legal, operations research, and business?

- ☐ What are the core competencies needed by DHS and supporting agencies to address next generation biothreats? What are the core competencies needed by industry to manage their products and services in this environment?
- ☐ Should employees be cross trained using professional scientific core competency standards or should DHS utilize anti-bioterrorism work?
- ☐ What procedures can best protect field agents from threats while inspecting good and people? What ongoing education is needed to protect DHS personnel from future biological threats?
- ☐ How effective are current training programs for inspectors or agents that address procedures for responding to biological incidents?
- ☐ Which academic programs provide the skills needed by next generation biological and other threat detection technology developers?
- ☐ What mechanisms can DHS provide to allow internship or apprenticeship, on temporary duty of assignment at component agencies, for potential employment?
- ☐ DHS and other agency employees deal with uncertainty daily, often putting themselves in danger. What methods are most effective in addressing scientific uncertainty in the field?
- ☐ How can current and future interdiction training incorporate new information and tools to facilitate and secure legitimate international trade and travel while simultaneously protecting U.S. borders?
- ☐ How should risk communication and current public guidance on biothreats be structured to ensure transparency?
- ☐ How can the homeland security enterprise (HSE) build partnerships with industry and the one health community to execute sustainable workforce development programs that set and maintain core competencies required to combat future biothreats?
- ☐ What training programs will improve the operational performance of CBP agricultural specialists and TSA officers in responding to biological threats (disinfecting/safeguarding/remedial actions)? How effective are these new training approaches in achieving operational improvements? Are there better ways to reference USDA quarantine recommendations?

Topic Area Five: Time Critical Response Support

DHS must be able to respond or support efforts to mitigate rapidly developing incidents. Under this COE, applicants may be asked to support time critical tasks – efforts that require scientific support to address rapidly emerging challenges that exist in the homeland security enterprise. University researchers can be a source of scientific expertise during incidents of concern. These efforts may include enhanced protocols, knowledge products, technical requirements/ specifications, proofs of concepts, or pilots that assist in the response to evolving, high consequence threats (usually 1-12 months).

DHS recognizes the need for university expertise and rapid response solutions to critical incidents.

Example areas may include: (not listed in priority order):

- ☐ How can research enhance operational protocols to address increased risks posed by high consequence biological, chemical, and other hazardous threats?
- ☐ What existing commercial off the shelf (COTS) technology exists that can help to address time critical tasks?
- ☐ What is the state of the art in the emergence of new technologies, what are the characteristics of, and links in the supply chains for these new technologies?, What are the risks and uncertainties of new and emerging biological and other hazardous threats?
- ☐ What information can be integrated into decision support tools that will quickly instruct a non-technical individual to determine how to identify and respond to a high consequence biothreat?
- ☐ Access to specialized facilities currently **approved** to perform, and are capable of performing, the following work may be part of this COE. DHS may need access to facilities capable of:
  - Pathogen genomics and characterization, with the capabilities to provide subject matter expert advice on current organisms and viruses and future developments
  - Preparation and validation of molecular detection and characterization assays for select agent organisms
  - Pathogen genomics sequencing in with BSL-3 capability for sequencing and performing rapid bioinformatics analysis on new pathogens and viruses; quickly and economically
  - Repository management and archival holdings of select agents, both current and emerging strains gathered internationally, characterized by above facilities and staff

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, 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): 03/31/2018

Projected Period of Performance End Date(s): 03/30/2020

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 research and development activities. See APPENDIX A: Terms and Conditions for additional details of substantial programmatic involvement.

Available Funding

Center for Cross-Border Threat Screening and Supply Chain Defense (CBTS) award: (1) one for Center Lead (DHS-16-ST-061-CBTS-Lead) and (2) one for Center Partner (DHS-16-ST-061-CBTS-Partner). Subject to availability of funds, DHS estimates that a ***total*** of up to $3.5 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 may allocate up to $250,000 of the $3.5 million per year to each selected Partner applicant, subject to availability of funds.

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 $3.5 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 Partner 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."

Proposals must be submitted by an accredited U.S. institution of higher education 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 partner applicants are strongly encouraged to partner with 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 or private 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 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 two year 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: 03/16/2017

Application Submission Deadline: 08/04/2017 at 11:59:59 PM EDT

Anticipated Funding Selection Date: 03/01/2018

Anticipated Award Date: 03/31/2018

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.

Event	Suggested Deadline For Completion
Informational Webinar	03/29/2017 (3:00PM EST) See details below
Obtaining DUNS Number	Four weeks before actual submission deadline 07/07/2017
Obtaining a valid EIN	Four weeks before actual submission deadline 07/07/2017
Updating SAM registration	Four weeks before actual submission deadline 07/07/2017

Starting application in Grants.gov	One week before actual submission deadline 07/28/2017

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:
melanie.bales@hq.dhs.gov

Applications will be processed through the Grants.gov portal

Informational Webinar

DHS will conduct an informational webinar for interested applicants on March 29, 2017 at 3:00pm [EST]. 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: 800-369-3109, Passcode: 2157929) and computer (https://go.hsuniversityprograms.org/?GOKNrT3d). The webinar will be recorded and posted on www.grants.gov for future reference.

Content and Form of Application Submission

A. SF424 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.

- **a.** Block 1, Type of Submission – please check "Application"
- **b.** Block 8, Type of Application – please check "New"
- **c.** Block 12, Proposed Project – please provide the start and end dates for your project

d. 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.
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://opgs.dc.gov/service/state-single-point-contact-spoc

e. 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

f. 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

B. **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.***

C. 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.

D. 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.

E. 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 font, Times New Roman, 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 A. II. 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)) as well as if you need another place to electronically attach portions of your application

Optional Forms

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

Other Submission Requirements

A. 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 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.

DUNS number. Instructions for obtaining a DUNS number can be found at the following website: http://www.grants.gov//web/grants/applicants/organization-registration/step-1-obtain-duns-number.html. The DUNS number must be included in the data entry field labeled "Organizational DUNS" on the Standard Forms (SF)-424 forms submitted as part of this application.

System for Award Management. In addition to having a DUNS number, applicants applying electronically through Grants.gov must register with SAM. Step-by-step instructions for registering with SAM can be found here: http://www.grants.gov/web/grants/applicants/organization-registration/step-2-register-with-sam.html. Failure to register with SAM will result in your application being rejected by Grants.gov during the submissions process.

Authorized Organizational Representative. The next step in the registration process is creating a username and password with Grants.gov to become an AOR. AORs will need to know the DUNS number of the organization for which they will be submitting applications to complete this process. Applicants must register the individual who is able to make legally binding commitments for the applicant organization as the AOR; this step is often missed and it is crucial for valid submissions. To read more detailed instructions for creating a profile on Grants.gov visit: http://www.grants.gov/web/grants/applicants/organization-registration/step-3-username-password.html.

AOR Authorization. After creating a profile on Grants.gov, the E-Biz Point of Contact (POC), who is a representative from your organization listed as the contact for SAM, will receive an email to grant the AOR permission to submit applications on behalf of their organization. The E-Biz POC will then log in to Grants.gov and approve an individual as the AOR, thereby giving him or her permission to submit applications. After you have been approved as an AOR you will be able to submit your application online. To learn more about AOR Authorization, visit: http://www.grants.gov/web/grants/applicants/organization-registration/step-4-aor-authorization.html. To track AOR status, visit: http://www.grants.gov/web/grants/applicants/organization-registration/step-5-track-aor-status.html.

Electronic Signature. Applications submitted through Grants.gov constitute a submission as electronically signed applications. When you submit the application through Grants.gov, the name of your AOR on file will be inserted into the signature line of the application.

If you experience difficulties accessing information or have any questions please call the grants.gov customer support hotline at (800) 518-4726 or email grants.gov at support@grants.gov.

The Federal awarding agency may not make a Federal award to an applicant until the applicant has complied with all applicable DUNS and SAM requirements and, if an applicant has not fully complied with the requirements by the time the Federal awarding agency is ready to make a Federal award, the Federal awarding agency may determine that the applicant is not qualified to receive a Federal award and use that determination as a basis for making a Federal award to another applicant.

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 review process with two distinct phases to select the partner institution(s) for a Center of Excellence (COE). The phases are: (1) an external scientific quality review by a panel of peers external to DHS, and (2) an internal relevancy review by a panel of DHS SMEs. Only the highest scoring proposals will be referred from the external to the internal review. Each review phase has separate ratings based on different criteria (e.g., scientific quality, relevance to DHS). A detailed description of the selection process follows.

Proposals will be reviewed and evaluated in accordance with the evaluation criteria identified in the Application Evaluation Criteria section below. Each proposal will be evaluated on its own merit and the relevance of the specific proposal as it relates to the DHS COE Program and the DHS mission. Only applications that achieve a rating of 3.0 or higher will be considered for funding. DHS reserves the right to not fund any partner proposals regardless of its rating.

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)

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 biology, chemistry, medical intelligence, supply chains, law, physical security, policy, computer science, organizational design, change management, education and training, diagnostics, epidemiology, public health, viral and bacterial pathogenesis, select agents, bio containment, sampling surveillance, infectious diseases, emergency response and field work. This includes public health, and data science sub-disciplines.

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, qualifications of personnel and suitability of facilities, as well as the appropriateness of research costs. Due to the anticipated number of proposals submitted in response to this NOFO, DHS will execute the External Review for Partner Proposals virtually using a secure portal.

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.

Additionally, prior to making a Federal award with a total amount of Federal share greater than the simplified acquisition threshold ($150,000), 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).

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.

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 CFR §200.205 Federal awarding agency review of risk posed by applicants.

II. DHS Relevancy Review (Internal DHS SMEs)

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. Under no circumstances will an application be considered if both the mean and the median overall ratings are below 3.0.

Application Evaluation Criteria

Prior to making a Federal award, the Federal awarding agency is required by 31 U.S.C. 3321 and 41 U.S.C. 2313 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, and (5) ability to effectively implement statutory, regulatory, or other requirements.

I. 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 each 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.

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%	1.80
Project Goals, Approaches, and Methodologies	5	30%	1.50
Qualifications of Personnel and Suitability of Facilities	5	15%	0.75
Costs	4	10%	0.40
External Review Rating			**4.45**

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):

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

Evaluation Criteria	Reviewer Score	Weight (%)	Weighted Score
Mission Relevance	5	75%	3.75
Transition Strategy	2	25%	.50
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.

Research Project Evaluation Criteria:

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 Program Originality (45%)

- Does the proposed effort shift current research or paradigms by utilizing novel theoretical concepts, approaches or methodologies? Or, is the proposal a refinement, improvement, or existing concepts, approaches, or methodologies proposed?
- Does the proposal outline appropriate stages and gates to evaluate project progress and technical maturity?
- 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, Approaches, 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?

- Does the proposal demonstrate that the researchers' possess a sufficient amount of knowledge of range of biological threats that exist in the operational environment at POEs?
- 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 costs appropriate and reasonable?

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% total)

- 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 research and development programs, information systems, and databases in relevant areas? Does the proposal describe an understanding of DHS protocols pertaining to screening passengers, goods, and cargo, and efforts to protect the DHS workforce?
- Does the proposed program address a knowledge gap not addressed by research and development programs sponsored by DHS or others?
-
- Has the applicant demonstrated an understanding of DHS's existing research and development programs, information systems, and databases in relevant areas? Does the proposal describe an understanding of DHS protocols pertaining to screening passengers, goods, and cargo, and efforts to protect the DHS workforce?
- Does the proposed program address a knowledge gap not addressed by research and development programs sponsored by DHS or others?

B. Transition Strategy (25%)

- Does the applicant describe the intellectual property protection efforts necessary to protect the work? Do the project proposals include efforts to assess the market and evaluate various transition pathways for the technologies being developed?
- Is there a schedule describing 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 effective are the proposed approaches to address sustainability and access concerns?
- Does the transition plan describe viable transition pathways for technologies, tools, and knowledge products to customers in the HSE to include: analyses of the competitive landscape, customer price expectations, delivery mechanisms, transition risk, and intellectual property ownership and protection?
- Does the transition plan propose a process to identify and engage customers throughout the entire duration of the project?
- 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?
- Does the application describe metrics to illustrate the ability to file patents, copyrights, and trademarks relevant to the scientific domains described in the NOFO?
- Does the application outline a comprehensive intellectual property management plan to support the timely decision making necessary to coordinate across partner institutions?
- 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?

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. 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?
- Is the proposed training or educate novel or does it exist elsewhere?
- 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?

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. Research Program Mission Relevance (100%):

- Does the applicant discuss where, in what circumstances, and by whom would research results be used? Are these relevant to DHS' mission?
- Has the applicant demonstrated an understanding of DHS's existing research and development programs, information systems, and databases in relevant areas? Does the proposal describe an understanding of DHS protocols pertaining to screening passengers, goods, and cargo, and efforts to protect the DHS workforce?
- Does the proposed program address a knowledge gap not addressed by research and development programs sponsored by DHS or others?

F. Federal Award Administration Information

Notice of Award

Customarily, applicants are notified about evaluation decisions within one year 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.

I. Work Plan Development Workshop

After award and subject to agreement from the DHS Program Manager, the selected Center Lead and Center Partners will hold a work plan development workshop with 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:

http://www.dhs.gov/publication/fy15-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) (See 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: http://www.whitehouse.gov/sites/default/files/omb/grants/approved_forms/SF-425.pdf, SF-425 *OMB #00348-0061*

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 has to be reported using the Real Property Status Report (Standard Form SF 429) available at *http://www.whitehouse.gov/sites/default/files/omb/grants/approved_forms/sf-429.pdf*.

After these reports have been reviewed and approved by DHS S&T OUP, a close-out 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 de-obligated, 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.

G. DHS Awarding Agency Contact Information

Contact and Resource Information

A. 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: Melanie Bales
Email: melanie.bales@hq.dhs.gov

B. 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: Matthew Coats
Email: matthew.coats@hq.dhs.gov

C. 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.

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

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, 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 management efforts;
      iii. Detailed descriptions on each Center project (including sub-recipient projects) to include:
         - Methodology
         - Project milestones
         - Performance metrics used to evaluate progress,
         - Transition plans
         - 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.
      iv. Budget information categorized by both object class and project, including budget justification

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 subject matter experts 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 one electronic copy (PDF) of all publications generated under this Award to the Program Officer at the time of publication, and shall send a near-final pre-publication draft to the DHS Program Officer. 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. Prior to initiating work on any research project that requires access to third party data, including data provided by DHS Component agencies, the Recipient must provide a plan for acquiring data as described in (b) below. The Recipient shall coordinate review of the plan with the University Privacy Officer prior to submission to DHS. The Recipient shall submit its plan to the DHS Program Officer for review and comment prior to initiating research. DHS will review the plan and notify the Recipient of any concerns that may be identified. The Recipient shall review the Data Acquisition and Management Plans at least annually and identify or update, as necessary, any new areas of research that require access to third party data.
    b. The plan must include the following information for each project:
        i. The purpose for collecting the data and characteristics of the data. If the data is deemed privacy sensitive, the Recipient must comply with the applicable federal, state, and local privacy laws, as well as DHS and university/research institute policies regarding the collection and use of personally identifiable information (PII).
        ii. The uses of the data.
        iii. A written commitment from the data's owner(s) to provide the Recipient the required data and the conditions under which the data will be provided.
        iv. A plan for the disposal or retention of the data after the research ends.

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

11. Information Protection Plan

a. 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).

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.

b. 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.

c. 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.

d. 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.

e. 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.

f. Definitions: For purposes of this section.

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

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

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

Personally Identifiable Information (PII). Any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department.

Sensitive PII is PII which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

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

12. 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.

13. Research Safety Plan

a. DHS COE research addresses issues of importance to intelligence and counter-terrorism agencies, law enforcement, or emergency responders, all of which involve inherent risks. To ensure that researchers and research facilities funded through this Award meet the highest safety standards possible, DHS requires every Recipient of a COE award to develop a Research Safety Plan. The Recipient shall review the Research Safety Plan at least annually and identify or update, as necessary, any new areas of research or sub-recipients conducting research activities under this plan. This review will also ensure that all sub-recipients conducting research covered by this plan have developed and implemented appropriate safety plans and periodic safety training in accordance with their institutional policies and procedures. Recipient will submit any updates to the Research Safety Plan to the DHS Program Officer for review and comment.

b. The Research Safety Plan must include, at a minimum, the following:

i. Identification of possible research hazards associated with the types of research to be conducted under this Award;

ii. Research protocols or practices that conform to generally accepted safety principles applicable to the nature of the research;

iii. The Recipient's processes and procedures to ensure compliance with the applicable protocols and standards;

iv. The Recipient's processes and procedures to ensure the prevention of unauthorized activities conducted in association with this Award;

v. Faculty oversight of student researchers;

vi. Research safety education and training to develop a culture of safety;

vii. Access control, where applicable;

viii. Independent review by subject matter experts of the safety protocols and practices; and

ix. Demonstrated adherence to all safety-related terms and conditions contained elsewhere in this Award.

c. Flowdown Requirements: The Recipient shall include the substance of this section in all sub-awards/contracts at any tier where the sub-Recipient may conduct research where safety protocols are necessary to conduct safe research.

14. 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.

15. 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.

i. 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 subject matter experts (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 Homeland Security Enterprise (DHS, federal/state/local 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 workplan and activities funded through this Award through face-to-face and/or telephone meetings and review of progress reports.

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

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

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

7. DHS employees may co-author publications with COE researchers. Any publication co-authored by DHS staff 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 13, in Section A.

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

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

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

C. AMENDMENTS AND REVISIONS

1. Budget Revisions.
   a. Transfers of funds between direct cost categories in the approved budget when such cumulative transfers among those direct cost categories exceed ten percent of the total budget approved in this Award require prior written approval by the DHS Grants Officer.
   b. The Recipient shall obtain prior written approval from the DHS Grants Officer for any budget revision that would result in the need for additional resources/funds.
   c. The Recipient is not authorized at any time to transfer amounts budgeted for direct costs to the indirect costs line item or vice versa, without prior written approval of the DHS Grants Officer.

2. Extension Request.
   a. Extensions to the Period of Performance can only be authorized in writing by the DHS Grants Officer.
   b. The extension request shall be submitted to the DHS Grants Officer sixty (60) days prior to the expiration date of the performance period.
   c. Requests for time extensions to the Period of Performance will be considered, but will not be granted automatically, and must be supported by adequate justification to be processed. The justification is a written explanation of the reason or reasons for the delay; an outline of remaining resources/funds available to support the extended Period of Performance; and a description of performance measures

necessary to complete the project. Without performance and financial status reports current and justification submitted, extension requests shall not be processed.

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

D. EQUIPMENT

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

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

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

E. FINANCIAL REPORTS

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

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

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

F. PAYMENT

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

G. PERFORMANCE REPORTS

1. Annual Performance Reports. The Recipient shall submit 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. These reports shall include:
      i. Summary reports on the Center's strategic vision and activities;
      ii. Summary of Center management efforts;
      iii. Performance reports on each Center Project to include:
         - Explanation of any changes from the initially approved workplan
         - Progress against each milestone and explanation of why milestones were not reached
         - Unanticipated problems and plans for addressing them; and
         - Information on how project outcomes will advance or impact current technologies or capabilities.
      iv. Budget information categorized by both object class and project
      v. If applicable, include a certification that no patentable inventions were created during the budget period.
      vi. Updates to the Center's Information Protection Plan and Researcher Safety Plan as needed.

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

2. 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 Department of Homeland Security's (DHS's), acceptance and approval of each non-competing continuation application, and the availability of the next year's annual DHS appropriations. The Recipient shall only incur costs or obligate funds within the Project Period for approved activities.

2. Budget Period. The Budget Period shall be for a period of 12 months, from July 1, 2017 through June 30, 2018.

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

3. Non-Competing Continuation Requirements.

    a. Ninety (90) days prior to the expiration date of each budget period, the Grants Officer will request submission of the annual incremental funding request details via Grants.gov website. The Recipient shall submit a non-competing continuation application to request the next Budget Period's incremental funding and a separate request for any possible carryover of prior year funds. The non-competing continuation application shall include:
        i. An annual project work plan as described in Article A, Item 3
        ii. Carryover of Funds. Recipients are required to submit a separate Carryover Application for the unobligated balances remaining from funds awarded in one budget period to be carried over to the next succeeding budget period. This submission is due to the DHS Grants Officer and DHS Program Manager 90 days prior to budget period expiration (e.g., March 31) and is a best estimate at the budget period expiration from the recipient (lead university and all sub-recipients). The Program Officer will review the Carryover justification, in consultation with the DHS Grants Officer, and provide input to the Grants Officer that the justification is reasonable and the carryover

funds should be used to complete any objectives which remain unmet from the prior budget period. Requests for carryover of funds from one Budget Period to the next Budget Period shall be submitted separately via email to the DHS Grants Officer with an SF 424 (R&R) face page and shall include:

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

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 15.

I. PRIOR APPROVAL REQUIRED

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

ARTICLE II. GENERAL TERMS AND CONDITIONS

A. ACCESS TO RECORDS.

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

1. If any litigation, dispute, or audit is started before the expiration of the 3-year period, the records shall be retained until all litigation, dispute or audit findings involving the records have been resolved and final action taken.

2. Records for real property and equipment acquired with federal funds shall be retained for 3 years after final disposition.

3. The DHS Grants Officer may direct the Recipient to transfer certain records to DHS custody when he or she determines that the records possess long term retention value. However, in order to avoid duplicate recordkeeping, the DHS Grants Officer may make arrangements for the Recipient to retain any records that are continuously needed for joint use.

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

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

B. COMPLIANCE ASSURANCE PROGRAM OFFICE 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 Compliance Assurance Program Manager. 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 Treaty Compliance Form and an updated Statement of Work detailing the proposed modification. 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 Form, 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.

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, 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 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 in Section **B.1** 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, Select Agent and Toxin Security. **In addition to the documentation referenced in Section B.1 above, each facility conducting activities involving BSAT under this Award must submit copies of the following documentation to the CAPO for review prior to the initiation of such activities:**

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

The Recipient should contact the CAPO at STregulatorycompliance@hq.dhs.gov to obtain the RCO Documentation Request Checklist, submit documentation, or request more information regarding the DHS RCO documentation and compliance review requirements. The 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 RCO documentation sufficient to illustrate this compliance. The RCO will evaluate compliance measures for these institutions on a case-by-case basis. The Recipient must not initiate work nor provide funds for the conduct of biological laboratory work under this Award without RCO's formal written approval.

E. 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; and any additional requirements set forth in the DHS Directive for the Care and Use of Animals in Research (026-01). Each Recipient and any

Recipient institution planning to perform research involving animals under this Award must comply with the requirements and submit the documentation outlined in this section.

1. Requirements for Initial Review of Research Involving Animals. Research Involving Animals includes any research, experimentation, biological testing, and other related activities involving live, vertebrate animals, including any training for such activities. Each facility conducting research involving animals under this Award must submit copies of the following documentation to the 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) inspection report(s) for AAALAC-accredited institution(s) housing and/or performing work involving animals under this Award.

All documentation, as well as any questions or concerns regarding the requirements referenced above, should be submitted to the 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 RCO compliance assurance functions, which may include but are not limited to periodic site visits, program reviews, and facility inspections.

2. Requirements for Ongoing Review of Research Involving Animals. For ongoing animal research activities, each Recipient and any Recipient institutions must submit updates to the 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 inspection report, 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 all DHS requirements for work involving animals. All entities involved in activities under this Award must comply with applicable national and regional/local regulations, and standards and guidelines equivalent to those described for U.S. institutions (e.g., Title 9, C.F.R, Chapter 1, Subchapter A; *Public Health Service Policy on Humane Care and Use of Laboratory Animals; the Guide for the Care and Use of Laboratory Animals; and the Guide for the Care and Use of Agricultural Animals in Agricultural Research and Teaching*). The Recipient must provide 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. 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 under this award 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 under this Award 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).

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, *Protection of Human Subjects*, and any related DHS policies and instructions prior to initiating any work with human subjects under this Award. Each Recipient and any Recipient institutions planning to perform research involving human subjects under this Award must submit the documentation outlined in this section for 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 is incorporated 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.

d. 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.

e. 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

f. 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.

g. 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 2 C.F.R. Part 200.

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:

CBP:	Customs and Border Protection
CBTS:	Center for Countering Biological Threats
COE:	Center of Excellence
DHS:	U.S. Department of Homeland Security
FEMA:	Federal Emergency Management Agency
FFRDC:	Federally Funded Research and Development Center
HSE:	Homeland Security Enterprise
ICE:	Immigration and Customs Enforcement
MSI:	Minority Serving Institution
NOFO:	Notice of Funding Opportunity
NPPD:	National Protection and Programs Directorate
OUP:	S&T's Office of University Programs
PPD:	Presidential Policy Directive
PPE:	Personal Protective Equipment
PBTH:	Priority biological threats and hazards
QHSR:	Quadrennial Homeland Security Review
RDP	S&T's Research and Development Partnerships Group
S&T:	Science and Technology Directorate
SME:	Subject Matter Expert
STEM:	Science, Technology, Engineering and Mathematics

TSA:	Transportation Security Administration
USCG:	U.S. Coast Guard
USSS:	U.S. Secret Service

APPENDIX C: 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
- HSPD-4 *National Strategy to Combat Weapons of Mass Destruction* -issued in 2002, Homeland Security Presidential Directive (HSPD) 4 depicts the "three pillars" in the fight against weapons of mass destruction: counter proliferation to combat WMD use; strengthened nonproliferation to combat WMD proliferation; and consequence management to respond to WMD use. The Strategy also details the four "cross-cutting enabling functions" to be pursued: intelligence collection and analysis on WMD, delivery systems, and related technologies; research and development to improve our ability to respond to evolving threats; bilateral and multilateral cooperation; and targeted strategies against hostile states and terrorists.[18]
- Critical infrastructure and key resources provide the essential services that underpin American society. The Nation possesses numerous key resources, whose exploitation or destruction by terrorists, or that is impacted 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, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being.[19] To help mitigate this risk, in 2003, Homeland Security Presidential Directive (HSPD) seven (7): *Critical Infrastructure Identification, Prioritization, and Protection* was established. 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.[20]
- 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

[18] "National Strategy to Combat Weapons of Mass Destruction". United States: White House Office (December 2002), https://www.hsdl.org/?view&did=860

[19] Department of Homeland Security. https://www.dhs.gov/homeland-security-presidential-directive-7

[20] Weekly Compilation of Presidential Documents (December 22, 2003), v.39 n.51, p.1816-1822 http://www.gpoaccess.gov/wcomp/index.html

delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities.[21]

- HSPD-18 *Medical Countermeasures Against Weapons of Mass Destruction*- issued in 2007, this directive addresses the need to be prepared for an attack by terrorist forces using a weapon of mass destruction. It acknowledges that having sufficient resources on hand at all times and at all places is not a realistic feasibility. The policy set forth in the HSPD is "a two tiered approach for development and acquisition of medical countermeasures, which will balance the immediate need to provide a capability to mitigate the catastrophic of the current CBRN threats with long-term requirements to develop more flexible spectrum countermeasures to address future threats." Tier I is a focused development of Agent-Specific Medical Countermeasures and Tier II concerns the development of a Flexible Capability for New Medical Countermeasures.[22]
- HSPD-21 *National Strategy for Public Health and Medical Preparedness*- was issued in October 2007 to establish a National Strategy for Public Health and Medical Preparedness, which builds upon principles set forth in HSPD-10 with the goal of transforming the national approach to protecting the health of the American people against all disasters.[23]
- PPD-2 *Implementation of the National Strategy for Countering Biological Threats*- This directive focused on supporting a subset of mission areas outlined in HSPD-10, largely with respect to international efforts. Specifically, PPD-2 outlines the President's vision for addressing the challenges from proliferation of biological weapons or their use by terrorists. It also emphasizes the need to (1) improve global access to the life sciences to combat infectious disease regardless of its cause; (2) establish and reinforce norms against the misuse of the life sciences; and (3) institute a suite of coordinated activities that collectively will help influence, identify, inhibit, and/or interdict those who seek to misuse the life sciences.
- National Biosurveillance Science and Technology Roadmap, June 2013; identifies and prioritizes research and development (R&D) needs with the goal of giving decision makers at all levels of government more accurate and timely information when biological incidents threaten health.[24]
- National Strategy for Biosurveillance, July 2012; promotes an all-of-Nation approach that brings together Federal, state, local, and tribal governments; the private sector; non-governmental organizations; and international partners to identify and understand threats

---

[21] "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

[22] "HSPD-18 Medical Countermeasures against Weapons of Mass Destruction". Government Publishing Office. Weekly Compilation of Presidential Documents (February 12, 2007), v.43 n.6, p.128-134,
https://www.gpo.gov/fdsys/pkg/PPP-2007-book1/pdf/PPP-2007-book1-doc-pg109.pdf

[23] "Biodefense for the 21st Century". The White House, Office of the Press Secretary. April 28, 2004.
http://fas.org/irp/offdocs/nspd/hspd-10.html

[24] "National Biosurveillance Science and Technology Roadmap". Executive Office of the President, Office of Science and Technology Policy. June 14, 2013.
https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/biosurveillance_roadmap_2013.pdf

as early as possible and provide accurate and timely information to support life-saving responses.[25]

- U.S. Public Law 107–56, *the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*- First, "Section 817. Expansion of the biological weapons statute," includes certain provisions put forth by H.R. 3160, the Bioterrorism Prevention Act of 2001, limits the possession of select agents to reasonable quantities for research purposes, and prevents the possession of select agents by restricted persons including illegal aliens and convicted criminals.
- Second, "Section 1013. Expressing the sense of the senate concerning the provision of funding for bioterrorism preparedness and response," calls for an investment to improve bioterrorism preparedness, response, food safety, and surveillance capabilities.
- U.S. Public Law 107–188, *the Public Health Security and Bioterrorism Preparedness and Response Act of 2002*- Directed the Secretary of HHS to create a strategy for responding to acts of bioterrorism and other public health emergencies, including the development of medical countermeasures against biological agents and toxins. This law allowed for the establishment of an Assistant Secretary for Public Health Emergency Preparedness within HHS to oversee these activities. Additionally, the Secretary of HHS was directed to maintain a strategic national stockpile of drugs, vaccines, medical devices, and other supplies in the event of a public health emergency and to improve state, local, and hospital preparedness for such emergencies.
- U.S. Public Law 107–296, *the Homeland Security Act of 2002*- Created the Department of Homeland Security (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 108–276, *the Project BioShield Act of 2004*- Authorized HHS to fund expedited research, development, and acquisition of priority medical countermeasures to be used in emergencies following terrorist attacks perpetrated using CBRN agents. This Law also directs the Secretary of HHS to coordinate with the Secretary of DHS regarding maintenance and deployment of the Strategic National Stockpile.
- U.S. Public Law 109-417, *the Pandemic and All-Hazards Act (2006)*- Granted HHS additional authority related to the development of medical countermeasures, including countermeasures against biological agents causing public health emergencies not caused by a terrorist attack.
- Requires the Secretary of HHS to lead the federal public health and medical response to public health emergencies.

[25] "National Strategy for Biosurveillance". Executive Office of the President, Office of Science and Technology Policy. July 31, 2012. https://obamawhitehouse.archives.gov/sites/default/files/National_Strategy_for_Biosurveillance_July_2012.pdf

- U.S. Public Law 110-53, *Implementing Recommendations of the 9/11 Commission Act of 2007*- Enacted wide-ranging legislation with many components affecting U.S. biodefense efforts, including (i) replacing the DHS Directorate of Information Analysis and Infrastructure Protection with the Office of Intelligence and Analysis and a separate Office of Infrastructure Protection as one step to improve information sharing and (ii) forming a National Biosurveillance Integration Center (NBIC) within DHS to provide early detection and warning of biological threats. This also expanded U.S. efforts to prevent the proliferation of WMD, by establishing a coordinator for the Prevention of Weapons of Mass Destruction Proliferation and Terrorism and a Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism.
- 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.
- U.S. Public Law 113-5, *Pandemic and All-Hazards Preparedness Reauthorization Act* - enacted in 2013 reauthorizes specific programs under the Public Health Service Act and the Federal Food, Drug, and Cosmetic Act with respect to public health security and all-hazards preparedness. The law authorized funding for public health and medical preparedness programs, such as the Hospital Preparedness Program and the Public Health Emergency Preparedness Cooperative Agreement, amending the Public Health Service Act, to grant State Health Departments greatly needed flexibility in dedicating staff resources to meeting critical community needs in a disaster.
- International Treaties and Partnerships:
- Convention on the Prohibition of the Development, Production, and Stockpiling of Bacterial (Biological) and Toxin Weapons and their Destruction- enforced by March 26, 1975 international parties agreed on disarmament, including the prohibition and elimination of all types of weapons of mass destruction, and convinced that the prohibition of the development, production and stockpiling of chemical and bacteriological (biological) weapons and their elimination, through effective measures, will facilitate the achievement of general and complete disarmament under strict and effective international control.[26]
- International Health Regulations - issued in 2005, these legally binding regulations strive to a) assist countries to work together to save lives and livelihoods endangered by the spread of diseases and other health risks, and b) avoid unnecessary interference with international trade and travel.[27]
- Global Health Security Agenda - launched in February 2014, consisting of a growing partnership of nearly 50 nations, international organizations, and non-governmental stakeholders to help build countries' capacity to help to prevent, detect, and respond to

[26] "Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction". The U.S. Department of State, Bureau of International Security and Nonproliferation. http://www.state.gov/t/isn/4718.htm

[27] "Strengthening health security by implementing the International Health Regulations". World Health Organization. 2005. http://www.who.int/ihr/publications/9789241596664/en/

human and animal infectious diseases threats whether naturally occurring or accidentally or deliberately spread.[28]

[28] Global Health Security Agenda, August 2016. https://ghsagenda.org/