NOTICE OF FUNDING OPPORTUNITY (NOFO)
Cybersecurity for Defense Manufacturing

EXECUTIVE SUMMARY

- **Federal Agency Name:** National Institute of Standards and Technology (NIST), United States Department of Commerce (DOC)

- **Funding Opportunity Title:** Cybersecurity for Defense Manufacturing

- **Announcement Type:** Initial

- **Funding Opportunity Number:** 2019-NIST-MEP-CYBERDEFMFG-01

- **Catalog of Federal Domestic Assistance (CFDA) Number:** 11.611, Manufacturing Extension Partnership

- **Dates:** Applications must be received at Grants.gov no later than 11:59 p.m. Eastern Time on May 22, 2019. Applications received after the deadline will not be reviewed or considered. The approximate start date for awards under this NOFO is expected to be in August 2019. (*See* Section V.3. in the Full Announcement Text of this NOFO.)

  Applicants should be aware of, and factor into their application submission planning, that the Grants.gov system is expected to be closed for routine maintenance at the times noted below. Applications cannot be submitted when Grants.gov is closed:

From 12:01 A.M. Eastern Time Saturday	To 6:00 A.M. Eastern Time Monday
April 20, 2019	April 22, 2019
May 18, 2019	May 20, 2019

  Applicants are strongly urged to read Section IV.2.b. – Attachment of Required Application Documents of this NOFO with great attention. Applicants should carefully follow the instructions and recommendations regarding attachments and use the Download Submitted Forms and Applications feature on Grants.gov to check that all required attachments were contained in their submission. Applications submitted without the required documents will not pass the Initial Administrative Review, described in Section V.2.a. of this NOFO.

  When developing the submission timeline, please keep in mind that: (1) all applicants are required to have a current registration in the electronic System for Award Management (SAM.gov) and Grants.gov; (2) the free annual registration process in the SAM.gov (*See* Section IV.3. and Section IV.8.a.(1). of this NOFO) often takes between three and five business days and may take as long as two weeks; (3) electronic applicants are required to have a current registration in Grants.gov; and (4) applicants

using Grants.gov will receive e-mail notifications over a period of up to two business days as the application moves through intermediate systems before the applicant learns via a validation or rejection notification whether NIST has received the application. (*See* Grants.gov for full information on application and notification through Grants.gov). Please note that a federal financial assistance award cannot be issued if the designated recipient's registration in SAM.gov is not current at the time of the award.

- **Application Submission Address:** Applications must be submitted using www.grants.gov. NIST will not accept applications submitted by mail, facsimile, or by e-mail. (*See* Section IV.2.c.(1). in Full Announcement Text of this NOFO.)

- **Funding Opportunity Description:** NIST invites proposals from current MEP Centers or consortia of Centers to provide outreach, education, and technical assistance to U.S. manufacturers who supply products within supply chains for the U.S. Department of Defense (DoD) and who must implement adequate cybersecurity protections as required in the supply of products to the DoD. The primary goal of the work to be conducted via an award issued pursuant to this NOFO is to leverage the expertise of MEP Centers to assist defense manufacturers, with an emphasis on small-to-medium sized contractors, in implementing cybersecurity protections needed to safeguard Controlled Unclassified Information (CUI) being handled in defense manufacturing supply chains. (*See* Section I. of this NOFO for additional information concerning this program.)

  Applicants are reminded that NIST is not a regulatory agency and that none of the activities contemplated under this NOFO should be directed at certifying an organization's compliance with the Defense Federal Acquisition Regulations Supplement (DFARS) clause 252.204-7012. The DoD has sole responsibility for determining compliance with the cited DFARS clause. The recipient will need to ensure that this information is conveyed to the defense contractors with which they or any subrecipients/contractors work.

- **Anticipated Amounts:** NIST anticipates funding one (1) award to a MEP Center or consortium of Centers up to a total of $1,074,000 to conduct cybersecurity awareness and educational activities for defense contractors, provide cybersecurity technical assistance to facilitate DFARS implementation for defense contractors, and pilot the implementation of enhanced operational technology security at defense contractors. The project awarded under this NOFO will have a performance period of up to 18 months. (*See* Section II.2. of this NOFO for more information regarding the availability of NIST funding for this funding opportunity.)

- **Funding Instrument:** Cooperative Agreement. (*See* Section II.1. of this NOFO for additional information concerning the funding instrument for these awards.)

- **Eligibility:** Eligible applicants for this funding opportunity are MEP Centers or consortia of Centers receiving current cooperative agreement base funding from NIST. NIST requires the submission of project proposals involving participation from multiple MEP

Centers. Proposals may also include the participation of other collaborating entities such as local economic development organizations, universities, community colleges, technology incubator programs, private third-party service providers, and other organizations.

A MEP Center may serve as the lead MEP Center applicant on only one (1) proposal. There are no restrictions on the number of applications in which a MEP Center may serve as a project collaborator. There are no restrictions on the number of MEP Centers that may be listed as participating in any individual proposal. (*See* Section III.1 of this NOFO for more information regarding program eligibility.)

- **Cost Sharing Requirements:** Non-federal cost share is not required for an award issued pursuant to this NOFO. Applicants are encouraged to submit proposals with budgets that maximize the application of award funding to the performance of project tasking and other direct project costs. (*See* Section III.2. of this NOFO for more information regarding cost sharing requirements and Section II.3. for more information regarding program income.)

Table of Contents

FULL ANNOUNCEMENT TEXT

I. Program Description

1) Statutory Authority.

The statutory authority for this program is 15 U.S.C. § 278k-1. This program is not a Federal research and development program and it is not expected that an award recipient will perform systematic research of any kind.

2) Background Information.

The National Institute of Standards and Technology (NIST) invites applications from current MEP Centers or consortia of Centers to support efforts to add capabilities to the nationwide Hollings Manufacturing Extension Partnership program (HMEPP) relative to the cybersecurity requirements and best practices for outreach, education, and assistance to manufacturers seeking to participate in various supply chains for the U.S. Department of Defense (DoD). The applicant selected pursuant to this NOFO will provide outreach, education, and technical assistance to U.S. manufacturers who supply products within DoD supply chains and who must implement adequate cybersecurity protections as required by DoD. This NOFO is being issued to support HMEPP's implementation of an Interagency Agreement (IAA) executed in 2019 between HMEPP and the Office of the Secretary of Defense (OSD).

The primary goal of the work to be conducted via an award issued pursuant to this NOFO is to leverage the expertise of MEP Centers to assist defense manufacturers,

with an emphasis on small-to-medium sized contractors, in implementing cybersecurity protections needed to safeguard Controlled Unclassified Information (CUI) being handled in defense manufacturing supply chains.

U.S. defense manufacturing supply chain operations rely on a nearly infinite number of touchpoints where information flows through a network – both within and across the manufacturers' information and operational systems that constitute the supply chains. In today's digital world, every one of these touchpoints represents a potential vulnerability to the security of our Nation's defense production through cybersecurity breaches. Data from surveys conducted by the Department of Commerce (DOC) Bureau of Industry and Security (BIS) have revealed the cybersecurity vulnerability of small manufacturers. A survey of over 9,000 classified contract facilities documented that 6,650 small facilities (<$25 million in sales) lagged medium and large firms across a broad range of 20 cybersecurity measures; among several measures, fewer than half of the small firms had cybersecurity measures in place.[1]

In 2017, the DoD issued clause 252.204-7012 of the Defense Federal Acquisition Supplement (DFARS) to ensure that defense contractors examine various control points and document adequate security to protect CUI relevant to defense manufacturing supply chains. Should shortcomings be identified during the examination, defense contractors need to develop plans to correct those shortcomings. To do this, the DFARS cybersecurity requirement calls for defense suppliers to follow the guidance contained in NIST Special Publication (SP) 800-171 rev 1[2], "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

HMEPP published a detailed Cybersecurity Self-Assessment Handbook[3] (Handbook) in November 2017 to assist small U.S. manufacturers in securing their critical information infrastructure. The Handbook provides a step-by-step guide to assessing a small manufacturer's information systems against the security controls in the SP. The Handbook strives to "reduce to practice" the security guidance for implementation by small manufacturers. Between its publication in November 2017 and the beginning of February 2019, the Handbook has been downloaded over 41,000 times, and the majority of MEP Centers have been trained in its usage. NIST also recognizes that the scope of cybersecurity for defense manufacturing – and, consequently, the impacts of risks and vulnerabilities – spans traditional

[1] "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806, September 2018, pp. 87-88.

[2] "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," NIST Special Publication 800-171 Rev. 1, December 2016. At this time, Rev. 2 is in process but has not been released, nor has DoD provided any guidance that Rev. 2 will be implemented as part of DFARS 252.204-7012. DoD's FAQs regarding implementation refer specifically to Rev. 1.

[3] NIST MEP Cybersecurity Self-assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf.

information and communications technology (IT), as well as operational technology (OT), which includes machines controlled by Programmable Logic Controllers (PLCs) and supervisory control and data acquisition (SCADA) systems. Manufacturers, therefore, face several significant challenges, many of which are unique to manufacturing operations, in implementing cybersecurity risk management safeguards, including those prescribed by DFARS clause 252.204-7012, as well as others that are also addressed in the work requirements in this NOFO.

Applicants are reminded that NIST is not a regulatory agency and that none of the activities contemplated under this NOFO should be directed at certifying an organization's compliance with the DFARS clause 252.204-7012. The DoD has sole responsibility for determining compliance with the cited DFARS clause. The recipient will need to ensure that this information is conveyed to the defense contractors with which they or any subrecipients/contractors work.

3) Program Priorities.

In accordance with 15 U.S.C. § 278k-1(e)(3), the program priorities for this competition are:

a. Improve the competitiveness of industries in the region in which the Center or Centers are located;
b. Create jobs or train newly hired employees;
c. Promote the transfer and commercialization of research and technology from institutions of higher education, national laboratories or other federally funded research programs, and nonprofit research institutes; and
d. Recruit a diverse manufacturing workforce, including through outreach to underrepresented populations, including individuals identified in section 33 or section 34 of the Science and Engineering Equal Opportunities Act (42 U.S.C. §§ 1885a and 1885b).

Applicants must articulate how their proposal achieves one or more of the program priorities listed above, while also adding new capabilities to the MEP Center program.

4) Program Requirements.

Through this NOFO, HMEPP intends to make one (1) funding award to a MEP Center on behalf of a team of MEP Centers or a consortium of MEP Centers to conduct a series of processes to improve the cybersecurity posture of the U.S. defense industrial base. The project funded pursuant to this NOFO will include activities that are consistent with HMEPP's program priorities listed above.

Total funding available under this NOFO is up to $1,074,000.00 and will be utilized to conduct the activities referenced in the three (3) bullets below and described in

further detail throughout this NOFO. Portions of this total amount will be made available for the three (3) main activities as detailed herein. Through the NOFO award, the participating MEP Centers will:

i. Conduct outreach events creating awareness by and educating defense contractors about the importance of cybersecurity to their operations, especially awareness of cybersecurity requirements contained in DFARS clause 252.204-7012 that apply to all DoD contracts that cover CUI and educating them on potential steps they can take to remediate any deficiencies;

ii. Provide defense contractors with the technical assistance they need to help ensure that they have implemented adequate security to protect CUI as required by DFARS cybersecurity requirements contained in DoD contracts; and

iii. Pilot the provision of technical assistance to defense contractors to ensure the operational technology aspects of supply chain production systems have adequate cybersecurity protections.

a. Awareness/educational outreach events.

The awareness/educational outreach events funded via this NOFO will primarily focus on the DFARS cybersecurity requirements referenced previously. Awareness/education events and activities should include but not be limited to live workshop-type events that include the participation of approximately 50-100 or more defense contractors in each state where events are held. The applicant should plan for a sufficient number of live events that it believes is required to reach between 500 and 1000 defense companies.

While the program anticipates such events will occur in up to 10 states with high concentrations of defense contractors, it is required that the these education events be able to occur on a National scale to enable coverage in any potential state that is identified as having either a high concentration of defense contractors and/or where defense contractors are operating who are identified as having a critical position within one or more defense manufacturing supply chains. The exact states to be targeted here will be identified by a combination of the MEP Centers involved in the funding award, HMEPP, and the DoD partners. Proposals submitted here should detail an approach that allows outreach to occur on a regional basis that covers any potential U.S. state and Puerto Rico.

Applicants should plan to allocate funding of approximately $300,000 of the $1,074,000 for the conduct of awareness/education events that will include participation from approximately 500 - 1,000 or more total defense contractors around the U.S. Should the applicant deviate significantly from this planning number, the applicant shall provide a specific rationale for the deviation to allow NIST to properly evaluate the task and associated budget. Awareness/education events should focus on the needs of defense contractors

who must implement adequate cybersecurity to protect CUI associated with defense contracts.

Additionally, awareness/education events should also address a range of topics on cybersecurity for manufacturing, including basic cybersecurity importance and protections that manufacturers should implement; information about the NIST Cybersecurity Framework and how to implement it within defense contractor organizations; resources available to assist defense contractors with implementing cybersecurity protections; and a primary focus on the requirements of DFARS clause 252.204-7012 that defense contractors must implement to ensure adequate security protections are in place for CUI in defense contracts. The DFARS focus of awareness/education events should also address what NIST SP 800-171 means for defense contractors with respect to its inclusion in DFARS 252.204-7012, and what defense contractors need to do to implement that guidance.

Awareness/education events should be coordinated by the team of MEP Centers participating in the proposal, including participation by the local MEP Center operating in the state where the event is held. Awareness/education events should also include the provision of subject matter expert presentations and training from NIST, DoD, MEP Centers, and other appropriate organizations at the local, state, regional, or national levels.

b. Technical assistance activities.

It is required that, in addition to the awareness/education activities, the technical assistance activities funded via this NOFO will also focus on the DFARS cybersecurity requirements for defense contractors referenced herein. Applicants should plan to allocate approximately $600,000 of the $1,074,000 total NOFO funding for the provision of direct, hands-on technical assistance by MEP Centers to approximately 10 defense contractors. Should the applicant deviate significantly from this planning number, the applicant shall provide a specific rationale for the deviation to allow NIST to properly evaluate the task and associated budget.

The exact number and identification of defense contractors who receive assistance will occur after project award, utilizing the proposed approach involving the participating MEP Centers, and in consultation with HMEPP and DoD partners. Processes in scope include taking the identified contractors through all necessary steps to ensure they have implemented adequate security to protect CUI and be compliant with DFARS 252.204-7012. Defense manufacturers who receive direct MEP Center technical assistance will be identified from among the contractors who participate in the awareness/education events also funded via this NOFO, and previously referenced herein. The exact identification of these contractors will occur after the NOFO is awarded because engagements with contractors to determine applicability will occur in conjunction with the conduct of the

awareness/education events.

Proposals should detail a flexible approach with National coverage that allows the consultations previously referenced in this section with HMEPP, the DoD, and participating Centers to occur so as to identify the contractors who will receive the assistance. These consultations may identify suppliers who participate in the awareness/education events who may be particularly critical to, or vulnerable within, DoD manufacturing supply chains.

Applicants should therefore articulate the process they propose to follow to work with HMEPP to identify contractors that will receive assistance, and what the MEP Center-provided assistance will entail.

c. Use Case Development and Implementation.

The work funded under this NOFO will also include a relationship with one or more NIST Laboratories (Labs). HMEPP will facilitate the relationship with the NIST Labs to demonstrate the pilot implementation of leading-edge manufacturing operational technology (OT) for cybersecurity for defense manufacturers.

The need for such a relationship, the details of which are provided below, is because most of the CUI protections being implemented in conjunction with DFARS 252.204-7012 relate to information systems. Additional and significant vulnerabilities also exist in conjunction with manufacturers' operational technology, including, for example, machine tools, programmable logic controllers, instrumentation, and sensors that are connected to networks.

Specifically, regarding this activity area, HMEPP will facilitate a relationship between the lead MEP Center funded through this NOFO and the NIST Labs. The work of the NIST Labs will develop implementation guidance for the NIST Cybersecurity Framework Manufacturing Profile (Manufacturing Profile) to apply to a typical small defense manufacturer's operating environment.

This implementation guidance will be based upon a set of approximately two (2) use-case scenarios from approximately two (2) small defense contractors. The participating MEP Centers will provide use-cases to HMEPP, based upon the operational environments of the identified contractors. HMEPP will review the use-cases and provide them to the NIST Labs for them to add to the implementation guidance. The two (2) defense contractors will be identified from among the manufacturers participating in the awareness/education events conducted via this NOFO. Applicants should plan to allocate $174,000 of the $1,074,000 available funding to conduct MEP Center work with the identified defense contractors for the OT implementation. Should the applicant deviate significantly from this planning number, the applicant shall provide a specific rationale for the deviation to allow NIST to properly evaluate the task and associated budget.

The funding amount will cover MEP Center assessment of each small manufacturer's operating environment to identify their OT vulnerabilities, as well as document a use-case for each contractor that details the production operations being conducted by each manufacturer, and where those production operations connect to networks that require cybersecurity protections. For planning purposes, MEP Centers can assume that approximately $30,000 could be allocated for use-case development, and the remaining approximately $144,000 allocated to use- case implementation. Should the applicant deviate significantly from this planning number, the applicant shall provide a specific rationale for the deviation to allow NIST to properly evaluate the task and associated budget.

The Manufacturing Profile implementation guidance will be provided to HMEPP by the NIST Labs. HMEPP will, in turn, work with the recipient to understand the guidance and how it should be implemented at the contractor facility. The MEP Center, in turn, will assist each manufacturer with this pilot implementation. It is not anticipated that there will be any contracted or financial assistance partnership between the participating MEP Centers and the NIST Labs. HMEPP will coordinate any needed collaboration between the participating MEP Centers and the participating NIST Labs. HMEPP will have substantial involvement with use-case development to ensure proper communication and coordination.

Submitted applications should detail the processes that the participating MEP Centers will follow to identify and to provide technical assistance to candidate small defense contractors for the pilot Manufacturing Profile OT implementations, including interactions with HMEPP and the participating NIST Labs, per the description above. This should include a description of how use-cases will be generated and how the participating MEP Centers will work with the candidate small defense contractors to pilot the implementation of the Manufacturing Profile OT guidance provided by the NIST Labs.

d. Other Program Requirements.

Applicants must include the participation of multiple MEP Centers operating in multiple states around the U.S. as part of the MEP National Network to reach and assist defense contractors on a national scale as described in this NOFO. Applications submitted in response to this NOFO should clearly articulate how the proposed effort utilizes multiple MEP Centers in the MEP National Network on a national scale to reach the targeted numbers and/or types of defense contractors in targeted states around the nation.

The approach should identify MEP Centers that will participate, including providing details of Centers' roles, and the approach should also be sufficiently flexible to allow defense contractors to be reached in any U.S. state or Puerto Rico, based upon consultation with NIST MEP and DoD partners post-award.

Applications should also clearly articulate how the proposed approach aligns with and leverages ongoing capabilities development occurring within the MEP National Network relating to cybersecurity for manufacturing. This may include, but is not limited to, interactions and collaborations with the MEP National Network Cybersecurity Working Group; the MEP National Network cybersecurity-focused activities of the MEP Center Leadership Team; the HMEPP-funded Competitive Awards Program cybersecurity project creating "Go-to" MEP Centers around the U.S. for manufacturing cybersecurity assistance; HMEPP cybersecurity efforts focused on defense manufacturers occurring in conjunction with funding provided by the DoD Office of Economic Adjustment (OEA); and the MEP National Network's use of HMEPP-published NIST Handbook 162 and other NIST-provided cybersecurity resources, including the NIST Cybersecurity Framework.

"Go-To" MEP Centers are defined by the following criteria:

- Cybersecurity is a service focus of the Center.
- The Center has staff trained dedicated to providing cybersecurity technical assistance.
- The Center has designated a National Network Coordinator for Cybersecurity.
- The Center consistently demonstrates cyber knowledge, market understanding and adds credibility to existing and potential stakeholders (*i.e.*, DoD, Homeland Security, etc.).
- The Center can act as a regional or national convener for cybersecurity best practices, awareness/education and training events.
- The Center can promote the unified "National Network" approach to cybersecurity (*e.g.*, offerings, policy, etc.).
- The Center can demonstrate an investment in identifying, developing and monetizing the next generation of cybersecurity technical assistance.
- The Center has consistently demonstrated the ability, capacity and desire to share, either virtually or in person, cybersecurity information, approaches, tools, delivery and training.
- The Center has developed a range of regional and national partners to support and promote the National Network Cybersecurity Program (State, DoD entities, FBI, Homeland Security, etc.).
- Cybersecurity is supported by the Center's Leadership as a service priority.
- The Center understands the variability of working with non-profit, university and state-based programs.
- The Center can identify other "Go-To" Centers as well as "Satellite" Centers and assist in dissemination of information to these other Centers.

A "Satellite" Center is defined by the following criteria:

- The Center is interested in providing some level of cybersecurity assistance.

- The Center meets most of the criteria of a “Go-To” Center but is unable to fill the role due to limitations such as staffing restrictions, financial restrictions, time/resource restrictions, or cybersecurity is not a “primary focus” area of the Center.
- Center is a willing recipient of assistance and support from “Go-To” Centers.

Further information regarding the HMEPP is provided at www.nist.gov/mep, with additional background information provided at https://www.nist.gov/mep/cybersecurity-defense-manufacturing. Refer to Section VII. of this NOFO, “Federal Awarding Agency Contacts,” if you seek the information via this link or via any link in this NOFO and it is either no longer working or you need more information.

II. Federal Award Information

1. Funding Instrument.

The funding instrument that will be used for any award issued pursuant to this NOFO is a cooperative agreement. The nature of NIST’s “substantial involvement” will generally be considered to be constituted as collaboration between HMEPP and the recipient organization. This includes HMEPP collaborating with the recipient on evaluating its progress and making changes relative to identification of companies and collaboration with the NIST Labs. Additional forms of substantial involvement that may arise are described in Final Office of Management and Budget (OMB) Guidance Implementing the Federal Grant and Cooperative Agreement Act, 43 Fed. Reg. 36860-65 (Aug. 18, 1978).

Examples of HMEPP involvement in cooperative agreements awarded pursuant to this NOFO may include activities such as, but not limited to:

i. Guidelines and assistance in developing scope(s) of work;
ii. Approval of key personnel;
iii. Assistance interacting with the NIST Labs, as appropriate; and
iv. Assistance to the recipient organization to define, understand, and resolve issues pertaining to the successful implementation of the pilot project.

2. Funding Availability.

HMEPP anticipates funding one (1) award, with a period of performance of up to 18 months. The total federal funding available this program is $1,074,000.

3. Program Income.

The recipient and any subrecipients of an award issued pursuant to this NOFO must expend all program income (as defined in 2 C.F.R. § 200.307) generated by the project using the "additive method" under 2 C.F.R. § 200.307(e)(2), with any excess program income to be disposed of pursuant to the “deductive method” under 2 C.F.R. § 200.307(e)(1).

In this connection, the applicant must clearly identify in its proposal whether the applicant or any of its subrecipients anticipate generating program income pursuant to the proposed project (*e.g.*, registration fees, client service fees, etc.).

If program income is anticipated under the project, the applicant must identify the anticipated amount of program income as part of the overall project budget (including subrecipient budgets) and must budget for the expenditure of such program income using the "additive method," with any excess program income to be disposed of pursuant to the “deductive method.” For purposes of this program, applicants should not budget program income as non-federal cost share.

4. Award Kick-Off Meeting.

The recipient will be required to attend a kick-off meeting, which will be held within the first 30 days of the start of the project period, to ensure that the recipient has a clear understanding of the program and project components. For planning purposes, applicants should plan for the kick-off to be held at NIST in Gaithersburg, MD. NIST may decide to conduct the kick-off meeting virtually, rather than in-person.

The kick-off meeting will last no longer than one (1) day and the project manager and appropriate key personnel who will play a significant role in managing and/or executing the award must participate. The kick-off meeting should also involve appropriate personnel from the lead MEP Center, as well as other MEP Center(s) participating in the project and may, as necessary, include personnel from other third-party collaborating entities.

Applicants must include travel and related costs for the kick-off meeting as part of the budget and these costs should be reflected in the budget table and budget narrative, which is submitted as part of the budget tables and budget narratives section of the Technical Proposal. (*See* Section IV.2.a.(6).(d). of this NOFO.)

5. MEP National Network Meetings.

HMEPP typically organizes MEP National Network meetings up to four times per year to share best practices and to discuss new and emerging trends as well as additional topics of interest. These meetings are planned throughout the United States and typically involve 2-3 days of resource time and associated travel costs for each meeting. One (1) key representative from the lead MEP Center should attend these meetings.

Applicants must include travel and related costs for at least one representative from the lead MEP Center to participate in the scheduled MEP National Network meetings in each of one (1) or two (2) project years (up to four (4) meetings per year; up to six (6) total meetings, over an award period of up to 18 months). These

costs must be reflected in the budget tables and budget narratives for each of the project's years of operation, which are submitted as part of the Technical Proposal. (*See* Section IV.2.a.(6).(d). of this NOFO). If travel and related costs for the MEP Center representative are already accounted for under another MEP award, the applicant should note this in the budget narrative and should not include travel and related costs in the budget.

The recipient MEP Center representative will be expected to actively participate during MEP National Network meetings and freely share lessons learned regarding MEP Centers serving the cybersecurity awareness/education and technical needs of small manufacturers operating in defense manufacturing supply chains, as well as information about the implementation by such manufacturers of the cybersecurity protections as required by DFARS, along with information about operational technology issues facing such manufacturers.

The recipient will be required to provide detailed analysis of the lessons learned through this work at the MEP National Network meetings. These analyses will include, but are not limited to, attributes of manufacturing companies served; participant roles from MEP Centers and partner organizations; planning of the intended approach and interactions with HMEPP, participating manufacturers, and other partners; root cause(s) for successes/failures**,** recommendations for how the outcomes of the NOFO-funded work might inform expansion of the intended goals; and how the NOFO-funded efforts align with and impact the many cybersecurity-related activities underway across the MEP National Network that are developing national capabilities for MEP Centers to provide cybersecurity assistance to U.S. manufacturers.

6. Indirect (F&A) Costs.

NIST will reimburse applicants for proposed indirect (F&A) costs in accordance with 2 C.F.R. § 200.414. Applicants proposing indirect (F&A) costs must follow the application requirements set forth in Section IV.2.a.(7). of this NOFO.

III. Eligibility Information

1. Eligible Applicants.

Eligible applicants for this program are MEP Centers receiving current cooperative agreement funding from NIST or consortia of such Centers. An applicant MEP Center must form a collaboration, teaming arrangement, or other appropriate relationship with multiple other MEP Centers to ensure the ability to reach defense manufacturers and provide hands-on technical assistance on a national basis. The relationships with other MEP Centers must have been established with the applicant MEP Center as required in Section IV.2.a.(12). of this NOFO at the time of application submission and must be documented with one (1) or more letters of commitment from the participating MEP Centers. It is anticipated that this approach

could occur via inclusion of MEP Centers in various regions around the Nation who would ensure service to manufacturers operating within their regions. It is anticipated that funding for this work through this NOFO would flow from HMEPP, to the lead MEP Center recipient, to the appropriate participating MEP Centers as subrecipients.

HMEPP recognizes that MEP Centers work with many partner organizations to most effectively reach and serve U.S. small manufacturers, and collaboration with partners of MEP Centers is encouraged as appropriate to serve the targeted defense manufacturers. In addition to multiple MEP Centers, NIST also encourages participation from other collaborating entities such as local economic development organizations, universities, community colleges, technology incubator programs, other federal programs as appropriate for awareness/education activities (*e.g.*, Procurement Technical Assistance Centers and Small Business Development Centers, among others) and other relevant organizations.

Applications submitted in response to this NOFO are required to clearly identify the lead MEP Center applicant, as well as the participating MEP Center sub-recipients, and other key organizations participating in the proposed project, including the specific teaming arrangements for each participating organization.

A MEP Center may serve as the applicant on only one (1) proposal. There are no restrictions on the number of applications in which a MEP Center can be proposed as a collaborator.

Eligibility for this program is contingent upon an applicant being an HMEPP Center at the time of application, at the time of award, and for the entire period of performance for awards issued pursuant to this NOFO. HMEPP reserves the right to take appropriate action, which may include not making an award, or terminating an award or a portion thereof, should a MEP Center fail to maintain its eligibility at all required times, whether by the lead MEP Center or a subrecipient MEP Center.

2. Cost Sharing or Matching.

Non-federal cost share is not required for awards issued pursuant to this NOFO. Applicants are encouraged to submit proposals with budgets that maximize the application of award funding to the performance of project tasking and direct project costs. While non-federal cost share is not required, applicants are reminded that, should they choose to charge registration or other fees for the awareness/education events and/or any other activities proposed, they should note those fees and treat them as described in Section II.3.

3. No Double Charging Against other NIST/MEP or Institute Awards.

Costs charged against awards issued pursuant to this NOFO may not also be charged as costs against any other HMEPP award (*i.e.*, no double-billing of

costs), or as non-federal cost share for another federal award without express permission of the funding federal agency.

IV. Application and Submission Information.

1. Address to Request Application Package.

The application package is available at Grants.gov under Funding Opportunity Number 2019-NIST-MEP-CYBERDEFMFG-01. Applicants may also request an application package by contacting the point of contact for administrative, budget, cost sharing, eligibility questions, and other programmatic questions listed in Section VII of this NOFO.

2. Content and Form of Application Submission.

a. Required Forms and Documents. The application must contain the following:

(1) SF-424, Application for Federal Assistance.

a) The SF-424 must be signed by an authorized representative of the applicant organization.

b) SF-424, Item 8.d. Zip/Postal Code field, should reflect the Zip code + 4 (#####-####) format.

c) SF-424, Item 12, should list the NOFO number 2019-NIST-MEP-CYBERDEFMFG-01.

d) SF-424, Item 18, should list the total budget information for the duration of the project.

e) The list of certifications and assurances referenced in Item 21 of the SF-424 is contained in the SF-424B.

(2) SF-424A and Budget Information.

a) An SF-424A form is not required for this application.

b) All applicants are required to use the OMB-approved, HMEPP budget templates when submitting a Budget workbook and a budget summary table. The budget should reflect anticipated expenses for the entire project, considering all potential cost increases, including cost of living adjustments. The budget should also include staff, travel, and other costs associated with the Award Kick-off Meeting and the HMEPP National Network meetings for the MEP Centers as described in Sections II.4. and II.5., respectively, of this NOFO.

c) The OMB-approved budget summary table and narrative template is available on the MEP website, https://www.nist.gov/mep/cybersecurity-defense-manufacturing. Applicants should use the Year 1 budget template and include all costs for the entire period of performance.

(3) SF-424B, Assurances – Non-Construction Programs. The SF-424B is required for all applicants that have not updated their System for Award Management (SAM.gov) entity registration since February 2, 2019 to include the Federal financial assistance certifications and representations (certs and reps). If an applicant has updated their SAM.gov entity registration since February 2, 2019 to include the certifications and representations, then the SF-424B is not required.

(4) CD-511, Certification Regarding Lobbying. For the Award Number, enter "2019-NIST-MEP-CYBERDEFMFG-01". In the Project Name field, use the Descriptive Title of Applicant's Project from field 15 of the SF-424, or an abbreviation thereof.

(5) SF-LLL, Disclosure of Lobbying Activities. (if applicable)

(6) Technical Proposal. The Technical Proposal, with a period of performance of up to 18 months, is a word-processed document, not exceeding 25 pages, that is responsive to the program description (*See* Section I of this NOFO) and the evaluation criteria (*See* Section V.1. of this NOFO). The following is a suggested format that applicants may use for the technical proposal.

a) Table of Contents. (Does not count toward the page limit.)

b) Executive Summary. (Does not count toward page limit). The executive summary should briefly (usually no longer than two pages) describe the proposed project, consistent with the evaluation criteria (*See* Section V.1. of this NOFO).

Please note, if an applicant's proposal is selected for funding, HMEPP may use all or a portion of the Executive Summary as part of a press release issued by HMEPP or for other public information and outreach purposes. Applicants are advised not to incorporate information that concerns business trade secrets or other confidential commercial or financial information as part of the Executive Summary. (*See also* 15 C.F.R. § 4.9(c) concerning the designation of business information by the applicant.) (Does not count towards page limit.)

c) Project Narrative. This section should provide a description of the proposed approach, sufficient to permit evaluation of the proposal, in accordance with details included in the proposal Evaluation Criteria. (*See* Section V.1. of this

NOFO.)

The project narrative must clearly identify the one (1) lead MEP Center applicant and the participating MEP Center sub-recipients. The project narrative must identify tasks, measurable milestones, and outcomes resulting from the proposed approach for each year of the proposed period of performance of up to 18 months (Year 1 and Year 2).

The project narrative should clearly identify the applicant's approach to the following technical aspects of project work:

- The mechanisms by which cybersecurity awareness/education for small manufacturers operating in defense manufacturing supply chains will occur in the project. Examples may include workshops, seminars, training, roundtables and forums, and other mechanisms. Additional possibilities can include internet-based approaches, and other forms of achieving direct contact with defense contractors. All mechanisms used must be able to track the manufacturer interactions that occur through the project.

- The processes to be followed in providing hands-on technical assistance to approximately 10 defense manufacturers to ensure that the proper cybersecurity protections are in place to protect the CUI in the manufacturers' defense contracts. This should specifically detail how the participating MEP Centers will provide assistance to a manufacturer to help them comply with the cybersecurity requirements in DFARS clause 252.204-7012 in their defense supply chain contracts. The manufacturers receiving assistance from the MEP Centers will be selected in consultation with HMEPP, and they will have participated in the awareness/education activities conducted in conjunction with this NOFO. Areas that should be addressed in MEP Center assistance to these manufacturers include the primary aspects of DFARS implementation as follows:

  - Development of a System Security Plan, to include an Incident Response Plan;

  - Assessment of company implementation of adequate CUI security protections, consistent with DFARS clause 252.204-7012, including a report of assessment;

  - Development of a Plan of Action with milestones for implementing all appropriate security controls, consistent with DFARS clause 252.204-7012, where the company is deficient. The processes should also address ongoing continuous monitoring and detection of company systems; and

- The processes to be followed to create manufacturer use-cases that will be delivered to the NIST Labs previously referenced herein for NIST Cybersecurity Framework Manufacturing Profile implementation guidance development. This should also address the processes to be followed to conduct a pilot implementation of the implementation guidance within the participating manufacturer operating environments. Details should be provided regarding proposed mechanics for MEP Center-HMEPP-NIST Lab interactions.

The project narrative should also clearly articulate how the proposed approach involving a lead MEP Center and a set of sub-recipient MEP Center participants will operate such that defense manufacturers operating in any region of the U.S. may be served by the educational outreach and technical assistance processes described above. For planning purposes, applications should identify an approach that specifically addresses activities and defense contractors in approximately 10 states.

The project narrative should clearly define how the proposed approach to conducting the required tasking will align with existing MEP National Network cybersecurity capabilities and capacities to build upon the many efforts of the Network occurring around the Nation. The approach should supplement and complement ongoing work and be consistent with Network-based approaches to serve the cybersecurity needs of any U.S. manufacturer anywhere in the U.S. The proposed approach should demonstrate consistency in the conduct of tasking across multiple MEP Centers in multiple states. Ongoing MEP National Network cybersecurity activities that should be aligned, complemented, and supplemented include work occurring in conjunction with the following:

- The MEP National Network Cybersecurity Working Group;
- The HMEPP-funded Competitive Award Program Cybersecurity Project developing “Go-To” Centers for cybersecurity;
- MEP cybersecurity assistance for defense contractors occurring with funding provided by the DoD OEA;
- MEP National Network cybersecurity development efforts of the MEP Center Leadership Team; and
- MEP Center utilization of HMEPP–provided resources such as NIST Handbook 162 and tips for implementing the NIST Cybersecurity Framework.

Applicants should provide details about the ability of the key personnel identified in the proposal and the applicant’s proposed management structure, as described in Section V.1.C., to successfully conduct the project being proposed. Applicants should clearly articulate how proposed organizational structures and participating personnel from the MEP Centers will be in position and ready to begin project operations upon receipt of funding award.

d) Budget Narrative and Justification. Applicants are required to use the OMB-approved, HMEPP budget templates when submitting their Single-year Budget Workbooks and budget narrative. Applicants must provide a detailed budget table and budget narrative for the entire proposed period of performance, fully explaining and justifying all proposed project funding (both revenue and expenses) in accordance with applicable federal cost principles.

The budget should be broken down by task and sub-task, consistent with the Program Requirements (*See* Section I.3. of this NOFO) and Project Narrative. (*See* Section IV.2.a.(6).c. of this NOFO.) Should an applicant deviate significantly from the budget planning number identified for each task, the applicant shall provide a specific rationale for the deviation to allow NIST to properly evaluate the task and associated budget. The budget information submitted by an applicant will be evaluated in accordance with the Budget evaluation sub-criteria. (*See* Section V.1.d(i) and Section V.1.d.(ii). of this NOFO.)

In the budget narrative, the recipient should provide adequate information to support the costs identified in each category of the budget table. At a minimum, applicants must provide: the annual salary and the percentage of time dedicated to the project by personnel to demonstrate the total cost of that individual; the airfare, lodging, per diem, number of days and number of travelers for each proposed trip; and anticipated subaward/contract amounts and the related subawardees/contractors, to the extent known at the time of application, and a detailed description of the purpose of each subaward/contract.

The lead MEP Center must also include the staff, travel and related expenses for travel to and participation in the required Award Kick-Off and MEP National Network meetings described in Sections II.4. and II.5. of this NOFO in the budget tables and budget narratives. If travel and related costs for the MEP Center representative are already accounted for under another MEP award, the applicant should note this in the budget narrative and should not include travel and related costs in the budget. The required budget table and budget narrative templates are available on the MEP website, https://www.nist.gov/mep/cybersecurity-defense-manufacturing

When preparing project budgets, applicants must be cognizant of the prohibition on double-billing costs against multiple federal awards. (*See* Section II.3 of this NOFO.) Applicants are reminded that, should they choose to charge registration or other fees for the awareness/education events and/or any other activities proposed, they should note those fees and treat them as described in Section II.3.

(7) Indirect Cost Rate Agreement. If indirect costs are included in the proposed budget, provide a copy of the approved negotiated agreement if this rate was negotiated with a cognizant Federal audit agency. If the rate was not

established by a cognizant Federal audit agency, provide a statement to this effect. If the successful applicant includes indirect costs in the budget and has not established an indirect cost rate with a cognizant Federal audit agency, the applicant will be required to obtain such a rate in accordance with the Department of Commerce Financial Assistance Standard Terms and Conditions dated October 9, 2018.

Alternatively, in accordance with 2 C.F.R. § 200.414(f), applicants that have never received a negotiated indirect cost rate may elect to charge indirect costs to a MEP award pursuant to a de minimis rate of 10 percent of modified total direct costs (MTDC), in which case a negotiated indirect cost rate agreement is not required. Applicants proposing a 10 percent de minimis rate pursuant to 2 C.F.R. § 200.414(f) should note this election as part of the budget portion of the application.

(8) Table of Abbreviations and Acronyms. (This does not contribute to the total number of pages). An alphabetical list of all abbreviations and acronyms, and their meaning, should be included.

(9) Table of Funded Project Participants and Unfunded Collaborators. (This does not contribute to the total number of pages). Provide a table that identifies all organizations that will participate in and contribute to the project, if funded, known at the time of the application submission. The table should consist of an alphabetically ordered list, by organization, of all funded project participants and all unfunded collaborators. The table should include the organization's name, address, administrative role*, scope of work (funded participants only) and proposed funding amount (funded participants only).

*Administrative roles are: applicant, subrecipient, or contractor for funded participants; and third-party contributor or collaborator if they will not receive funding.

(10) Bibliographic List of References. (This does not contribute to the total number of pages.) A complete bibliographic listing of all references used within the application should be included.

(11) Resumes of Key Personnel. (These do not contribute to the total number of pages.) One-page resumes of no more than five key personnel from each participant organization may be included; these do not count toward the page limit. Any information beyond one page for each resume and any additional resumes submitted will not be considered.

(12) Required Letters of Commitment. (These do not contribute to the total number of pages.) Letters that commit specific resources (not funding) to the project in the event that the application is funded are required from all of the following that apply:

a) Each application must include a Letter of Commitment from an authorized representative of the MEP Center applicant. The letter should describe the submitting organization's commitment to and activities in support of the proposed project.

b) If the application includes subawards, contracts or other payments to known third parties, including other MEP Centers, a draft copy of each subaward, contract or other funding vehicle must be included, to the extent known at the time of application. Subrecipient MEP Centers must also include a letter of commitment from the Center Director. The reviewers will consider the scope of each agreement and its relevance to the proposed project but will not review the agreement for legal sufficiency or for the allowability of the proposed budget.

c) Letters of Commitment should not be letters submitted by non-proposing entities wishing to vouch for the applicant's (or entities associated with the applicant) knowledge, skills, and abilities or entities to conduct the proposed work. These should be in the form of a Letter of Interest. (*See* Section IV.2.a.(13). of this NOFO.)

(13) Letters of Interest. (These do not contribute to the total number of pages.) Optional letters may be included with an application that indicate willingness from any third party to help accelerate establishment of a new, or strengthening of an existing, industry-driven technology consortium and/or dissemination of consortium project results. This may include letters from unfunded collaborators who will participate as unfunded team members, potential organizations involved across stages of the value chain, or strategic partners who can aid in any element of the plan to realize impact. Letters of Interest should outline the nature and importance of the collaboration or involvement being offered. Letters of Interest may also be from non-proposing entities wishing to vouch for the applicant's knowledge, skills, and abilities or entities to conduct the proposed work. All letters of interest must be included with the application and not sent separately to NIST.

b. Attachment of Required Application Documents. When submitting the application electronically via Grants.gov, items IV.2.a.(1) and IV.2.a.(4) are part of the standard application package in Grants.gov and can be completed through the download application process.

If items IV.2.a.(3) and IV.2.a.(5) apply to the applicant, they should be clicked on and added to the standard application package in Grants.gov and completed through the download application process.

Items IV.2.a.(2) and items IV.2.a.(6) through IV.2.a.(13) must be completed and attached by clicking on "Add Attachments" found in item 15 of the SF-424, Application for Federal Assistance. This will create a zip file that allows for transmittal of the documents electronically via Grants.gov.

Applicants should carefully follow specific Grants.gov instructions at www.grants.gov to ensure the attachments will be accepted by the Grants.gov system. A receipt from Grants.gov does not provide details concerning whether all attachments (or how many attachments) transferred successfully. Applicants using Grants.gov will receive a series of e-mail messages over a period of up to two business days before learning whether a Federal agency's electronic system has received its application.

Applicants are urged to use Grants.gov's Download Submitted Applications feature to check that all required attachments were contained in their submission. Go to the *Grants.gov Online Users Guide available at the Grants.gov site (http://go.usa.gov/cjaEh), choose Applicants, then Applicant Actions, then select the "Check My Application Status" option, click on the* Download Submitted Applications feature, and follow the directions.

Applicants can track their submission in the Grants.gov system by following the procedures at the Grants.gov site (http://go.usa.gov/cjamz). It can take up to two business days for an application to fully move through the Grants.gov system to NIST.

NIST uses the Tracking Numbers assigned by Grants.gov and does not issue Agency Tracking Numbers.

c. Application Format

(1) Paper, E-mail, and Facsimile (fax) Submissions. Will not be accepted

(2) Figures, graphs, images, and pictures. Should be of a size that is easily readable or viewable and may be landscape orientation.

(3) Font. Easy to read font (11-point minimum). Smaller type may be used in figures and tables but must be clearly legible.

(4) Line spacing. Single.

(5) Margins. One (1) inch top, bottom, left, and right.

(6) Page layout. Portrait orientation only (except figures, graphs, and pictures.)

(7) Page Limit. Twenty-five (25) pages.

a) **Page limit includes:** Cover page, Technical Proposal (with the exception of the Executive Summary), figures, graphs, tables, images, pictures, and all other pages of an application, with the exception of the page limit exclusions listed below.

b) **Page limit excludes**: Table of Contents; Executive Summary; SF- 424,

Application for Federal Assistance; Budget Information – HMEPP OMB approved Budget Table and Summary form; SF-LLL, Disclosure of Lobbying Activities; CD-511, Certification Regarding Lobbying; Budget Tables and Budget Narratives; Indirect Cost Rate Agreement; Table of Abbreviations and Acronyms; Table of Funded Project Participants and Unfunded Informal Collaborators; Bibliographic List of References Resumes of Key Personnel; Required Letters of Commitment; and Letters of Interest;

(8) Page numbering. Number pages sequentially.

(9) Paper size. 21.6 centimeters by 27.9 centimeters (8 ½ inches by 11 inches).

(10) Application language. English**.**

(11) Typed document. All applications, including forms, must be typed.

d. Application Replacement Pages. Applicants may not submit replacement pages and/or missing documents after an application has been submitted. Any revisions must be made by submission of a new application that must be received by NIST by the submission deadline.

e. Pre-Applications. NIST is not accepting pre-applications or white papers under this NOFO.

f. Certifications Regarding Federal Felony and Federal Criminal Tax Convictions, Unpaid Federal Tax Assessments and Delinquent Federal Tax Returns. In accordance with Federal appropriations law, an authorized representative of the selected applicant(s) may be required to provide certain pre-award certifications regarding federal felony and federal criminal tax convictions, unpaid federal tax assessments, and delinquent federal tax returns.

3. Unique Entity Identifier and System for Award Management (SAM). Pursuant to 2 C.F.R. part 25, applicants and recipients (as the case may be) are required to: (i) be registered in SAM before submitting their applications; (ii) provide a valid unique entity identifier in their applications; and (iii) continue to maintain an active SAM registration with current information at all times during which they have an active Federal award or an application or plan under consideration by a Federal awarding agency, unless otherwise excepted from these requirements pursuant to 2 C.F.R. § 25.110.

NIST will not make a Federal award to an applicant until the applicant has complied with all applicable unique entity identifier and SAM requirements and, if an applicant has not fully complied with the requirements by the time that NIST is ready to make a Federal award pursuant to this NOFO, NIST 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.

4. **Submission Dates and Times**. Applications must be received at Grants.gov no later than 11:59 p.m. Eastern Time on May 22, 2019. Applications received after the deadline will not be reviewed or considered. The approximate start date for awards under this NOFO is expected to be in August 2019.

5. **Grants.gov and SAM.gov**. Applicants should be aware, and factor into their application submission planning, that the Grants.gov system is expected to be closed for routine maintenance at the times noted below. Applications cannot be submitted when Grants.gov is closed:

From 12:01 A.M. Eastern Time Saturday	To 6:00 A.M. Eastern Time Monday
April 20, 2019	April 22, 2019
May 18, 2019	May 20, 2019

Applicants are strongly urged to read Section IV.2.b. – Attachment of Required Application Documents of this NOFO with great attention. Applicants should carefully follow the instructions and recommendations regarding attachments and use the Download Submitted Forms and Applications feature on www.Grants.gov to check that all required attachments were contained in their submission. Applications submitted without the required documents will not pass the Initial Administrative Review, described in Section V.2.a of this NOFO.

When developing the submission timeline, please keep in mind that: (1) all applicants are required to have a current registration in the SAM.gov and Grants.gov; (2) the free annual registration process in the SAM.gov (*See* Section IV.3. and Section IV.8.a.(1). of this NOFO.) often takes between three and five business days and may take as long as two weeks; and (3) electronic applicants are required to have a current registration in Grants.gov; and (4) applicants using Grants.gov will receive e-mail notifications over a period of up to two business days as the application moves through intermediate systems before the applicant learns via a validation or rejection notification whether NIST has received the application. (*See* Grants.gov for full information on application and notification through Grants.gov.) Please note that a federal assistance award cannot be issued if the designated recipient's registration in the SAM.gov is not current at the time of the award.

6. **Intergovernmental Review.** Applications under this Program are not subject to Executive Order 12372.

7. **Funding Restrictions.** Construction activities are not an allowable cost under this program. In addition, a recipient or a subrecipient may not charge profits, fees or other increments above cost to an award issued pursuant to this NOFO. Pre-award costs under this NOFO are subject to the prior written approval of the NIST Grants Officer.

8. Other Submission Requirements

a. Applications must be submitted electronically. Applications must be submitted via Grants.gov at www.grants.gov under announcement 2019-NIST-MEP-CYBERDEFMFG-01.

(1) Applicants should carefully follow specific Grants.gov instructions to ensure the attachments will be accepted by the Grants.gov system. A receipt from Grants.gov indicating an application is received does not provide information about whether attachments have been received. For further information or questions regarding applying electronically for the 2019-NIST-MEP-CYBERDEFMFG-01 announcement, refer to Section IV.8.

(2) Applicants are strongly encouraged to start early and not wait until the approaching due date before logging on and reviewing the instructions for submitting an application through Grants.gov. The Grants.gov registration process must be completed before a new registrant can apply electronically. If all goes well, the registration process takes three (3) to five (5) business days. If problems are encountered, the registration process can take up to two (2) weeks or more. Applicants must have a valid unique entity identifier number and must maintain a current registration in the Federal government's primary registrant database, the System for Award Management (https://www.sam.gov/), as explained on the Grants.gov Web site. (*See* also Section IV.3. of this NOFO.) After registering, it may take several days or longer from the initial log-on before a new Grants.gov system user can submit an application. Only individuals authorized as organization representatives will be able to submit the application, and the system may need time to process a submitted application. Applicants should save and print the proof of submission they receive from Grants.gov. If problems occur while using Grants.gov, the applicant is advised to (a) print any error message received and (b) call Grants.gov directly for immediate assistance. If calling from within the United States or from a U.S. territory, please call 800-518-4726. If calling from a place other than the United States or a U.S. territory, please call 606-545-5035. Assistance from the Grants.gov Help Desk will be available around the clock every day, with the exception of Federal holidays. Help Desk service will resume at 7:00 a.m. Eastern Time the day after Federal holidays. For assistance using Grants.gov, you may also contact support@grants.gov.

(3) To find instructions on submitting an application on Grants.gov, Applicants should refer to the "Applicants" tab in the banner just below the top of the www.grants.gov home page. Clicking on the "Applicants" tab produces two exceptionally useful sources of information, Applicant Actions and Applicant Resources, which applicants are advised to review.

Applicants will receive a series of e-mail messages over a period of up to two business days before learning whether a Federal agency's electronic system has received its application. Closely following the detailed

information in these subcategories will increase the likelihood of acceptance of the application by the Federal agency's electronic system.

Applicants should pay close attention to the guidance under "Applicant FAQs," as it contains information important to successful submission on Grants.gov, including essential details on the naming conventions for attachments to Grants.gov applications.

All applicants should be aware that adequate time must be factored into applicants' schedules for delivery of their application. Applicants are advised that volume on Grants.gov may be extremely heavy on the deadline date.

The application must be both received and validated by Grants.gov. The application is "received" when Grants.gov provides the applicant a confirmation of receipt and an application tracking number. If an applicant does not see this confirmation and tracking number, the application has not been received. After the application has been received, it must still be validated. During this process, it may be "validated" or "rejected with errors." To know whether the application was rejected with errors and the reasons why, the applicant must log in to Grants.gov, select "Applicants" from the top navigation, and select "Track my application" from the drop-down list. If the status is "rejected with errors," the applicant may still seek to correct the errors and resubmit your application before the deadline. If the applicant does not correct the errors, the application will not be forwarded to NIST by Grants.gov.

Refer to important information in Section IV.4. – Submission Dates and Times, to help ensure your application is received on time.

(4) Amendments. Any amendments to this NOFO will be announced through Grants.gov. Applicants may sign up on Grants.gov to receive amendments by email or may request copies. *(See* Section VII. of this NOFO.)

V. Application/Proposal Review Information

1. Evaluation Criteria.

The evaluation criteria, selection factors, and review and selection processes for this program are set forth below. Reviewers will evaluate how well the applicant's proposed approach will achieve the goals, objectives and priorities of this competition and support the HMEPP mission, as described in Section I. of this NOFO. NIST will use the following evaluation criteria in evaluating applications and assigning weights, with a maximum score of 100.

a. National-scale alignment with MEP National Network cybersecurity capabilities and capacities (30 points; sub-criteria will receive equal weight). The award funded through this NOFO will meld and operationalize many activities that have been ongoing for the past several years around the

MEP National Network to develop and deploy a consistent nationwide delivery capability in providing cybersecurity assistance to U.S. manufacturers, including defense manufacturers. This criterion evaluates how extensively the proposed approach utilizes the MEP National Network to successfully achieve NOFO goals and objectives.

i. Reviewers will assess the extent to which the proposed approach aligns with, draws upon, and complements the ongoing MEP National Network cybersecurity developmental efforts including the MEP National Network Cybersecurity Working Group, the HMEPP-funded Competitive Award Program Cybersecurity Project, MEP Center work occurring around the country with funding provided by the DoD OEA, MEP National Network efforts being pursued by the MEP Center Leadership Team, and HMEPP resources such as NIST Handbook 162 (*See* footnote 3).
ii. Reviewers will evaluate the extent to which the proposed approach demonstrates the coordinated operation of a team of MEP Centers working together to deploy consistent cybersecurity approaches that conduct the defined tasking and provide the defined services to defense manufacturers on a nationwide-scale through the participation of MEP Centers from every region of the nation.

b. Rigor of the proposed approach for MEP National Network provision of awareness/education and hands-on technical assistance to defense manufacturers (30 points; sub-criteria will receive equal weight). The technical quality and merit of the proposed approach to providing defense manufacturing cybersecurity assistance will be evaluated to ensure that NOFO goals and objectives are successfully met. This includes evaluation of the quality of the approach for awareness/education, in addition to the hands-on technical assistance for defense manufacturers.

i. Reviewers will evaluate the thoroughness and rigor of the proposed provision of hands-on technical assistance from MEP Centers to participating defense manufacturers.
ii. Reviewers will evaluate the quality of the approach to providing awareness/education to the targeted numbers of defense manufacturers as referenced herein. This includes evaluation of likelihood of reaching the desired defense contractors around the nation and the extent to which proposed awareness/education addresses cybersecurity information from authoritative sources and with national consistency. This also includes an evaluation of the extent to which awareness/education includes, but is not limited to, training on DFARS requirements, supply chain requirements flow down, and approaches to assessments.
iii. Reviewers will evaluate the quality and technical merit of the proposed approach for implementing cybersecurity protections for manufacturer operational technology via the use of the NIST Cybersecurity Framework Manufacturing Profile implementation guidance. This includes description

of the attributes and operating parameters that will be sought by MEP Centers for approximately two (2) manufacturers to create use cases and conduct pilot implementations. This also includes the technical merit of the proposed approach for piloting the implementation of the Manufacturing Profile implementation guidance in manufacturer facilities.

c. Key Personnel and Organizational Structure (20 points; sub-criteria will receive equal weight). Reviewers will assess the ability of the key personnel and the applicant's proposed management structure to successfully conduct the project being proposed. All applications must include the participation of multiple MEP Centers operating in multiple states. Reviewers will assess the significance of the effort being proposed in terms of amount of staff time being allocated to the project personnel identified by the lead MEP Center applicant and participating MEP Centers in relation to the overall proposed effort.

Reviewers will also assess the quality, merit, and extent to which the following is evident when evaluating the qualifications of the applicant and the effectiveness of the proposed program management approach:

i. Proposed personnel identified from the participating MEP Center(s) have the appropriate experience in providing MEP cybersecurity assistance to U.S. manufacturers, including manufacturers who operate in defense manufacturing supply chains; and

ii. Proposed management structure and organizational roles are clearly defined and aligned to plan, direct, monitor, organize and oversee the implementation of the proposed approach to achieve project objectives, and the proposed organizational structure flows logically from the specified approach to the project deliverables.

d. Budget. **(20 points; sub-criteria will receive equal weight).** Reviewers will assess the suitability and focus of the applicant's budget. It is expected that the amount of project award funding that is applied to direct project activity costs should be maximized and allocated among participating MEP Centers to appropriately support the achievement of project tasking, goals, and objectives. The reviewers will consider the extent to which the:

i. Proposed budget projections are reasonable and appropriate for the scale of effort to be undertaken by the applicant over each year of the proposed project plan; and

ii. The proposal's narrative explains the rationale for each of the budgeted items, including assumptions the applicant used in budgeting for the overall project, and the proposed budget is aligned to support the execution of the proposed project consistent with the objectives of the project, the objectives and expectations of this

program, and to advance HMEPP National Network goals.

2. Review and Selection Process

Proposals, reports, documents and other information related to applications submitted to NIST and/or relating to financial assistance awards issued by NIST will be reviewed and considered by federal employees, federal agents and contractors, and/or by non-federal personnel, all of whom enter into appropriate nondisclosure agreements covering such information.

a. Initial Administrative Review of Applications. All applications received in response to this NOFO will be reviewed to determine whether they are eligible, complete, and responsive to this NOFO and aligned with the program objectives as described in the Program Description (*See* Section I. of this NOFO.). Applications determined to be ineligible, incomplete, and/or non-responsive may be eliminated from further review. However, NIST, in its sole discretion, may continue the review process for an application that is missing non-substantive information, the lack of which may easily be rectified or cured.

b. Full Review of Eligible, Complete, and Responsive Applications. Applications that are determined to be eligible, complete, and responsive will proceed for full reviews in accordance with the review and selection processes below:

(1) Evaluation/Review and Ranking. All eligible, complete and responsive applications will be peer reviewed by at least three (3) independent, objective individuals with appropriate professional and technical expertise relating to the topics covered in this NOFO. Reviews will be limited to technical and cost matters, based on the evaluation criteria. (*See* Section V.1. of this NOFO.) A mix of Federal and non-Federal reviewers may be used. If non-Federal reviewers are used, the reviewers may discuss the applications with each other, but scores will be determined on an individual basis, not as a consensus. The reviewers may ask questions of some or all applicants in writing. Reviewers will assign each application a score, based on the application's responsiveness to the NOFO evaluation criteria, with a maximum score of 100.

Applicants whose applications receive an average score of 70 or higher out of 100 will be deemed "finalists all finalists. A rank order will be prepared based on the average of the reviewers' scores and assigned adjectival ratings in accordance with the following scale:

Fundable, Outstanding (90-100);
Fundable, Very Good (80-89);
Fundable (70-79); or
Unfundable (0-69).

For decision-making purposes, applications receiving the same adjectival

rating will maintain a rank order based on the average of the reviewers' scores – both within the particular adjectival ranking, as well as overall.

The Subject Matter Expert, who will be a HMEPP federal employee, will review all the reviewers' final scores, written technical comments and the final ranking of the proposals, and will provide a written recommendation to the Selecting Official concerning the funding of awards under this NOFO. The Subject Matter Expert may recommend to the Selecting Official that awards be made out of rank order (*i.e.*, from a lower adjectival category) based upon one or more of the selection factors described in Section V.2.b.(3). of this NOFO.

(2) Selection. The Selecting Official is the HMEPP Director or designee. The Selecting Official makes the final recommendation to the NIST Grants Officer regarding the funding of applications under this NOFO. The Selecting Official shall be provided all applications, all scores and all technical assessments of the reviewers, a written funding recommendation from the Subject Matter Expert, and all information obtained from the applicants during the evaluation, review, and negotiation processes.

The Selecting Official will generally select and recommend the most meritorious applications for awards based on the technical comments and adjectival rankings, recommendation from the Subject Matter Expert, and/or one or more of the selection factors described in Section V.2.b.(3). of this NOFO. The Selecting Official retains the discretion to select and recommend an application out of rank order based on one or more of the selection factors, or to recommend no applications for funding. The Selecting Official's recommendation to the Grants Officer shall set forth the bases for the selection decision.

As part of the overall review and selection process, NIST reserves the right to request that applicants provide pre-award clarifications and/or to enter into pre-award negotiations relative to programmatic, financial, or other aspects of an application, such as, but not limited to, the revision or removal of proposed budget costs, or the modification of proposed project activities, work plans, or program goals and objectives. In this regard, NIST may request that applicants provide supplemental information required by the Agency prior to award. NIST also reserves the right to reject an application where information is uncovered that raises a reasonable doubt as to the responsibility of the applicant. The final approval of selected applications and issuance of awards will be by the NIST Grants Officer. The award decisions of the NIST Grants Officer are final.

(3) Selection Factors. The Selection Factors for this NOFO are as follows:

a. The availability of Federal funds;
b. Relevance of the proposed project to the program goals and policy objectives;

c. Reviewers' evaluations, including technical comments;
d. Ensuring appropriate geographic coverage in the award of HMEPP funding to achieve national coverage of defense manufacturing needs;
e. Detailed participation from multiple MEP Centers in the conduct of the project, with broader potential participation from other MEP Centers as needed; the work
f. The selection factors contained in 15 U.S.C. § 278k-1(e)(3) and
g. Whether the project duplicates other projects funded by DOC or by other federal agencies.

c. Federal Awarding Agency Review of Risk Posed by Applicants. After applications are proposed for funding by the Selecting Official, the NIST Grants Management Division (GMD) performs pre-award risk assessments in accordance with 2 C.F.R. § 200.205, which may include a review of the financial stability of an applicant, the quality of the applicant's management systems, the history of performance, and/or the applicant's ability to effectively implement statutory, regulatory, or other requirements imposed on non-federal entities.

In addition, prior to making an award where the total federal share is expected to exceed the simplified acquisition threshold (currently $150,000), NIST GMD will review and consider the publicly available information about that applicant in the Federal Awardee Performance and Integrity Information System (FAPIIS). An applicant may, at its option, review and comment on information about itself previously entered into FAPIIS by a federal awarding agency. As part of its review of risk posed by applicants, NIST GMD will consider any comments made by the applicant in FAPIIS in making its determination about the applicant's integrity, business ethics, and record of performance under federal awards. Upon completion of the pre-award risk assessment, the Grants Officer will make a responsibility determination concerning whether the applicant is qualified to receive the subject award and, if so, whether appropriate special conditions that correspond to the degree of risk posed by the applicant should be applied to an award.

3. Anticipated Announcement and Award Date. The anticipated start date for awards made under this NOFO is expected to be in August 2019.

4. Additional Information

a. Notification to Unsuccessful Applicants. Unsuccessful applicants will be notified in writing.

b. Retention of Unsuccessful Applications. An electronic copy of each non-selected application will be retained for three (3) years for record keeping purposes. After three (3) years, it will be destroyed.

VI. Federal Award Administration Information

1. **Federal Award Notices.** Successful applicants will receive an award package from the NIST Grants Officer.

2. **Administrative and National Policy Requirements**

   a. **Uniform Administrative Requirements, Cost Principles and Audit Requirements.** Through 2 C.F.R. § 1327.101, the Department of Commerce adopted Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards at 2 C.F.R. Part 200, which apply to awards in this program. Refer to http://go.usa.gov/SBYh and http://go.usa.gov/SBg4.

   b. **Department of Commerce Financial Assistance Standard Terms and Conditions.** The Department of Commerce will apply the Financial Assistance Standard Terms and Conditions dated October 9, 2018, accessible here, to this award. The Department of Commerce Financial Assistance Standard Terms and conditions may be updated by the time of award, and those in effect at the time of award will be applied to awards made under this NOFO. Refer to Section VII. of this NOFO, Federal Awarding Agency Contacts, Grant Rules and Regulations, if you seek the information at this link and it is no longer working, or you need more information.

   c. **Pre-Award Notification Requirements.** The Department of Commerce will apply the Pre-Award Notification Requirements for Grants and Cooperative Agreements dated December 30, 2014 (79 FR 78390), accessible here. Refer to Section VII. of this NOFO, Federal Awarding Agency Contacts, Grant Rules and Regulations, if you seek the information at this link and it is no longer working, or you need more information.

   d. **Funding Availability and Limitation of Liability.** Funding for the program listed in this notice is contingent upon the availability of federal funding. Under no circumstances will NIST or the Department of Commerce be responsible for proposal preparation costs if these programs fail to receive funding or are cancelled because of agency priorities.

   e. **Publication** of this announcement does not oblige NIST or the Department of Commerce to award any specific project or to obligate any available funds.

   f. **Supporting Documentation.** Following the issuance of an award, NIST may require recipients to provide copies of sub-tier agreements, including subawards and contracts over $150,000, as well subrecipient performance monitoring plans.

3. **Reporting**

a. **Reporting Requirements.** The following reporting requirements described in Sections A.01 Reporting Requirements of the Department of Commerce Financial

Assistance Standard Terms and Conditions (October 9, 2018), apply to awards in this program (*See* Section VI.2.b. of this NOFO).

(1) Financial Reports. The recipient shall submit an SF-425, Federal Financial Report, into the MEP's Enterprise Information System (MEIS) on a semi-annual basis after the sixth and twelfth month of each operating year, unless other reporting intervals and/or due dates are identified by the NIST Grants Officer pursuant to a Special Award Condition. Reports will be due within 30 calendar days after the end of each semi-annual reporting period. The recipient shall submit a final SF-425 within 90 days after the expiration date of the award.

(2) Performance (Technical) Reports. The recipient shall submit a Technical Report (completing all required MEIS fields) on a semi-annual basis after the sixth and twelfth month of each operating year, unless other reporting intervals and/or due dates are identified by the NIST Grants Officer pursuant to a Special Award Condition. Reports are due in MEIS no later than 30 calendar days following the end of each reporting period. The recipient shall submit a final Technical/Quarterly report within 90 days after the expiration date of the award, and publication citation information as well as links to publicly available data shall be submitted as soon as they become available.

Technical/Quarterly Report details are accessible on the MEIS website (https://meis.nist.gov/). Technical progress reports shall contain information as prescribed in the HMEPP Reporting Guidelines (OMB Control Number 0693-0032). For further information regarding the HMEPP Reporting Process, you may download a copy of the HMEPP Reporting Guidelines at http://nist.gov/mep.

(3) Post Client Project Follow-Up. The recipient will be required to provide client and project data on a quarterly basis (unless otherwise directed by the NIST Grants Officer) and in a specified format to the organization identified by HMEPP for post-project follow-up data to be obtained (OMB Control Number 0693-0021). For further information regarding the HMEPP Reporting process, you may download a copy of the HMEPP Reporting Guidelines at https://www.nist.gov/mep/cybersecurity-defense-manufacturing

(4) Patent and Property Reports. From time to time, and in accordance with the Uniform Administrative Requirements set forth in 2 C.F.R. part 200 and in accordance with other terms and conditions governing the award, the recipient may be required to submit property and patent reports.

(5) Recipient Integrity and Performance Matters. In accordance with section 872 of Public Law 110-417 (as amended; *see* 41 U.S.C. 2313), if the total value of a recipient's currently active grants, cooperative agreements, and procurement contracts from all Federal awarding agencies exceeds $10,000,000 for any period of time during the period of performance of an award made under this NOFO, then the recipient shall be subject to the

requirements specified in Appendix XII to 2 C.F.R. Part 200, http://go.usa.gov/cTBwC, for maintaining the currency of information reported to SAM that is made available in FAPIIS about certain civil, criminal, or administrative proceedings involving the recipient.

b. Audit Requirements. 2 C.F.R. 200 Subpart F adopted by the Department of Commerce through 2 C.F.R. § 1327.101 requires any non-Federal entity (including non-profit institutions of higher education and other non-profit organizations) that expends Federal awards of $750,000 or more in the recipient's fiscal year to conduct a single or program-specific audit in accordance with the requirements set out in the Subpart. Applicants are reminded that NIST, the Department of Commerce Office of Inspector General, or another authorized Federal agency may conduct an audit of an award at any time.

c. Federal Funding Accountability and Transparency Act of 2006. In accordance with 2 C.F.R. Part 170, all recipients of a Federal award made on or after October 1, 2010, are required to comply with reporting requirements under the Federal Funding Accountability and Transparency Act of 2006 (Pub. L. No. 109-282). In general, all recipients are responsible for reporting sub-awards of $25,000 or more. In addition, recipients that meet certain criteria are responsible for reporting executive compensation. Applicants must ensure they have the necessary processes and systems in place to comply with the reporting requirements should they receive funding. Also see the Federal Register notice published September 14, 2010, at 75 FR 55663, available here.

VII. Federal Awarding Agency Contacts

Questions should be directed to the following contact persons;

Subject Area	Point of Contact
Administrative, budget, cost-sharing, eligibility questions and other programmatic questions.	J. Michael Simpson Phone: (240) 446- 7027 or Adelwiza Lequin Phone: (301) 646-4534 Fax: (301) 963-6556 E-mail: mepnofo@nist.gov
Technical Assistance with grants.gov	Leon Sampson Phone: (301) 975-3086 Fax: (301) 975-8884 E-mail: grants@nist.gov Grants.gov Phone: (800) 518-4726 E-mail: support@grants.gov

Grant Rules and Regulations	Gilberto Castillo Phone: (301) 975-3726 E-mail: gilberto.castillo@nist.gov

VIII. Other Information

1. **Frequently Asked Questions (FAQs).** Questions from potential applicants pertaining to NOFO eligibility, cost sharing requirements, evaluation criteria and selection factors, selection process, and the general characteristics of a competitive proposal will not be considered on an informal basis. Potential applicants must submit all such questions in writing to mepnofo@nist.gov. Answers to such written questions submitted to HMEPP may be made available to the public as part of an FAQ document, which will be periodically updated on the MEP website at https://www.nist.gov/mep/cybersecurity-defense-manufacturing.

2. **Protected and Proprietary Information.** The applicant acknowledges and understands that information and data contained in applications for financial assistance, as well as information and data contained in financial, performance and other reports submitted by applicants, may be used by the Department of Commerce in conducting reviews and evaluations of its financial assistance programs. For this purpose, applicant information and data may be accessed, reviewed, and evaluated by Department of Commerce employees, other federal employees, federal agents and contractors, and/or by non-federal personnel, all of whom enter into appropriate conflicts of interest and nondisclosure agreements covering the use of such information. As may be provided in the terms and conditions of a specific financial assistance award, applicants are expected to support program reviews and evaluations by submitting required financial and performance information and data in an accurate and timely manner, and by cooperating with Department of Commerce and external program evaluators. In accordance with 2 C.F.R. § 200.303(e), applicants are reminded that they must take reasonable measures to safeguard protected personally identifiable information and other confidential or sensitive personal or business information created or obtained in connection with a Department of Commerce financial assistance award.

   In addition, Department of Commerce regulations implementing the Freedom of Information Act (FOIA), 5 U.S.C. Sec. 552, are found at 15 C.F.R. Part 4, Public Information. These regulations set forth rules for the Department regarding making requested materials, information, and records publicly available under the FOIA. Applications submitted in response to this NOFO may be subject to requests for release under the Act. In the event that an application contains information or data that the applicant deems to be confidential commercial information that should be exempt from disclosure under FOIA, that information should be identified, bracketed, and marked as Privileged, Confidential,

Commercial, or Financial Information. In accordance with 15 CFR § 4.9, the Department of Commerce will protect from disclosure confidential business information contained in financial assistance applications and other documentation provided by applicants to the extent permitted by law.

3. **Recorded Information Session:** HMEPP will post one information recording for organizations that are considering applying for or participating as a team member in this funding opportunity. The posted recording will provide general information regarding HMEPP and this funding opportunity and offer general guidance on preparing proposals. The recording will provide information about potential participants, eligibility, evaluation criteria and selection factors, the selection process, program priorities and objectives, and the general characteristics of a competitive proposal during the webinar(s). A link to the recording will be provided at https://www.nist.gov/mep/cybersecurity-defense-manufacturing.