PARTNERSHIP INTERMEDIARY AGREEMENT

BETWEEN
THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
AND
THE MARYLAND DEPARTMENT OF BUSINESS & ECONOMIC DEVELOPMENT
AND
THE MONTGOMERY COUNTY DEPARTMENT OF ECONOMIC DEVELOPMENT
REGARDING THE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Institute of Standards and Technology (NIST) of the United States Department of Commerce, the Maryland Department of Business & Economic Development (DBED), and Montgomery County, Maryland, through its Department of Economic Development (DED), (hereinafter referred to individually as a Party or collectively as the Parties) enter into this Partnership Intermediary Agreement (PIA or Agreement) pursuant to Section 3715 of Title 15 of the United States Code, "Use of Partnership Intermediaries."

Article 1. Purpose

This Agreement is entered into in furtherance of the collaboration memorialized in the Memorandum of Understanding between Montgomery County, Maryland and the State of Maryland and the National Institute of Standards and Technology (NIST) dated February 21, 2012 (MOU), which intended to establish the National Cybersecurity Center of Excellence (NCCoE) as a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. A copy of the MOU is attached as Exhibit A.

Article 2. Parties

NIST is a non-regulatory agency of the United States Department of Commerce, the mission of which is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.

DBED is an agency of the State of Maryland which stimulates private investment and creates jobs by attracting new businesses, encouraging the expansion and retention of existing companies, and providing workforce training and financial assistance to Maryland companies. DED is an agency of Montgomery County, Maryland, the job of which is to stimulate job growth and encourage business location and expansion in Montgomery County. Both DBED and DED assist, counsel, advise, evaluate, or otherwise cooperate with small business firms that need or can make demonstrably productive use of technology–related assistance from a Federal laboratory. As such, each is a "partnership intermediary" within the meaning of 15 U.S.C. § 3715(c).

Article 3. Background

Section 3715 of Title 15 of the United States Code (Use of Partnership Intermediaries) specifically authorizes the Director of a Federal Laboratory (including the Director of a Federally Funded Research and Development Center (FFRDC) laboratory) to enter into memoranda of understanding and contracts with State and local governmental agencies and nonprofit entities owned, chartered, funded, or operated by or on behalf of a State or local government to perform services for the Federal Laboratory that increase the likelihood of success in the conduct of cooperative or joint activities with small business firms, institutions of higher learning and educational institutions.

In the face of the Nation's cybersecurity challenges, the NCCoE was established in 2012. The NCCoE's initial operations, carried out at facilities located on the campus of the University of Maryland at Shady Grove, in Rockville, Maryland, have affirmed the viability of this public-private collaboration model, which has brought together experts from industry, government and academia to build and demonstrate integrated cybersecurity solutions that are cost-effective, repeatable and scalable. In 2013, the NCCoE launched its first "Use Case," the Secure Exchange of Electronic Health Information Demonstration Project, to develop a platform that allows health care providers to securely document, maintain and exchange clinical information using electronic methods. This first Use Case focused on securely exchanging health information via a mobile device. In addition to sector-specific Use Cases, the NCCoE is working on "Building Block" solutions that can be applied across industry sectors. The first of these, Trusted Geolocation in the Cloud, has as its objective strengthening the security of virtualized infrastructure cloud computing technologies by using Infrastructure as a Service (IaaS) to address security challenges tied to shared cloud servers.

It is envisioned that the NCCoE will serve as a national resource to integrate commercially available technologies to build practical cybersecurity solutions that can be applied to industry sector cyber challenges. In so doing, the NCCoE will create a pre-competitive environment for public and private sector organizations to work together to develop cybersecurity solutions, and create an environment where new cybersecurity technologies and applications can be identified, tested, and refined. Important objectives of the NCCoE include engaging a spectrum of technology and industry partners to accelerate the transfer and availability of solutions to the marketplace, and creating an effective access point for government-developed cybersecurity technologies and applications to be made available for licensing and co-development by the private sector. The Parties anticipate that the NCCoE will leverage federal cybersecurity assets located in Maryland, and increase commercial opportunities that can further economic development objectives.

The Parties contemplate the need to expand the NCCoE facilities as the NCCoE prepares to undertake multiple simultaneous specific industry sector Use Cases and Building Block solution efforts, each of which will involve one or more different teams of collaborators. In addition to participation of industry partners from large information technology sector firms, an important aspect of the NCCoE's activities will be engagement with small business firms as well as institutions of higher learning and educational institutions. The Parties also concur in the particular importance of facilitating the participation of small business firms, including start-ups,

in the NCCoE. Such small business firms may not have the resources that allow large business firms, such as many National Cybersecurity Excellence Partnership (NCEP) partners, to co-locate at NCCoE facilities and/or to otherwise participate along with academic experts and NIST staff. Yet, such participation will be critical to the success of the NCCoE mission.

Accordingly, the Parties recognize the need for expanded facilities operations services to increase the likelihood of success in the conduct of cooperative NCCoE activities with small business firms, institutions of higher learning and educational institutions, as well as with other NCCoE partners, which may include other Federal agencies, under this Agreement.

Article 4. Designated Representatives

The NIST designated representative responsible for coordination of activities under this Agreement is Donna Dodson, Acting Director, NCCoE. The NIST representative will coordinate directly with the designated DBED representative and the designated DED representative.

The DBED designated representative responsible for coordination of activities under this Agreement is Jeffrey Wells, Executive Director of Cybersecurity, DBED. The DBED representative will coordinate directly with the designated NIST representative and the designated DED representative.

The DED designated representative responsible for coordination of activities under this Agreement is Steve Silverman, Director, DED. The DED representative will coordinate directly with the designated NIST representative and the designated DBED representative.

Each Party agrees to notify the other Parties in writing of a change in that Party's designated representative.

Article 5. Agreement Activities

5.1 General.

To accomplish the purposes of this Agreement, the Parties' designated representatives will use their best efforts to identify activities under which small business firms, institutions of higher learning and educational institutions can make demonstrably productive use of technology-related assistance through the NCCoE. The Parties will use their best efforts to accomplish the purpose of this Agreement.

The NCCoE is under the technical direction and control of NIST. NIST has published its intention to sponsor an FFRDC to support the NCCoE.[1] Assuming approval for NIST to

[1] The first of three Federal Register Notices, "Proposed Establishment of a Federally Funded Research and Development Center-First Notice," is at https://federalregister.gov/a/2013-09376. The second, "Proposed Establishment of a Federally Funded Research and Development Center-Second Notice," is at http://www.gpo.gov/fdsys/pkg/FR-2013-06-21/html/2013-14897.htm. The third, "Proposed Establishment of a Federally Funded Research and Development Center-Third Notice," is at https://federalregister.gov/a/2013-17025.

establish an FFRDC is granted, NIST anticipates issuing a solicitation in the spring of 2014 for proposals to operate the FFRDC. The proposed FFRDC contract will provide research, development, engineering, and technical support to the NCCoE; program and project management; and facilities management, if necessary. Accordingly, NIST contemplates, and the Parties understand and agree, that this Agreement may be amended, once the FFRDC is established and a contract for its operation is awarded, including the possibility of adding the FFRDC as a Party.

5.2 Technology Transfer Activities.

The NCCoE is dedicated to furthering innovation through the rapid identification, integration and adoption of practical cybersecurity solutions. It is contemplated that the NCCoE will evolve into a technology transfer hub for cyber solutions derived from government and private sector tools as they apply to specific sectors of the Nation's infrastructure, such as energy, financial services, telecommunications, transportation, and health, and as a key location for major research and development in cybersecurity as it applies to these and other key sectors of the U.S. economy. It is contemplated that DBED and DED will serve as primary agents, and all Parties will work in active collaboration in generating and facilitating technology transfer of security capabilities and platforms developed through NCCoE programs and projects and other federal entities. Once the FFRDC is established and a contractor is chosen, more specific objectives and metrics will be identified and may be agreed to by the Parties. It is also understood and agreed that DBED and DED will be primarily responsible for efforts to engage with institutions of higher learning, educational institutions, and private sector entities that may desire use of facilities in connection with the NCCoE through direct agreements with such institutions or entities. In these capacities, it is contemplated that the activities of DBED and DED may include active collaboration with the NCCoE for:

a) developing and maintaining significant interactions with key commercial industry sectors for the identification of cybersecurity needs within those industry sectors where the NCCoE can contribute in accordance with its mission;

b) facilitating access for small and emerging businesses in order to encourage their participation in the development of use case solutions;

c) empowering commercial organizations to use the NCCoE as a tool to proactively develop and deploy cybersecurity solutions for specific industry sectors;

d) fostering a physical environment in which businesses can locate in and around the NCCoE in order to work more closely with the Federal government, but also to work more closely in development of pre-competitive and non-competitive cybersecurity solutions;

e) supporting the creation and growth of innovative cyber security platforms, mechanisms, and demonstrations developed at the NCCoE, including facilitating the ability of small business firms to co-locate at or locate near the NCCoE through the provision of flexible terms such as below market rent, short-term lease options, and lease options without requirement for personal guarantees;

f) establishing industry incubators for commercial availability and adoption of, and participation in, NCCoE security platforms, especially by small business firms;

g) integrating incubator activities into state and local economic development planning;

h) identifying industry association partners and facilitating meetings between the NCCoE and private sector representatives (including both large and small business firms) to allow for the NCCoE to provide overviews of its mandate and goals and solicit feedback and input from the private sector regarding those elements;

i) working with key representatives at NIST to develop a communication protocol by which information regarding cybersecurity standards is shared to provide an opportunity for various industry sectors to hear first-hand what is being proposed and interact directly with NCCoE participants in understanding the solution;

j) coordinating with NIST to identify other Federal agencies that will be relevant to achieve the NCCoE's cybersecurity mission and that will also be beneficial to achieve the economic development objectives of the State and County;

k) working with NIST, the NCCoE, and private sector companies to identify cybersecurity workforce needs and requirements, and to advance the programmatic development of workforce training and education;

l) working with high schools, colleges, universities, and the Federal Government to implement appropriate programs to meet the need of these groups;

m) assisting in developing and implementing strategies to recruit local, state, regional and national organizations for issue solicitation and development; and

n) promoting the NCCoE's business and physical environment, accomplishments, and participants.

5.3 Facilities Operation Services.

The Parties agree that the identification and ongoing management of facilities is a critical step in the development of the NCCoE. NIST has developed a Program Of Requirements (POR) for a facility to meet the needs of the NCCoE during its development and maturation. In addition to the NCCoE, there is also a need for space that can be used to incubate and support new and emerging cybersecurity and cybersecurity-related companies, house representatives from firms working on various projects at the NCCoE, and for firms to locate in proximity to accelerate co-development efforts. The financial arrangements between NIST, DBED and DED are pending the capital cost assessment for the expanded NCCoE facilities. DBED and DED have prospectively identified the William Hanna Center for Innovation at Shady Grove (previously known as the Shady Grove Innovation Center and as the Maryland Technology Development Center) (the "Center") as the location for the expanded NCCoE, and the agencies will play a role in the ongoing support for the Center. Additionally, as noted above, Facilities Operations Services under this Agreement will include, but are not limited to, property provisioning, ownership/leasehold and management of non-Federal property, and development and management of technology transfer relationships through business incubation activities.

It is contemplated that the responsibilities of DBED and DED, as part of their responsibilities for Facilities Operation Services in accordance with this Agreement, and reflecting their experience and expertise in Business Innovation Network programs, will include providing NCCoE laboratory, office, conference, and collaboration facilities in accordance with the POR for the duration of NCCoE residency at the Center; and managing facility occupancy agreements with the NCCoE. It is expected that the Parties, along with the Maryland Economic Development Corporation (MEDCO) will enter into a license agreement outlining specific terms and conditions for the NCCoE occupancy of the Center including, but not limited to, NCCoE's responsibility for providing payments for utility costs, licensee services and other operational elements. In addition, the Parties will coordinate efforts to identify and manage, as appropriate, facilities not contractually associated with Federal NCCoE development, demonstration, and documentation activities; establishing industry incubators for commercial availability and adoption of NCCoE security platforms, especially by small business firms; supporting the NCCoE structure both physically and procedurally in order to attract firms to co-locate near the NCCoE, by providing clear opportunities for them to access and interact directly with the NCCoE; coordinating with NIST to support maximum allowable access for companies co-locating at or locating near the NCCoE; and promoting the NCCoE's business and physical environment, accomplishments, and participants.

5.4 Support for Outside Activities.

NIST will identify to DBED and DED research and development capabilities of the NCCoE that may be made available to small businesses and educational institutions that need or can make use of technology-related assistance from the NCCoE. DBED and DED may attempt to locate and advise such small businesses and interested educational institutions of the availability of such capabilities and the related procedures and conditions. In the preparation and submission of proposals, DBED and DED may choose to participate and provide such other assistance to interested small businesses or educational institutions as is consistent with their missions. NIST will fully consider all requests submitted for such support. Support may be provided as appropriate in accordance with applicable Federal laws and regulations.

5. 5 Technology Marketing Programs and Showcases.

NIST and DBED and DED, as appropriate, will cooperate in planning and presenting various programs that showcase NCCoE technology, research and development, collaborations, opportunities and capabilities.

Article 6. Effective Date and Termination

6.1 Effective Date. This Agreement will be effective upon full execution by the Parties hereto and will remain in effect for 5 (five) years thereafter, unless extended by written amendment in accordance with Section 8.2 or unless sooner terminated by a Party.

6.2 Termination. Any Party may terminate this agreement upon 60 (sixty) days written notice to the other Parties or upon mutual written agreement of the Parties.

8.7 Applicable Law. The Parties agree that the Agreement will be governed by the laws of the United States of America and the State of Maryland, as applicable to the Parties.

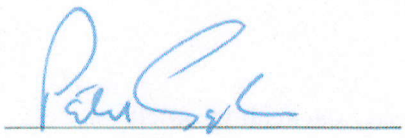
Signed by:

_____ _____

Dominick Murray Date
Secretary
Maryland Department of Business and Economic Development

_____ _____

Isiah Leggett Date
County Executive
Montgomery County



31 Jan 2014

Patrick D. Gallagher Date
Under Secretary for Standards and Technology
Director
National Institute of Standards and Technology
United States Department of Commerce

Article 7. Conditions

Activities undertaken pursuant to this Agreement shall be subject to the availability of funds and other necessary resources. Each Party to this Agreement is responsible for its own costs, unless otherwise provided for in a separate written agreement. No funds are obligated by this agreement.

Article 8. Miscellaneous

8.1 Entire Agreement. This Agreement constitutes the entire agreement between the Parties concerning the subject matter hereof.

8.2 Modification. This Agreement may be extended or modified by written agreement signed by the Parties hereto.

8.3 The Use of Name or Endorsements. No Party shall use the name or logo of any other Party on any advertisement, product or service directly or indirectly related to this Agreement without prior written authorization of the Party owning such name or logo.

8.4 Government Liability. The NCCoE is an activity of the U.S. Government. As such, the sovereign immunity of the United States applies to the activities of NIST. The Government shall be liable for the negligent or wrongful acts of its officers and employees to the extent provided for in the Federal Tort Claims Act (28 U.S.C. § 2671 et seq.) and other applicable laws and regulations of the United States that specifically waive sovereign immunity. Nothing in this Agreement shall be construed as a waiver of the sovereign immunity of the United States.

8.5 DBED and DED Liability. DBED and DED are public instrumentalities of the State of Maryland and Montgomery County, Maryland, respectively, and shall be solely responsible for the actions of their respective employees and the actions of those acting for them in the performance of this Agreement to the extent provided for under the applicable provisions of the laws of the State of Maryland. Nothing in this Agreement shall be construed as a waiver of the sovereign immunity of the State of Maryland or Montgomery County, Maryland, in accordance with applicable State law.

8.6 Montgomery County Liability. Any obligation or liability of Montgomery County arising in any way from this Agreement is subject to, limited by, and contingent upon the appropriation and availability of funds, as well as the damage caps and notice requirements provided for in state law, including the Local Government Tort Claims Act. Any obligation of the County arising under this Agreement that is deemed to require the expenditure of money by the County is expressly subject to the appropriation and encumbrance of funds by the Montgomery County Council, in the absence of which, the County shall have no liability therefor. This Agreement is not intended to create any rights or causes of action in any third parties or to increase the County's liability above the caps established by law.

8.7 Applicable Law. The Parties agree that the Agreement will be governed by the laws of the United States of America and the State of Maryland, as applicable to the Parties.

Signed by:

1/24/14

Dominick Murray
Secretary
Maryland Department of Business and Economic Development

Date

Isiah Leggett
County Executive
Montgomery County

Date

Patrick D. Gallagher
Under Secretary for Standards and Technology
Director
National Institute of Standards and Technology
United States Department of Commerce

Date

8.7 Applicable Law. The Parties agree that the Agreement will be governed by the laws of the United States of America and the State of Maryland, as applicable to the Parties.

Signed by:

Dominick Murray
Secretary
Maryland Department of Business and Economic Development

Date

Isiah Leggett
County Executive
Montgomery County

Feb 4, 2014
Date

Patrick D. Gallagher
Under Secretary for Standards and Technology
Director
National Institute of Standards and Technology
United States Department of Commerce

Date

EXHIBIT A

MEMORANDUM OF UNDERSTANDING BETWEEN MONTGOMERY COUNTY MARYLAND AND THE STATE OF MARYLAND AND THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY FOR THE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
DATED FEBRUARY 21, 2012

MEMORANDUM OF UNDERSTANDING

BETWEEN
MONTGOMERY COUNTY MARYLAND
AND
THE STATE OF MARYLAND
AND
THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)
FOR THE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Article 1. Purpose

The purpose of this Memorandum of Understanding (MOU) is to advance the mutually beneficial interests of Montgomery County, Maryland, the State of Maryland and the National Institute of Standards and Technology in collaborating on the establishment of the National Cybersecurity Center of Excellence, hereafter referred to as the 'Center.'

Article 2. Background

Cybersecurity is vital to the economic and national security interests of the United States. The cyber infrastructure of the U.S. is a strategic asset that enables more than $200 billion of e-commerce transactions in the U.S. This strategic asset of interconnected networks of computers is essential for critical functions such as air traffic control, factory operations, supply-chain logistics, electric power distribution, telecommunications, and health care delivery. The Nation's dependence on information technologies continues to deepen, and its cybersecurity efforts must expand accordingly to keep pace.

These networked systems face an ever-increasing threat of attack from individuals, organizations, and nation-states that target key information technology (IT) operations and assets. Many IT systems have a poorly implemented and maintained security configuration, hard-to-use security controls, and security postures that are too complex for most administrators to understand. This combination allows many threats to successfully compromise systems and delays reactions to these compromises, which can result in significant damage. In addition, the proliferation of security technologies targeting single applications, combined with users that are often inadequately educated or trained in cybersecurity best practices, makes the protection of cyber networks and systems a significant challenge.

In the face of such challenges, resources concentrated in the State of Maryland, including Montgomery County, have made it a national leader in securing the nation's critical infrastructure. With the National Institute of Standards and Technology (NIST), the National Security Agency, U.S. Cyber Command and other Federal cybersecurity activities, Maryland is the base for many U.S. efforts to protect and defend the country's information networks. Both the Federal government and the State of Maryland have outlined comprehensive strategies for strengthening cybersecurity, and it is important that Montgomery County, the State of Maryland, and NIST collaborate to and maximize synergies through the establishment of the Center.

A knowledge-driven economy, world-class academic institutions, Federal assets, innovative technology companies developing cutting-edge security products and a highly-educated workforce form a

foundation upon which to establish the Center. The Center will support collaborative research and development efforts between government, industry and academia to foster the accelerated development, rapid adoption, and broad deployment of comprehensive cybersecurity platforms that support automated and trustworthy cyber infrastructure.

Article 3. Cooperative Work

3.1 Roles and Responsibilities.

3.1.1 Montgomery County intends to:

a) partner with the State of Maryland and NIST on the establishment of the Center;
b) utilize the departments, agencies and economic development assets of the County to support the mission of the Center; and
c) support the creation and growth of innovative cybersecurity technologies and companies developed at the Center.

3.1.2 The State of Maryland intends to:

a) partner with Montgomery County and NIST on the establishment of the Center;
b) utilize the departments, agencies, and academic assets of the State to support the mission of the Center; and
c) support the creation and growth of innovative cybersecurity technologies and companies developed at the Center.

3.1.3 The National Institute of Standards and Technology intends to:

a) partner with Montgomery County and the State of Maryland on the establishment of the Center;
b) utilize the research assets of the Institute to support the mission of the Center; and
c) support the creation and growth of innovative cybersecurity technologies developed at the Center.

Article 4. Effective Date and Termination

4.1 Effective Date. This MOU will be effective upon full execution by the parties hereto and will remain in effect until January 1, 2017 unless extended by written agreement prior to expiration in accordance with Article 6.2 or unless sooner terminated by the parties.

4.2 Termination. Any party may terminate its participation in this MOU upon 60 (sixty) days written notice to the other parties or upon mutual written agreement of the parties.

Article 5. Conditions

Activities undertaken pursuant to this MOU shall be subject to the availability of funds and other necessary resources. Each party to this MOU is responsible for its own costs, unless otherwise provided for in a separate written agreement. No funds are obligated by this MOU.

Article 6. Miscellaneous

6.1 Entire Agreement. This MOU constitutes the entire agreement between the parties concerning the subject matter hereof.

6.2 Modification. This MOU may be extended or modified by written agreement signed by the parties hereto.

6.3 The Use of Name or Endorsements. No party shall use the name or logo of any other party on any advertisement, product or service directly or indirectly related to this Agreement without prior written authorization of the party owning such name or logo. The State of Maryland and Montgomery County shall ensure that their respective departments and agencies do not use the name or logo of NIST on any advertisement, product or service directly or indirectly related to this MOU without prior written authorization of NIST.

6.4 Not Legally Binding. This MOU is a statement of intent of the parties to collaborate as detailed above. This MOU is not legally binding upon the parties and creates no legal rights or responsibilities.

Signed by:

Isiah Leggett
County Executive
Montgomery County

02/21/2012
Date

Anthony G. Brown
Lt. Governor
State of Maryland

02/21/2012
Date

Patrick D. Gallagher
Under Secretary for Standards and Technology
Director
National Institute of Standards and Technology

02/21/2012
Date

Witness:

Barbara A. Mikulski
United States Senator
Maryland

02/21/2012
Date