Here is the text version of the webinar, "Clean Energy Manufacturing Innovation Institute: Cybersecurity in Energy Efficient Manufacturing FOA," presented on April 16, 2019.

Hello, everyone and welcome to our Funding Opportunity Announcement, or FOA, webinar. Thank you for your interest in the U.S. Department of Energy's efforts on renewable energy and energy efficiency. My name is Chad Schell, and I am a Technology Manager in the Advanced Manufacturing Office within the DOE's Office of Energy Efficiency and Renewable Energy, which I will refer to as EERE.

Before we begin, I'd like to draw your attention to the email address on the left hand side of this cover page. This is the official mailbox to direct all of your questions during the entire FOA process, or to send information to be added to the Teaming Partner list, which we will maintain for this FOA to facilitate the formation of project teams. More information about what details to include when requesting to be added to the Teaming Partner list will be covered later in this webinar. Please do not contact EERE individuals directly with questions, including myself. All questions received at this mailbox are posted publicly at the Q&A section of the FOA page on EERE Exchange in an anonymous way. Please be careful not to submit any language that might be business sensitive, proprietary or confidential. The official answers to your questions will typically be posted on Exchange within 3 business days.

If you have questions during this webinar, you can send them to the email address on this slide and we'll post the answers on EERE Exchange. Alternately, you can type in your questions in the chat field as they come up. Again, please be careful not to submit any language that might be business sensitive, proprietary or confidential. We will be posting all Q&As to EERE Exchange after the webinar. We will not be answering any questions real time today. Please check EERE Exchange in the next few days as the answer will be posted there.

DOE's Office of Energy Efficiency and Renewable Energy - EERE - and Office of Cybersecurity, Energy Security and Emergency Response - also called CESER - are partnering on this effort to best leverage the capabilities of our offices. Within EERE, the Advanced Manufacturing Office will lead the effort.

The AMO is the only technology development office within the U.S. Government that is dedicated to improving the energy and material efficiency, productivity, and competitiveness of manufacturers across the industrial sector.

AMO's vision is to provide U.S. global leadership in sustainable and efficient manufacturing for a growing and competitive economy.

AMO's mission is to catalyze research, development, and adoption of energy-related advanced manufacturing technologies and practices to drive U.S. economic competitiveness and energy productivity.

Organizationally, AMO pursues its goals through the following three subprogram approaches:

First, there is R&D projects for bridging the innovation gap. The Advanced Manufacturing R&D Projects subprogram supports innovative advanced manufacturing applied R&D projects that focus on specific high-impact manufacturing technology and process challenges. The subprogram invests in foundational energy-related advanced manufacturing technologies that impact areas relevant to manufacturing processes and broadly applicable platform technologies.

Second is R&D Consortia focusing on a Public-Private consortia model. The Advanced Manufacturing R&D Consortia subprogram helps the United States position itself as a world leader in strategic areas of manufacturing by bringing together manufacturers, suppliers, companies, institutions of higher education, national laboratories, and state and local governments in public-private R&D consortia. These partnerships create an innovation ecosystem that accelerates technology development and facilitates the transition of innovative advanced manufacturing technologies to the industry.

The final subprogram is Technical Partnerships for bringing direct engagement with Industry. The Technical Partnerships subprogram provides critical support to the adoption of advanced energy efficiency technologies and practices. The subprogram supports the adoption of cost-effective combined heat and power technologies; provides resources to assist manufacturers in reducing their energy use intensity; promotes the adoption of energy management programs, provides targeted energy efficiency, productivity, and waste/water use reduction practices to small- and medium-sized manufacturers.

As I previously mentioned, the AMO is partnering with the CESER office.

The Office of Cybersecurity, Energy Security, and Emergency Response - or CESER - leads DOE's efforts to secure our Nation's energy infrastructure against all hazards, reduce the risks of and impacts from cyber and other disruptive events, and assist with restoration activities.

CESER's priorities are aligned with the Administration's National Cyber Strategy, and are informed by DOE's Multiyear Plan for Energy Sector Cybersecurity. These priorities include:

- Strengthening energy sector cybersecurity preparedness

- Accelerating the research, development, and demonstration of resilient energy delivery systems

- Coordinating cyber incident response and recovery by working closely with local, state, and Federal agency partners, as well as industry partners.

For more information, go to the CESER website listed here at energy.gov.

Just to be clear, today's webinar participation provides no particular advantages or disadvantages to the application evaluation process. Participation in the webinar is completely voluntary.

All applicants are strongly encouraged to read the Funding Opportunity Announcement in its entirety and to adhere to the submission requirements stated in the FOA.

Today's presentation is a summary of the FOA contents. If any inconsistencies arise in the presentation or with statements sent to you from DOE today, applicants should rely on the language in the FOA document and seek clarification through the FOA mailbox.

Here is the anticipated FOA schedule. It is imperative to note that an applicant must submit a Concept Paper by 5pm Eastern May 15, 2019 deadline in order to be eligible to submit a Full Application. Full applications will be due August 20, 2019.

So today we are going to go over the FOA Description, the FOA Topic Areas, associated Award Information, Statement of Substantial Involvement for work performed under awards resulting from the FOA, Cost Sharing requirements, Timelines of activities and deadlines for the FOA, we'll discuss the Concept Papers, talk about the Full Applications, outline the Merit Review and Selection Process to be

used, explain the purpose and form of the pre-selection interviews, and go over the Registration Requirements in order to apply.

This FOA intends to establish a new Clean Energy Manufacturing Innovation Institute that is dedicated to advancing cybersecurity in energy efficient manufacturing. We'll later discuss what it means to be an "Institute" in this context.

As noted previously, DOE's EERE and CESER offices are partnering on this effort to best leverage our respective capabilities.

The Institute will not only pursue R&D targeted on understanding the evolving cybersecurity threats to greater energy efficiency in manufacturing technologies and industries, but also the development of new technologies and methods to combat these threats while sharing information and knowledge to the broader U.S. manufacturing community.

It's important that the Institute leverage expertise from a wide array of public and private organizations, ranging from industry, academia and government institutions.

This Institute is expected to achieve some specific outcomes.

- The first goal is enabling greater manufacturing energy efficiency through cyber-secure process controls.

- The Institute will lead a national consortium in early-stage applied R&D around low-cost technologies and methods to reduce risk and improve cybersecurity preparedness, response, and recovery.

- A third outcome is to establish and support a shared R&D infrastructure around the understanding and implementation of mitigations for cybersecurity vulnerabilities and risk specific to manufacturing.

- The Institute will also work towards increasing awareness and implementation of cybersecurity best practices for a more efficient manufacturing sector.

- The Institute must become financially self-sustaining and a world-leading innovation center, bringing together public and private entities to invest in R&D that promotes security and economic resilience of U.S. manufacturing.

- Last, the Institute will address the technical education and workforce development needed to manage and implement cyber-secure approaches in manufacturing.

Manufacturing in the U.S. consumes a significant amount of energy- approximately 25% of all that is consumed in the country. Energy efficiency gains in the manufacturing sector can greatly reduce our national energy use AND increase the competitiveness of U.S. manufacturing in the global economy.

Implementation of advanced automation and control systems can have significant impact on energy efficiency in all manufacturing sectors, including semiconductors, and energy intensive industries for transportation equipment, petroleum refining, iron or steel, forest products, agriculture and food, cement, and particularly the clean energy sector.

Automation, advanced control systems, and increased use of advanced sensors and controls increase the connectivity points which increases the cyber vulnerabilities of the manufacturing process and supply chain.

Sharing information on cyber issues in a timely manner is key to defend against cyber risks. Information sharing is critical with Coordinated Vulnerability Disclosures as one key approach to sharing information.

New technologies cannot be deployed successfully without a trained workforce to design and implement the technologies.

DOE identified 2 challenge areas in manufacturing where the Institute can address resilience against cyberattacks and global competitiveness in U.S. manufacturing:

1. Securing Automation and 2. Securing the Supply Chain Network.

Moving on to discuss the 2 challenge areas in more detail, first up is Securing Automation. In order to realize the benefits from automating manufacturing processes, the cyber risks introduced must be mitigated. Some of the challenges DOE identified in this area include: monitoring machines for threats and connectivity, controls for risk identification and migration, streamlining specific manufacturing processes with actionable intelligence and intrusion alerts, security screening for parts or components qualification, and developing next-generation control systems and interfaces that are secure and openly available without licensing and other barriers.

To address those challenges in automation, the FOA outlines the innovation areas that the Institute should address. This includes: vulnerabilities in automated process control systems for equipment, tools, and components; securing communication for smart and digital manufacturing; computing architectures and hardware designed and built with a cybersecurity focus from the ground up; approaches to identify, alert, and mitigate cybersecurity threats, enabling greater energy efficiency; and improving the safety and security of manufacturing industry through Consolidated Vulnerability Disclosure activities.

The second area identified by DOE is Securing the Supply Chain. A major challenge for the manufacturing sector is the need for improving resiliency of the supply chain network against emerging cyber-threats while balancing demand, consumption of resources, and production of goods. The challenges that DOE outlines in the FOA are: verifying/validating materials and components for counterfeit or off-specification materials, strategies to physically track and prevent tampering for components and inventories, suppliers and customers at all levels communicating securing and efficiently, protection of data and IP from theft, integration of systems of varying age, sophistication, and architecture, and finally the difficulty in analyzing and modeling such diverse systems, equipment and processes.

In the area of Securing the Supply Chain, the FOA outlines the following innovation areas: security that enables an on-demand, dynamic, energy-aware, and cost effective supply chain network; standardization of security protocols, architectures and networking in such a way to promote greater energy efficiency; autonomy of process controls with secure asset and energy management; real-time prescriptive data analytics for reducing and mitigating threats; and security innovations that increase the supply chain network efficiency.

To achieve innovations in Securing Automation and Securing the Supply Chain Network for energy efficient manufacturing, the Manufacturing Innovation Institutes model was chosen for the unique characteristics of these institutes.

Manufacturing Innovation Institutes are designed to bring together industry, academia, state and local governments, NGOs, non-profits and national laboratories, to:

- Accelerate manufacturing innovation by investing in industry-relevant, cross-cutting product and process technologies;

- Provide education and training opportunities to build and enhance the skills of the American manufacturing workforce; and

- Transition to a privately funded model approximately 5 years after launch (which is also referred to as "self-sustaining").

Each Institute is expected to:

- Foster an open exchange of pre-competitive manufacturing best-practices and know-how;

- Protect intellectual property;

- Allow manufacturers of all sizes access to use and share the R&D infrastructure for research, development, validation, and verification;

- Provide the opportunity for its members to improve their own technologies by learning from other members;

- Engage the manufacturing community at all levels of the supply chain network, from technology developers to implementers to users, including industry, academia, state and local governments, NGOs, non-profits, national laboratories, and FFRDCs to transition relevant advanced manufacturing technologies to commercial applications;

- Focus on problems relevant to manufacturing;

- Engage with the broader community by hosting research internships and developmental assignments for individuals from industry, academia, and government to accelerate pre-competitive development of advanced manufacturing technologies;

- Support educational, and workforce development of the energy efficient manufacturing community around the Institute and the associated new technologies developed and implemented;

- Have a strong management team and a strong organizational director; and

- Have a clearly defined governance structure, and well-defined operational plan to enable efficient operations that demonstrate value to Institute stakeholders.

The efforts of the Institute should provide significant impacts in developing technology that will improve the energy efficiency and cybersecurity of U.S. manufacturing. The Institute will need to use the developed Roadmap, described in Section I.B.iv of the FOA, Development of a Roadmap, to prioritize work. The Roadmap will outline the relevant activities to achieve the cybersecurity goals.

Technology development and education and workforce development efforts must be targeted towards the following performance metrics:

- Development of technologies that result in energy efficiency gains of 15% or more in manufacturing processes through secure process automation. The applicant should validate and verify how the process is more secure than existing state-of-the-art approaches. Solutions in energy intensive industries or manufacturing processes with renewable and clean energy product outputs should be prioritized;

- Improvement of 50% or more in energy efficiency or speed (at equal energy efficiency) of specified cybersecurity solutions (and the total energy savings as a result);

- Quantified prevention of, or mitigation of, negative cybersecurity impact on manufacturing assets and output quality;

- Percentage improvements in mean time-to-detect as well as time-to-recover from cyber-attacks. The applicant should specify which industry and/or systems type, and provide a baseline mean time-to-detect and/or mean time-to-recover. Recovery success measures should be defined and justified by the applicant to be relevant to the specific industry;

- Reduction of 10% or more in a specific supply chain network activity energy use realized through cybersecurity technologies developed under this funding opportunity;

- Number of coordinated vulnerability disclosures by U.S. based manufacturers, including the number of solutions developed based on CVD actions. Applicants should explain how they will show that Institute actions link to measured CVDs;

- Number of trained workforce at educational institutions and for industry;

- Number of certified coursework/curriculums developed;

- And finally, be financially self-sustaining at the end of the 5 year federal award project period. Self-sustaining must be a transition to a privately funded model, not relying on federal funding.

We'll now discuss "a more detailed description of the Institute's topic areas and the activities the Institute is expected to complete."

Both topic areas, Securing Automation and Securing the Supply Chain Network, must be addressed in your application.

DOE intends to select and fund only one award under this FOA.

A portfolio of activities that makes progress in both topic areas must be proposed in the work plan.

Education and workforce development must be addressed in the work plan for <u>both</u> topic areas.

Applicants can propose additional activities beyond those outlined in the FOA. However, applicants must show how those activities are justified and relevant to the Institute and its goals.

It is important to note that all work under this Institute must be performed in the United States, unless approved by DOE under the waiver process described in the FOA.

For securing automation, the R&D efforts will focus on improving security measures needed for integrating hardware and software systems that improve automation and efficiency in manufacturing, as well as developing automated diagnostics for manufacturing systems. Improving security of all manufacturing processes will also allow manufacturers to improve productivity, flexibility and connectivity. Control interfaces for manufacturing equipment, tools, or components is another area the Institute must address. In addition to other critical areas identified by applicants, the Institute must focus on:

- Developing advanced sensors for manufacturing process monitoring and control – Work here should address design and implementation of physical and software approaches to assess and ensure the security of these sensors.

- Second, developing countermeasures to emerging technologies being leveraged by adversaries across all sectors – These countermeasures can include both hardware and software solutions. Countermeasures considered should include not only control interfaces but also architectures, control systems, and other communication interfaces.

- And third, designing and developing advanced manufacturing technologies that include robust cybersecurity from the ground up – These advanced manufacturing technologies can be widely applicable or specific to an industry or process.

The need to secure automation spans securing the communication interfaces between equipment to enabling faster and more secure data transfer and analysis across plant locations and companies. Industry-driven open reference architectures, standards and protocols for various control systems are important for enabling the next generation of cyber-secure manufacturing systems. Architectures and hardware design focused on and customized for cybersecurity are additional areas crucial to hardware and software integration for manufacturing automation. The goal of R&D efforts will be to avert cyber-attacks on industrial equipment, tools, and materials, including networked systems.

In addition to other critical areas identified by applicants, the Institute must focus on:

- Developing security solutions for digital control systems that lead to greater energy efficiency – This work can include design, modeling and prototyping. Applicants are encouraged to consider Supervisory Control and Data Acquisition (SCADA) and open source control interfaces, for manufacturing equipment, tools, and materials.

- Improving the security of advanced analytics based on industry driven open reference architectures, standards and protocols – Advanced analytics enable automated and advanced manufacturing. Open source/reference approach is required to ensure widespread availability and applicability.

- Designing and implementing new secure control systems and integration of related hardware and software – This work can include prototyping or be limited to design and implementation plans. Such systems and integration can be process/industry specific or more widely applicable.

- Developing an industry driven cybersecurity and resiliency framework for network-centric manufacturing – Applicants should focus on a standard framework that can be as widely applicable as possible.

- And finally, developing and implementing data privacy, encryption and standards for manufacturing process planning and information exchange – Work in this area must consider existing guidance and standards as well as industry wide input.

It is impossible to identify and eliminate all possible cybersecurity vulnerabilities when developing new energy efficient technologies. Identifying, alerting, and mitigating when cyber intrusions occur are thus instrumental in manufacturing resiliency and should be considered in any design and implementation approaches considered under all focus areas of automation. Additionally, improving abilities for third parties to work with manufacturers on detecting and disclosing information on vulnerabilities is essential. Institute efforts must include fostering increased and improved CVD activities through the development of guidelines, best practices, and more direct engagements. In addition to other critical areas identified by applicants, the Institute must focus on:

- Automation related threat identification, alerts and mitigation – This work should consider approaches that identify threats and intrusions as well as strategies for industry to mitigate problems.

- Knowledge bases focused on cyber vulnerabilities and detection of intrusions to common manufacturing systems – Such knowledge bases must consider effective documentation and communication as well as strategies to protect non-public information while balancing information sharing with U.S. manufacturers.

- Advanced behavioral anomaly detection for designing and manufacturing – Applicants should propose general detection strategies or innovation for specific processes/industries. Work could include designing and modeling as well as actual prototyping and testing.

- CVD guidelines, standards and education must be developed, at a minimum – Implementation and piloting of an industry-wide CVD program can also be considered. Any CVD program must include a process for documenting disclosures, reporting the disclosures to DOE, and a plan to share information with targeted organizations where appropriate.

Next, the Securing Supply Chain Networks topic. R&D must consider all aspects of the manufacturing supply chain network –including those that span across multiple supplier tiers – for equipment, tools, and materials. Recent advances in modeling and simulation, machine learning, and Artificial Intelligence can be leveraged to improve energy efficiency and performance across entire supply chain networks by reducing the risks and consequences of cyber threats. Supply chain security work proposed must allow for agile on-demand, dynamic, energy-aware and cost-effective ecosystems. Work must address autonomy for manufacturing systems with secure asset and energy management. In addition to other critical areas identified by applicants, the Institute must focus on:

- Integrating cybersecurity with energy and equipment management – Proposed work in this area can consider the hardware and software solutions required for energy and equipment management in the supply chain network.

- The Institute also must focus on, improving equipment maintenance through secure status monitoring – Work can focus on hardware or software strategies for status monitoring that enables robust equipment maintenance. Such strategies should include the ultimate benefits of the maintenance in increasing efficiency and/or reducing cost.

- And third. Securing manufacturing asset management tools across the supply network (including, but not limited to, between original equipment manufacturers and Tier1 and Tier 2 suppliers) – Applicants should propose hardware and software strategies that overcome the differences in systems traditionally experienced in the supply network.

The Institute's focus must include enabling a vibrant and comprehensively secure supply network that consists of large, small and medium enterprises distributed across the U.S. The Institute must also focus on supporting efforts to identify, fix, and raise awareness of cyber-vulnerabilities across supply chain networks. Software, vulnerability detection and mitigation activities must include standards, CVD, and other activities. Additionally, the Institute must address the standardization of security protocols, architectures, and networking infrastructure as appropriate to overcome the barrier of these historically incongruent systems. Real-time data analytics in the supply chain network for security threat discovery, detection, disclosure, and mitigation must be addressed. Innovation in the security requirements of efficiency in the supply chain network must also be considered. In addition to other critical areas identified by applicants, the Institute must focus on:

- Enabling secure energy efficient manufacturing services and maintenance across the supply network – Securely implementing emerging approaches and theories on supply chain network-wide servicing and maintenance that consider the entire supply network should be addressed;

- Developing and implementing approaches for testing the cybersecurity framework to address the supply network risks and resiliency – SCADA and ICS should be prioritized. Work on SCADA should take into consideration DOE's 21 Steps to Improve Cyber Security of SCADA Networks;

- And simulating and testing strategies should be developed and piloted to manage cybersecurity updates and maintenance, to minimize their negative impacts on productivity and profitability;

- And finally, creating shared research facilities focused on supply chain network cyber vulnerabilities discovery, detection, disclosure, and mitigation – Proposed facilities can be physical or virtual, but should emphasize inclusion and accessibility for the widest range of participants possible.

Educational Workforce Development is vital to address the shortage of cybersecurity practitioners and skills gap in the existing workforce. Both topic areas must focus on innovative methods for workforce training, certification, apprenticeship, student curriculums and other learning programs to address the skills and knowledge gap in deploying the new technologies developed under the Institute. EWD must be considered alongside the technical efforts and could address:

-Training in new technologies of cybersecurity for energy efficient manufacturing through certification, apprenticeship and lifelong learning programs;

-Curriculum development on best practices with new technologies for cybersecurity in energy efficient manufacturing;

-Curriculum development emphasizing design for secure manufacturing and supply chain network; and

-New learning programs and accessible learning facilities on secure and efficient manufacturing.

The applicant will identify R&D, modeling, and analysis activities which will be further informed by the Institute's road mapping activities that will be undertaken during the Institute's first year, to identify and prioritize the highest impact areas from early-stage to applied R&D for a range of technology options.

Applicants must include their vision for the development of a Roadmap including how the applicant has the subject matter expertise, resources, and facility capabilities to address the technical challenges and opportunities in the two topic areas.

As an outcome of road mapping, the Institute will identify specific R&D, modeling and analysis activities and technical targets that align with the Roadmap priorities that would be negotiated with DOE into Budget Periods 2-5.

The Institute will develop a consistent process to compete and select projects (e.g., Request for Proposal). Note that the projects selected under that process are subject to DOE approval and the process must reflect that requirement.

The Institute's scope and budget are subject to change after each budget period based on year-to-year progress of the Institute's activities and project portfolio as well as ongoing alignment of the Institute's capabilities and expertise to the Roadmap priorities.

The recipient must work closely with its members and DOE to establish and operate a coordinated Institute. The Institute must have a clearly defined governance structure and a written set of Institute policies.

The governance documents should identify any boards, committees, or groups that comprise the Institute, and describe how they will be structured and operate, including the applicable voting rights. As part of the Technical Volume, the applicant must describe its proposed governance structure. If selected for award, the governing documents (e.g., bylaws) and Institute policies must be in place before an award is issued.

Each member of the Institute must enter into a membership agreement that sets forth the terms and conditions of the membership, and by which the members agree to be subject to the governance structure and the Institute policies. As part of the Full Application, each applicant must submit a draft membership agreement.

If selected for award, the membership agreement must be final before an award is issued.

All work under EERE funding agreements must be performed in the United States.

At a minimum, the applicant is expected to propose work to address the primary focus of the Institute within the topic areas, including EWD in both topic areas.

Applicants may propose to address additional application areas and other cybersecurity issues in manufacturing but must justify the benefit of this additional work along a pathway towards achieving the goals of this FOA.

The applicant must identify clear milestones and how the Institute will demonstrate progress towards the defined targets for the award project period at regular intervals. Additionally, the applicant must show a path to achieve the long term goals identified post award project period.

All milestones and targets must be supported by credible analysis that is updated throughout the award.

And for any and all proposed application areas, it is strongly encouraged to have end users and/or OEMs from the relevant industries included in the Institute, demonstrating market pull and technical relevance for subsequent technology transfer and commercial adoption.

The Institute leadership team must be primarily focused on the operation and management of the proposed Institute. The Institute Chief Executive Officer must be a full time position and other key personnel are expected to provide at least a 75% time commitment to the Institute, with a 100% time commitment recommended during the Budget Period 1 start-up phase.

Before DOE can issue an award under this FOA, a number of documents related to the Institute's governance and management must be completed. These documents are subject to DOE review and approval. Please note that because these activities are required prior to the issuance of an award and are not part of the activities performed under the award, the costs associated with these activities are not allowable for reimbursement or allowable as cost share.

The documents that must be completed and in place prior to DOE issuing an award include:

- U.S. Manufacturing Plan;

- Data Management Plan;

- Conflict of Interest disclosure statement;

- Institute Conflict of Interest Plan that defines a consistent approach to identifying and mitigating COIs across the Institute;

- Governance documents;

- Membership Agreement;

- Cybersecurity Plan;

- Foreign Entity Participation Plan;

- IP Management Plan;

- Non-disclosure agreement that the Institute members must all agree to;

- Export Control Management Plan for the Institute;

- Conference Management Directive; and

- Operations Plan to include project management plan, risk management plan, and project selection plan.

The first budget period is expected to be 12 months in duration.

During this first 12 month period, start up and Roadmapping activities must be completed. Specific items required include:

- Working closely with DOE to create and develop a Roadmap with prioritized R&D activities;

- Developing technology and project-level baselines, performance metrics, and technical targets, to define and achieve goals that will be used across the Institute;

- Develop and execute a competitive Request for Proposals process to solicit and add new projects that support the Roadmap priorities;

- Map specific projects into the Roadmap;

- Develop an execution plan for activities to support CVDs in the manufacturing sector;

- Identify approaches that integrate across Roadmap areas and develop a plan for implementation across the Institute; and

- Develop a continuation package with DOE for incorporating specific projects' scopes of work and budgets into the award for Budget Period 2.

During Budget Periods 2-5, the Institute will work in a collaborative manner on R&D priorities defined by the Roadmap and provide progress updates to DOE and stakeholders.

Updates to the Roadmap must be done based on Institute activities. DOE will be involved in these updates. The Institute will provide data to update the Roadmap, based on the outcomes of its activities.

The Institute will provide a detailed outline and budget estimate for the R&D, modeling, and/or analysis activities for the remainder of the project period. It is important to note, the Institute's scope and budget are subject to change after each budget period based on year-to-year progress of the activities and project portfolio as well as ongoing alignment of the capabilities and expertise to the Roadmap priorities.

The Roadmap and all supporting analysis conducted must track technological progress and inform how the Institute is performing against the technical baseline. The Roadmap must track technological progress to targets, and performance metrics identified in this FOA to achieve the outlined Institute goals. These baseline targets and metrics are expected to be further developed and refined during roadmapping activities.

DOE will use this information to assess how the Institute should adjust R&D priorities. See the FOA Go/No-Go Review for more information.

The DOE and Institute will work together to maintain a single Roadmap for the Institute as progress is made and various aspects evolve. The Institute must align and map R&D, modeling, and analysis activities and projects into the Roadmap.

To facilitate the formation of new project teams for this FOA, a Teaming Partner List is available at the website listed on this slide.

We'll update the Teaming Partner List periodically to reflect new Teaming Partners who have provided their information.

Any organization that would like to be included on this list should submit the information shown on this slide to the email address provided. Keep in mind, though that by submitting this information, you consent to the publication of that information.

Please also note that by facilitating this Teaming Partner List, EERE does not endorse or otherwise evaluate the qualifications of the entities that self-identify themselves for placement on the Teaming Partner List.

In addition, EERE will not pay for the provision of any information, nor will it compensate any respondents for the development of such information on this list.

The following types of applications will be deemed nonresponsive and will not be reviewed or considered for an award:

- Applications that fall outside the technical parameters specified in Section I.A or I.B of the FOA

- Applications for proposed technologies that are not based on sound scientific principles

- Applications that are outside Technology Readiness Levels 2 - 6

- And applications that only propose a single R&D project

EERE expects to make a total of approximately $70,000,000 of federal funding available for one new five year award under this FOA subject to the availability of appropriated funds.

EERE will establish up to 5 budget periods for the award, however only funding for Budget Period 1 will be authorized initially. Budget Period 1 will have a duration of approximately 12 months of the overall project period.

A total of up to $14,000,000 in federal funds is anticipated to be available for the award for each budget period, however early budget periods, especially Budget Period 1, are anticipated to be funded at lower than $14,000,000 with funding allocations increasing as project activities increase. Funding for Budget Periods 2-5 are not guaranteed.

EERE intends to fund a cooperative agreement or a funding agreement with an FFRDC under this FOA. Cooperative Agreements include Substantial Involvement, which we will discuss next.

- Under cooperative agreements, there will be what is known as “substantial involvement” between DOE and the Recipient during the performance of the project.

- DOE does not limit its involvement to administrative requirements and will have substantial involvement in the direction and redirection of the technical aspects of the Institute.

- Substantial involvement includes, but is not limited to, the following:

-- Shared responsibility for the management, control, direction, and performance of the Project.

-- DOE may interrupt or modify the conduct or performance of activities for programmatic reasons.

-- DOE may redirect or discontinue funding project wide at go/no go decision points.

-- DOE may redirect or discontinue funding for individual activities at go/no go decision points.

-- DOE participates in major project decision-making processes to include but not limited to:

--- Completion of Roadmap

--- Selection of the Institute Activities;

--- Individual Institute Activity Go/No-Go reviews; and

--- Project redirection based on progress reviews.

For cost sharing requirements: The cost share must be at least 20% of the total allowable costs for research and development projects and must come from non-federal sources unless otherwise allowed by law.

Please see Appendix A to this FOA for a cost share information sheet and sample cost share calculation.

The total budget presented in the application must include both Federal and Non-Federal portions. All costs must be verifiable from the Recipient's records and be necessary and reasonable for the accomplishment of the project.

Cost share must be approved in advance by the Contracting Officer.

It is important to note that vendors and contractors may not provide cost share. Additionally, partial donations of goods and services are considered a discount which is not an allowable form of cost share as well.

Cost Share must be allowable and must be verifiable upon submission of the Full Application. Please refer to this chart for your entity's applicable cost principles. It is imperative that you follow the applicable cost principles when creating your budget for the full application.

Cost share can provided in cash and/or in-kind. Cost share can be provided by the Prime Recipient, sub recipients, or a third party.

Cash contributions include, but are not limited to: personnel costs, fringe costs, supply and equipment costs, indirect costs and other direct costs.

In-kind contributions are those where a value of the contribution can be readily determined, verified and justified but where no actual cash is transacted in securing the good or service comprising the contribution. Allowable in-kind contributions include, but are not limited to: the donation of volunteer time or the donation of space or use of equipment.

Be aware that there are items that are considered unallowable cost share. If a cost is considered unallowable, it cannot be counted as cost share. Some examples of cost share that is unallowable, include:

- Revenues or royalties from operations after the project period

- Proceeds from the sale of an asset

- Federal funding and property

- Expenditures already reimbursed under another Federal Office

- Cash or in-kind contributions counted on other programs or projects

- Vendor and contractor contributions

- And it is important to note that program income, including membership fees, earned during the period of performance may not be used to meet recipient cost share.

Documentation is required for cost share contributions.

Cost Share must be provided on an invoice basis, unless a waiver is requested and approved by the Contracting Officer.

EERE's Evaluation and Selection Process is shown here in blue. EERE will review Concept Papers, Replies to Reviewer Comments - which we will cover later in the presentation, and Full Applications. The green boxes represent the actions that apply to applicants throughout the FOA process. The Institute award is anticipated by March of 2020.

Concept Papers are required for this FOA. Concept Papers are brief descriptions of the proposed project. It allows applicants to submit their ideas with minimal time and expense. EERE will provide feedback to the proposed project so the Applicant can make an informed decision whether to expend additional resources to prepare a full application.

If an applicant fails to submit an eligible Concept Paper, the applicant is not eligible to submit a Full Application.

Concept Papers must be submitted by May 15, 2019, 5:00 PM Eastern, through EERE Exchange.

EERE will provide applicants with either an encouraged or discouraged notification. A "discouraged" notification conveys EERE's lack of programmatic interest in the proposed project. An applicant who receives a "discouraged" notification may still submit a Full Application, however.

EERE will provide applicants with (1) either an "encouraged" …

Concept Papers are evaluated based on consideration of the following factors. All sub-criteria are of equal weight.

Criterion 1: Technical Description, Innovation and Impact - 50%

- This criterion involves consideration of the following factors:

- Quality of the proposed integrated cybersecurity in energy efficient manufacturing technical approach;

- The proposed topic areas are well-defined and have well-defined, aggressive quantitative technical objectives and metrics for success;

- The applicant's understanding of the current state-of-the-art in the field of cybersecurity in energy efficient manufacturing, including key opportunities and challenges;

- Extent to which the applicant has described how the proposed technical work will overcome the challenges identified;

- The estimated energy and competitiveness impact that the proposed Institute would have on cybersecurity and energy efficient manufacturing;

- Quality of the approach presented in the technical education and workforce development plan summary; and

- Quality of the approach to strengthen U.S. manufacturing competitiveness while engaging a broad range of stakeholders with both horizontal and vertical reach across and within supply chain networks.

Criterion 2 for Concept Paper Review: Team and Resources is 25%

This criterion involves consideration of the following factors:

- Extent to which the roles and responsibilities of the leadership team are well-defined;

- Whether the Principal Investigator - Institute Director/Executive - and Project Team have the skill, expertise and prior experience needed to successfully execute the Institute; and

- Whether the applicant has adequate access to equipment and facilities necessary to accomplish the effort and/or clearly explains how the proposed Institute intends to obtain access to the necessary equipment and facilities.

The third Criterion for the Concept Paper Review: Operations and Management Approach Description, which is also 25%

This criterion involves consideration of the following factor:

- The proposed management and operations structure and approach, including the role of the U.S. government in the management of the proposed Institute.

A complete full application must include all of the items on this slide. Only omit those items that truly do not apply to your application. For example, if all project participants are US entities and all work will occur in the United States, then a Foreign Entity and Foreign Work waiver is not needed.

The key technical component of the full application is the Technical Volume, which helps applicants frame the technical information that the application will be evaluated on. The Technical Volume provides information regarding what the project is, how the project tasks will be accomplished, and the project timetable.

The Technical Volume is comprised of a cover page; Institute overview; technical description, innovation, and impact section; qualifications and resources; and operations and management approach. Please note that the percentages listed here are suggested and are not mandatory.

The FOA document outlines the requirements for each of these sections.

As we previously pointed out, applicants must submit full applications by August 20, 2019.

EERE will conduct an eligibility review, and full application will be deemed eligible if:

- The Applicant is an eligible entity;

- The Applicant submitted an eligible Concept Paper;

- The Cost Share requirement is satisfied;

- The Full Application meets the compliance criteria;

- The proposed project meets the responsiveness criteria;

- The Applicant is compliant with the limitation on Number of Concept Papers and Full Applications eligible for review; and finally

- The Full Application meets any other eligibility requirements listed in Section III of the FOA.

Eligible applicants for this FOA include:

- U.S. citizens and lawful U.S. permanent residents

- For-profit entities

- Educational institutions

- Nonprofits

- State, local, and tribal government entities

- and DOE/NNSA FFRDCs

Please note the eligibility limitations on nonprofit organizations that engaged in lobbying activities.

It is also important to note that all Prime Recipients receiving funding under this FOA must be incorporated and have a physical location for business operations in the United States.

An entity may only submit one Concept Paper and one Full Application for consideration under this FOA. For example, EERE will only consider one Concept Paper and one Full Application per university for this FOA (not one submission per each college or school under the university). If an entity submits more than one Concept Paper and Full Application, EERE will request a determination from the applicant's authorizing representative as to which application should be reviewed. Any other submissions received listing the same entity as the applicant will not be eligible for further consideration. This limitation does not prohibit an applicant from collaborating on other applications (e.g., as a potential subrecipient or partner) so long as the entity is only listed as the applicant on one Concept Paper and Full Application submitted under this FOA.

The Merit review process includes an eligibility review and thorough technical review.

Subject matter experts will conduct rigorous technical reviews.

The Selection Official will consider the reviewer recommendations and other considerations such as program policy factors in the selection decision.

Full Applications will be evaluated against the following merit review criteria:

Criterion 1: Technical Merit, Innovation and Impact - 50%:

Technical Merit and Innovation

- Quality of the integrated technical approach, including core competencies identified for the proposed Institute to research, develop and demonstrate innovative cybersecurity for energy efficient manufacturing technologies that meet the goals and the objectives of the Institute in Section I.B. and those proposed by the applicant;

- Degree to which the applicant has defined and justified the proposed topic areas building upon those identified in Section I.B. of this FOA, and has clearly defined Institute objectives, goals, and performance metrics including aggressive technical targets to achieve the goals of the FOA;

- Extent to which the applicant demonstrates a strong understanding of the state of the art, and the sufficiency of technical detail in the application to assess whether the proposed technical work as described in the Technical Volume and the SOPO is scientifically meritorious, feasible and innovative, to achieve greater energy efficiency, technical targets, goals and objectives of the Institute; and

- Quality of the technical education and workforce development plan to integrate and support technical education and career training into the Institute ecosystem, and leverage existing resources.

Further on Criterion 1: Technical Merit, Innovation and Impact - 50%:

Statement of Project Objectives

- Adequacy, appropriateness, and reasonableness of the proposed work and schedule overall and allocation among the team members to accomplish the stated objectives;

- Relative to a clearly defined baseline, the strength of the quantifiable metrics, milestones, Go/No-Go decision points, and a mid-point deliverables defined in the application, such that meaningful interim progress will be made; and

- The quality of the SOPO for the first two budget periods (Budget Period 1 and Budget Period 2) that describes the initial startup phase for the Institute and the initial technology development activities, as well as the overall plan for the full award project period.

Continuing on Criterion 1:

Impact

- The quality of the market transformation plan for the initial proposed projects and technical work and the extent to which the applicant demonstrates the likelihood of successful technology adoption by industry, and supports energy efficient manufacturing technology development;

- Extent to which the applicant demonstrates a high and credible impact of the Institute for cybersecurity protection over ten years relative to existing available energy efficiency technologies;

- Extent to which the applicant demonstrates the potential impact of the Institute to support security and resiliency of U.S manufacturing and supply chain networks against cyber threats, such as greater energy efficiency, growth of domestic supply chain networks, number and quality of CVDs involving manufacturers, as well as regional economic development as a result of successful technology deployment and commercialization from Institute related activities over ten years; and

- The degree to which the applicant illustrates how DOE funding will enable acceleration of energy efficiency in manufacturing, and how the Institute will appropriately leverage existing resources that will result in more impactful outcomes, including but not limited to, DOE/NNSA resources, National Laboratories, National Institute of Standards and Technology's MEP Centers, National Science Foundation's ATE Centers, national laboratories, and other government investments.

Criterion 2: Qualifications and Resources is 25%:

- Quality of the Institute's key technical personnel and their level of technical capabilities and relevance to achieving the goals and objectives of the Institute and the FOA;

- Qualifications, relevant experience, experience and time commitment of the proposed Institute Director/Chief Executive Officer and key management staff, e.g., Chief Financial Officer, Chief Technology Officer, Chief Operating Officer, in successfully managing a national effort to research and develop cybersecurity in energy efficient manufacturing technologies;

- The sufficiency of the existing and proposed equipment, facilities and capabilities to support the work and horizontal and vertical supply chain network activities;

- Adequacy of budget and spend plan for the proposed project to achieve the defined objectives;

- Adequacy of funding availability to encourage openness and new participants as the Institute goes forward, and to accommodate changes in strategic direction that may occur once the Institute is formalized and aligned with strategic roadmaps; and

- Degree to which applicant demonstrates strong operational and financial capability and assets, and explains how these will be utilized to provide a full cadre of resources to support the applicant's role as Institute lead.

And finally, Criterion 3: Operations and Management is also 25%:

Management and Governance Approach

- Effectiveness of management approach and governance structure to enable strategic and technical decision-making;

- Degree to which the Institute can operate as an independent, neutral, non-biased coordinating and convening body for a diverse set of stakeholders;

- Adequacy of the inclusion of federal government (DOE and other federal government participants identified by DOE) on decision making and advisory bodies (boards/committees) at both a strategic and technical level within the Institute; and

- The adequacy and quality of the proposed participation structure (e.g., tiered membership structure, pay-for-use arrangements) including the benefits and restrictions for each level of participation (such as IP rights) to incentivize broad private sector participation from SMEs, minority-owned businesses, and women-owned businesses.

Criterion 3 continued includes Operations

- The adequacy and quality of annual planning processes, including the strategic planning and industry roadmap activities, periodic update of the industry roadmap (annual or bi-annual) and incorporation of the industry roadmap to Institute strategic planning;

- Strength of the technical management plan for selecting and prioritizing R&D work, tracking performance, and planned periodic (annual) review of processes for Institute and project performance;

- Quality of the stakeholder engagement plan, and how it demonstrates openness to new participants, in particular with SMEs, minority-owned businesses, and women-owned businesses, and ability to engage stakeholders along the supply chain network including end-users;

- Adequacy of the discussion of the economic and operational key risk areas involved in the operations and management plan, and the quality of the mitigation strategies to address them, specifically with respect to Intellectual Property management and strengthening U.S. manufacturing competitiveness;

- The adequacy of the Institute's strategy to manage export control compliance;

- Degree to which the Institute can meet the goal of strengthening U.S. manufacturing competitiveness while engaging a wide range of stakeholders that may include foreign participants; and

- Adequacy of how metrics will be tracked to gauge success of the Institute and impact in the technology area.

And finally in Criterion 3:

Project Management, Intellectual Property Management Plan, and Transition Plan

- The adequacy, reasonableness, and soundness of the proposed project management plan for accomplishment of the Institute objectives; and

- Extent to which the applicant demonstrates a strong level of integration across the Institute elements to provide value which is greater than the sum of the individual activities (i.e., how will the shared facilities support the technical education and workforce development plans and project activities).

- Adequacy of the IP management plan for supporting the needs of the Institute and its participants, which addresses the precompetitive landscape and the broader U.S. manufacturing sector; and

- Quality of the IP Management plan and any other IP agreements (attached as an Appendix to the Narrative) demonstrating that the IP issues inherent with collaborations and/or multi-user facilities are addressed, including those outlined in Section VI.B.x of this FOA.

And finally, Transition Plan

- Likelihood that the Institute can achieve financial self-sufficiency from dedicated federal funding within five years; and

- Reasonableness of the extended profit and loss estimates for an additional three years beyond the award project period.

The Full Application are reviewed by experts in the FOA topic areas. After those experts review the applications, EERE will provide applicants with reviewer comments. Applicants will have a brief opportunity to review the comments and prepare a short Reply to Reviewer Comments responding to comments however they desire. The Reply to Reviewer Comments is due by September 26, 2019. Applicants should anticipate receiving the independent reviewer comments approximately three business days before this due date. The Reply to Reviewer Comments is an optional submission; applicants are not required to submit a Reply to Reviewer Comments.

This a **customer centric** process that provides applicants with a unique opportunity to correct misunderstandings and misinterpretations and to provide additional data that might influence the selection process in their favor. The Replies are considered by the reviewers and the selection official.

Replies to Reviewer Comments must conform to the content and form requirements listed in the FOA and repeated on this slide. If a Reply to Reviewer Comments is more 10 pages in length, EERE will review only the first ten pages and disregard any additional pages.

As part of the merit review process, EERE may invite certain applicants to participate in Pre-Selection Interviews.

The invited applicants will meet with EERE representatives to provide clarification on the contents of the Full Applications and to provide EERE an opportunity to ask questions regarding the proposed project. The information provided by applicants to EERE through Pre-Selection Interviews contributes to EERE's selection decisions.

If EERE conducts Pre-Selection Interviews for this FOA, EERE will notify the invited applicants and provide more details about the format for the interviews at that time.

EERE will not reimburse applicants for travel and other expenses relating to the Pre-Selection Interviews, nor will these costs be eligible for reimbursement as pre-award costs.

EERE may select applications for funding and make awards without Pre-Selection Interviews. Participation in Pre-Selection Interviews with EERE does not signify that applicants have been selected for award negotiations.

The Selection Official may consider:

- Merit review recommendation

- Program policy factors

- And amount of funds available in arriving at selections for this FOA.

After the Merit Review process, the Selection Official may consider program policy factors to come to a final selection decision.

The following program policy factors may be considered:

The degree to which the proposed project exhibits technological diversity when compared to the existing DOE project portfolio;

The degree to which the proposed project, including proposed cost share, optimizes the use of available EERE funding to achieve programmatic objectives;

The level of industry involvement and demonstrated ability to accelerate commercialization and overcome key market barriers;

The degree to which the proposed project is likely to lead to increased employment and manufacturing in the United States;

The degree to which the proposed project will accelerate transformational technological advances in the area that industry by itself is not likely to undertake because of technical and financial uncertainty; and

The degree to which the proposed project, or group of projects, represent a desired geographic distribution (inserting past awards and current applications).

There are several one-time actions before submitting an application in response to this FOA, and it is vital that applicants address these items as soon as possible. Some may take several weeks, and failure to complete them could interfere with an applicant's ability to apply to this FOA, or to meet the negotiation deadlines and receive an award if the application is selected.

Obtain a Dun and Bradstreet Data Universal Numbering System or DUNS number.

Applicants must register with the System for Award Management, abbreviated as SAM. Designating an Electronic Business Point of Contact and obtaining a special password called an MPIN are both important steps in the SAM registration process. SAM registration should be updated annually.

Applicants should register in FedConnect. To create an organizational account, your organization's SAM MPIN is required.

And applicants should register in Grants.gov to receive automatic updates when Amendments to this FOA are posted. However, please note that Concept Papers and Full Applications will not be accepted through Grants.gov.

All required submissions must come through EERE Exchange. EERE will not review or consider applications submitted through any other means.

Some Key Submission Points:

-Check your entries in EERE Exchange

--Submissions could be deemed ineligible due to an incorrect entry

-EERE strongly encourages Applicants to submit your application 1-2 days prior to the deadline to allow for full upload of application documents and to avoid any potential technical glitches with EERE Exchange

-Make sure you hit the submit button

--Anytime you make a change you must hit the submit button again, because any changes will un-submit your application and you will need to hit that button again

-For your records, we advise you to print out the EERE Exchange Confirmation page at each step, which contains the application's Control Number

For points of contact:

- Applicants must designate primary and backup points-of-contact in EERE Exchange with whom EERE will communicate to conduct award negotiations

- It is imperative that the Applicant/Selectee be responsive during award negotiations and meet negotiation deadlines

-- Failure to do so may result in cancellation of further award negotiations and rescission of the Selection

As previously mentioned, all questions to this FOA should be submitted to the FOA mailbox: cemii@ee.doe.gov.

All Q&As will be posted on EERE Exchange.

And EERE will attempt to respond to questions within 3 business days.

If you have any problems uploading or submitting application documents, please email the EERE Exchange helpdesk at EERE-ExchangeSupport@hq.doe.gov.

Note that all questions asked during today's webinar will be posted on Exchange.

And thank you for your attendance. This concludes the webinar.