CYBERSECURITY MANUFACTURING INNOVATION INSTITUTE

Cybersecurity in Energy Efficient Manufacturing

DE–EE0009046

CYMANII

2023 Request for Proposals (RFP) for Research, Development, and Demonstration (RD&D)

Release Date: August 17, 2023
Released by: The Cybersecurity Manufacturing Innovation Institute (CyManII)

Key Dates for this Request for Proposal	
RFP Release	August 17, 2023 at 11:30 a.m. EST
Informational Webinar	September 6, 2023 at 4 p.m. EST
Proposal Due Date	September 29, 2023 at 7 p.m. EST
Notification of Selection	October 31, 2023
Anticipated Award Date	November 17, 2023

Contents

1   CyManII Overview

The Cybersecurity Manufacturing Innovation Institute ("Institute" or "CyManII") is one of 18 Manufacturing USA Innovation Institutes designed to revitalize American manufacturing and support domestic manufacturing competitiveness.

The Cybersecurity Manufacturing Innovation Institute (CyManII) was awarded to the University of Texas at San Antonio (UTSA) under the U.S. Department of Energy (DOE) Cooperative Agreement DE-EE0009046. CyManII is a national network that brings together over $111 million in public-private investment and more than 50 partners from leading manufacturers and universities across the US. The Institute will implement a national vision for manufacturing cybersecurity that unleashes American innovation for decades to come.

THE PROBLEM: As U.S. manufacturers continue to digitalize in pursuit of energy savings and competitive gains, they are increasingly vulnerable to cyber-attacks due to unsecured IT/OT systems. In 2022, 25% of all reported industrial cyber-attacks occurred in manufacturing companies, accounting for the most attacked industry sector above finance, professional services, and energy[1]. While ransomware is the most common form of threat vector for manufacturers, attacks can occur through unpatched software vulnerabilities, insider threats, organized cybercriminals, and nation-state attacks. Many of the cyber vulnerabilities seen in manufacturing environments result from lack of attention to progressively digitizing traditionally analog and isolated OT systems and equipment. Once breached, manufacturers often face denial of service, IP/data theft, product quality manipulation, and even threats to workers and/or environmental safety[2]. Unlike predominately IT systems who can schedule patch maintenance at night or establish backup systems to support updates, manufacturers are typically challenged in real time protection of vulnerable OT systems as this physical equipment is critical to production and cannot afford downtime.

1.1   Institute Goals and Objectives

CyManII's objective is to secure and sustain American leadership in global manufacturing competitiveness by providing U.S. companies, namely small- and medium-sized businesses, with the tools, support, and training needed to secure their energy-efficient smart manufacturing processes and connected supply chains. Our quantitative goals are to help manufacturers save one quad of energy, mitigate one trillion vulnerability instances, train one million workers, and save $1 billion. CyManII will achieve these goals by:

- Securing the digital thread.
- Creating a cyber-informed workforce.
- Developing a network of trusted partners so that we can **Secure. *Together*.**

A secure digital transformation of the U.S. manufacturing ecosystem is critical if the United States is to be the global leader in manufacturing. The technical innovations that are introduced through the

---

[1] Global distribution of cyber attacks in top industries 2022 | Statista
https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/
[2] Yampolskiy, M., King, W., Gatlin, J. (et. al) (2018). "Security of additive manufacturing: Attack taxomony and survey," *Additive Manufacturing* 21, p 431-457.

Institute will drive a cybersecure and energy efficient manufacturing economy, while also supporting widespread decarbonization efforts.

1.2   Institute Approach

As a National Manufacturing Innovation Institute, CyManII adopts a unique approach to realizing these goals that prioritizes industry involvement, development speed and agility, and early demonstration. CyManII activities reflect:

- **The CyManII Roadmap** is a strategic document that outlines the business and technical needs of U.S. manufacturers relative to cybersecurity and energy efficiency. The roadmap specifies a deliberate approach to addressing these needs by detailing research paths.
- **Industry Engagement and Agile Development.** We use product owners from industry and an Agile Development process with 2–3-week sprints, each having defined outcomes that are reviewed in sprint retrospectives. Day-to-day project work at CyManII is highly integrative and CyManII team members are flexible in supporting project teams as required by the SCRUM process.
- **Institute Foundational Tasks (IFTs).** Our fundamental research tasks are driven by the research paths identified in the CyManII Roadmap. These IFTs are the building blocks for industrial solutions advanced in the Industrial Use Cases, and include:
  - *Cybersecure Energy and Emissions Quantification* applies baselining techniques for securely quantifying energy productivity, costs, and emissions to guide the design of products, processes, and supply chain networks
  - *Secure Defensible Architecture* designs and develop effective cybersecure architectures for product-process automation and product supply chain networks to reduce downtime and accelerate innovations
  - *Secure Research and Development* Infrastructure builds a federated manufacturing infrastructure that allows secure development and evaluation of CyManII innovations and establishes the CyManII member ecosystem
  - *Coordinated Vulnerability Awareness* reshapes industry risk management practices around mitigating/preventing categories of vulnerabilities in manufacturing automation and supply chain networks
  - *Education and Workforce Development* provides state-of-the-art support to help manufactures level-up their people to enhance cybersecure, energy efficient production.
- **Industry Use Case (IUCs) Projects**
  CyManII's priority is to continue to advance its foundational research capabilities and apply those innovations to specific Industry Use Cases (IUCs) that reflect industry needs. The purpose of the IUCs is to both integrate our IFT foundational research and to advance the Technology Readiness Levels (TRL) of our innovations, thereby helping to accelerate the adoption of these solutions into industry. The IUCs will provide industrial environments together with practical business constraints and facilitate rapid learnings translatable to commercialization (higher TRL) and future research (lower TRL). IUCs will align to the NIST Cybersecurity Framework[3] as a key resource for planning, executing, and evaluating activities.

---

[3] Cybersecurity Framework | NIST, https://www.nist.gov/cyberframework

To execute CyManII activities, we rely on both dedicated CyManII resources and existing CyManII members. This RFP is open to both existing members of CyManII and those interested in becoming members (see Section 4. Eligibility Information). Necessary Capabilities: Technical Areas

To support our TRL 4-6 development objectives, we seek capabilities from applicants in any or all of the following technical areas:

- **Technical Area 1 (TA1) – Industrial Environments.** Applicants provide access to and experience with a specific manufacturing or design environment, ideally in traditionally energy-intensive sectors for clean energy manufacturing. Examples include small and medium manufacturers, large manufacturers, OEMs, IT/OT equipment manufacturers.
- **Technical Area 2 (TA2) – Industrial Solutions.** Applicants provide the capabilities to develop cybersecurity tools, methods, or processes that reflect CyManII technologies per the roadmap vision. Examples include IT development firms in cybersecurity and/or enterprise data management, hardware developers, cloud service providers.
- **Technical Area 3 (TA3) – Industrial Integration.** Applicants provide the capabilities to deploy CyManII solutions into industrial environments in a way that optimizes business objectives, decarbonization, and energy consumption. Examples include IT/OT integrators, ERP/PLM integrators and service providers, cybersecurity service providers with OT capabilities.
- **Technical Area 4 (TA4) – Research.** Applicants provide demonstrated expertise in related CyManII research areas such as, but not limited to, equipment energy efficiency modeling, cyber-physical systems, cybersecurity, manufacturing and supply chain modeling, electrical engineering and hardware development, cloud-based computing, etc. Examples include For-profit and not-for-profit research organizations, research universities and academic institutions, national labs, research divisions within corporate enterprises.
- **Technical Area 5 (TA5) – General Capabilities.** Applicants provide experience, resources and/or support related to CyManII's Institute Foundational Tasks and/or manufacturing workforce development. These applicants help with the integration and translation of research to practice and may provide services such as project management, access to facilities and resources, subject-matter expertise, coding and development support, equipment development and maintenance. Examples include Industry organizations and professional organizations, for-profit and not-for-profit research organizations, research universities and academic institutions, national labs, research divisions within corporate enterprises.

To bridge the "valley of death" and move innovations to higher TRLs in preparation for commercialization, multiple capabilities and resources are necessary. Industry Use Cases require capabilities from fundamental research, as well as different industry stakeholders. The following diagram (Figure 1) shows the different Technical Area capabilities needed to support both IFT projects and IUC projects.
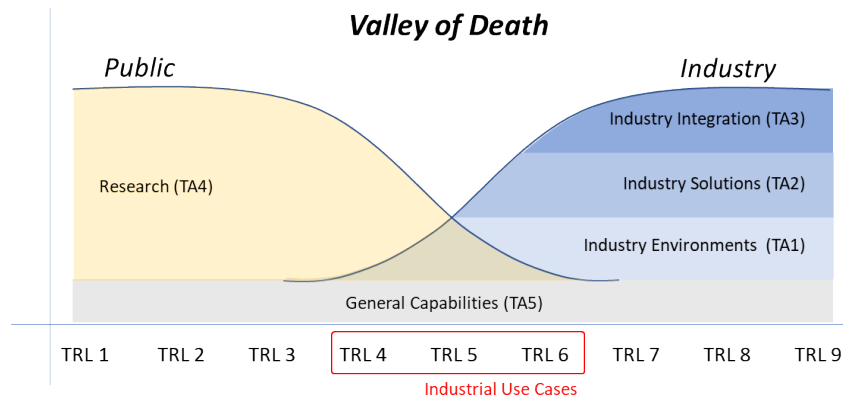
Figure 1. RFP Technical Areas' role in bridging the technology transfer "valley of death"

1.3 CyManII Projects for Budget Period 3

For the current budget period, CyManII has identified three Industry Use Case (IUC) Projects to be completed. These projects will serve as the basis for the capabilities solicited in this RFP.

The three Industry Use Case (IUC) Projects will serve to integrate our Institute Foundational Tasks and advance our TRL maturity in applied industrial environments. To execute these projects, support and interaction is needed from all five Technical Areas (see Figure 1). The following subsections outline the scope and intended outcomes of each IUC project.
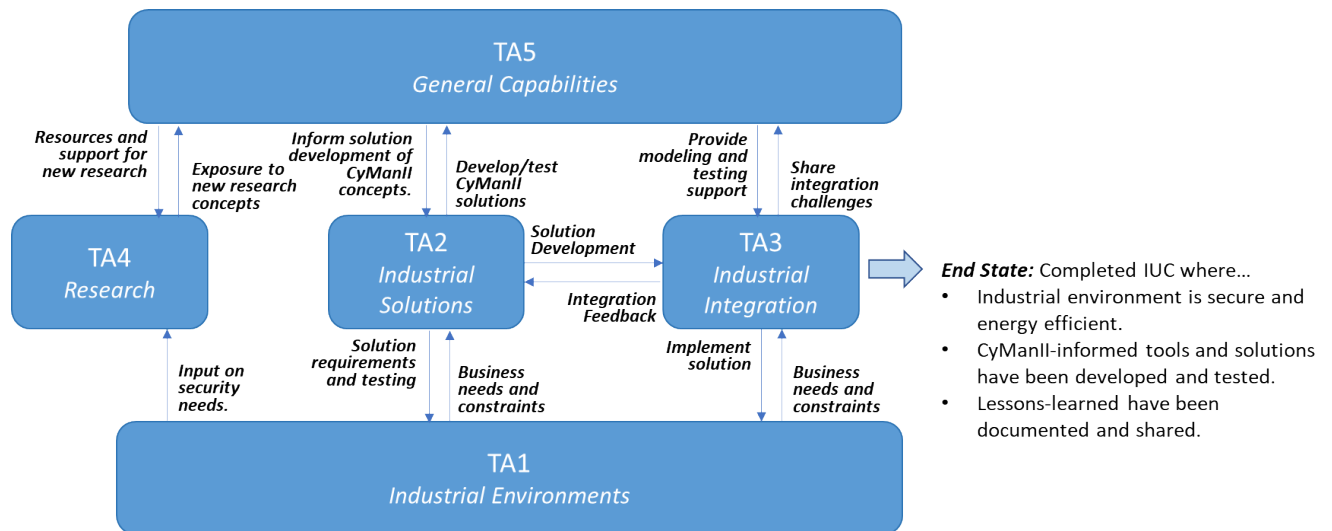
Figure 2. Technical Areas all support the execution of an Industrial Use Case Project

1.3.1 Industrial Control System Use Case

Cyber vulnerabilities to Industrial Control Systems are on the rise, and correspondingly so is the frequency of ICS cyber-attacks[4]. CyManII's own industry surveys from 2020-2023 echo these findings

---

[4] B. Babu, T. Ijyas, Muneer P. and J. Varghese, "Security issues in SCADA based industrial control systems," *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, Abha, Saudi Arabia, 2017, pp. 47-51, doi: 10.1109/Anti-Cybercrime.2017.7905261.

with a strong correlation toward uncertainty surrounding the security of ICS systems. Vulnerabilities present in the ICS's control components, industrial networks, authentication and authorization protocols, and secure communications protocols can open the door to attacks that target availability, integrity and data confidentiality[5]. To ensure the cybersecurity of industrial controllers in the field, it is critical to understand, address and track the mitigation of cyber-vulnerabilities that may emerge during the production value chain.

The objective of this IUC is to demonstrate industry-relevant security controls surrounding the production and associated supply chain of ICS systems to ensure digital integrity and supply chain traceability while improving resilience to a cyber event. This project will implement an end-to-end application of the CyManII Secure Defensible Architecture (SDA) and deploy CyManII's Cyber-Physical Passport to the production of an industrial controller, including its integrated circuit design, firmware, and associated network communications protocol of the end control system. The applicant should explain the specific cybersecurity problem as it relates to the use case and also explain why this is critical to be solved and how it will help CyManII in improving their TAs. This effort addresses the challenge of securing tight control loops for ICS systems and the integrity of the supply chain that supports critical manufacturing functions. A successful IUC will be defined when a Cyber Physical Passport has been applied to the production of an industrial controller (including relevant integrated circuits and firmware) and a sample production unit can be assessed for verifiable security guarantees of its cyber-physical integrity. To complete this IUC, the capabilities from the following Technical Areas are needed:

Table 1. Technical Area capabilities needed for Energy Controller Industrial Use Case

Technical Area	Specific IUC Outcomes
(TA1) Industry Environments	The project should reflect an industrial environment that focuses on the design, manufacture and testing of industrial control systems.
(TA2) Industry Solutions	The project should develop a solution applicable to the above industrial environment (TA1) and that incorporates the following CyManII technologies: 1) design and deploy the at least a portion of the industrial environment using CyManII's Secure Defensible Architecture (SDA) modeling 2) deploy a portion of CyManII's Cyber-Physical Passport (CPP) in the ICS, 3) conduct a Cyber Energy Efficiency Quantification (CEEQ) analysis along the defined system to identify potential secure energy savings. For more information on the above technologies, please contact rfp@cymanii.org.
(TA3) Industry Integration	The project should deploy the developed solution in a production-level industrial environment so impacts can be measured with respect to the TA2 solution's effectiveness. While specific impact metrics will be defined through the course of the use case, general measures should consider impacts to energy savings, system efficiency, cyber threat identification and mitigation, system resiliency[6] and provenance traceability. For the purposes of this use case, example impact metrics may include, but are not limited to: Energy

---

[5] Z. Drias, A. Serrhouchni and O. Vogel, "Analysis of cyber security for industrial control systems," *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, Shanghai, China, 2015, pp. 1-8, doi: 10.1109/SSIC.2015.7245330.
[6] Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring (mitre.org), https://www.mitre.org/sites/default/files/2021-11/prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

	saved with the addition of secure IIoT to the ICS production process (for instance, to support enhanced energy monitoring and operational efficiency); Number of vulnerability instances mitigated during a time-limited production run of the ICS system; Change of recovery following a cyber-attack.
(TA4) Research	Per the foundational technologies identified in the CyManII Roadmap, the project should showcase the following new innovations: *Cybersecure Energy and Emissions Quantification:* A novel risk, energy, and carbon interdependency model of the selected industrial control system. The model should enable analysis of flows of risk, energy, and carbon in the context of CyManII's current models, methods, and tools. This effort addresses the challenges of building integrated and dependency-informed multi-level models of risk, energy, and carbon flows. *Secure Defensible Architecture:* This effort addresses the challenge of protecting sensitive decision logic in ICS systems through novel data encryption methods. CyManII aims to protect ICS integrity (minimizing down time) and intellectual property (avoiding loss of competitiveness). *Secure Research and Development Infrastructure:* Novel use of virtual containers to allow the secure integration of protected intellectual property (e.g., software) in a context relevant to this use case. The use of secure containers must be in the context of CyManII's current tools, methods, and processes. This effort addresses the challenge of protecting proprietary capabilities (software, hardware, data) in a shared pre-competitive environment. *Coordinated Vulnerability Awareness:* Novel descriptions in mathematical logic of three Industrial Control Systems/Operational Technology (ICS/OT) CWEs relevant to ICS. The use of formal expressions of CWEs will verify/prove mitigation of categories of vulnerabilities including vulnerabilities in those categories not yet discovered. The expression of CWEs in mathematical logic must be in the context of CyManII's current models, tools, methods, and processes. This effort addresses the challenge of using categorical mitigation strategies given that there are too many known and known ICS/OT vulnerabilities to mitigate individually. For more information on these foundational technologies, the applicant should refer to the 2022 CyManII Roadmap, which can be requested at the following link: https://cymanii.org/roadmap2022/
(TA5) General capabilities	The project deliverables include a final report and quarterly presentations that highlight key findings, lessons learned, and educational opportunities. The General Capabilities Technical Area will be responsible for assembling these deliverables, facilitating cross-TA integration, and promoting CyManII mission alignment. A minimum of 10% of the overall project budget must be in this TA.

1.3.2 Secure Digitalization Industrial Use Case

The objective of this IUC is to demonstrate the application of secure digitalization to a small manufacturing enterprise's digital transformation and to identify and develop good practices, supported by a relevant business case. The applicant team will work with a small manufacturing business to digitalize an existing process while implementing security controls under a Cyber-Informed Engineering[7] paradigm consistent with CyManII technologies. This topic addresses the challenge of helping small and medium sized manufacturing businesses digitalize their systems through the interconnection and instrumentation of equipment without introducing new cyber risks. The applicant should clearly explain the cybersecurity problem they are solving and at what levels; product, process, shopfloor, and/or supply chain. A successful IUC will be defined when a small manufacturer has digitalized and demonstrated improved system hardening, also sharing good practices and business-informed guidelines in the form of a cybersecurity playbook. To complete this IUC, the capabilities from the following Technical Areas are needed:

Table 2. Technical Area capabilities needed for Secure Digitalization Industrial Use Case

Technical Area	Specific IUC Outcomes
(TA1) Industry Environments	The project should reflect an industrial environment that is undergoing a process of digitalization searching for greater competitiveness through energy efficiency, decarbonization, and system resiliency to cyberattack. The project should represent the needs and constraints of a small to medium manufacturer within a sector that is traditionally energy intensive for clean energy manufacturing[8].
(TA2) Industry Solutions	The project should enhance the company's overall cybersecurity posture and readiness, including that of its new and existing digital OT systems by developing a solution (or solution set) pertinent to the company's risk tolerance, business needs, and sector type. The NIST cybersecurity Framework will be leveraged to aid in the identification and design of an appropriate solution set for the company. The project should 1) help the company establish a cybersecurity program in alignment with the NIST cybersecurity Framework 2) develop a technical solution or solution set to ensure the cyber protection of the company's newly acquired digital OT and 3) demonstrate the effectiveness of the solutions in mitigating cyber vulnerabilities, reducing costs due to cyber-attacks, and energy saved as a result of implementing secure OT. Solutions may leverage current and ongoing CyManII technologies such as those developed for SDA, CEEQ, and CPP, but should at a minimum consider CIE principles and CWEs. Solutions may include, but are not limited to, unique processes, architectural designs, system models (e.g. "digital twins" for use in security), or the development of new hardware. For more information on the above technologies, please contact rfp@cymanii.org..

---

[7] Robert Anderson, Jacob Benjamin, Virginia Wright, Luis Quinones, Jonathan Paz (March 2017). Cyber-Informed Engineering (https://inldigitallibrary.inl.gov/sites/sti/sti/7323660.pdf)

[8] Energy- and Emissions-Intensive Industries | Department of Energy, https://www.energy.gov/eere/iedo/energy-and-emissions-intensive-industries

(TA3) Industry Integration	The project should implement the developed technical solution(s) into the actual industrial environment such that impact can be measured on solution effectiveness. Additionally, the project should implement the developed cybersecurity program wholistically across the business or business unit to support the technical solution. This may include, for example, training employees, working with the business's operations divisions to establish cybersecurity-relevant KPIs, and/or modifying supplier procurement requirements to consider cybersecurity-relevant controls. While specific impact metrics will be defined through the course of the use case, general measures should consider impacts to business competitiveness, energy savings, system efficiency, cyber threat identification and mitigation, and system resiliency[9]. For example, impact metrics may include, but are not limited to: Energy saved and process cost reduction with the addition of secure IIoT and/or sensors to the manufacturing process scope as defined by the proposal; Business costs resulting from reduction in attack surface area following secure digitalization of OT; Number of cyber weaknesses identified in defined process scope.
(TA4) Research	The project focuses on applied research, where new findings should produce generalizable findings and good practices on secure digitization within a small or midsized manufacturer and documented in the form of a playbook. The playbook should align with NIST cybersecurity Framework guidelines, highlight the application of CIE in operational environments, and focus on needs and constraints of small manufacturers.
(TA5) General capabilities	The project deliverables include a final report (which includes the Playbook) and quarterly presentations that highlight key findings, lessons learned, and educational opportunities. The General Capabilities Technical Area will be responsible for assembling these deliverables, facilitating cross-TA integration, and promoting CyManII mission alignment. A minimum of 10% of the total project budget must be allocated to TA5.

1.3.3 Additive Manufacturing Industrial Use Case

The objective of this IUC is to demonstrate how an additive manufacturer can implement security provenance tracking of their products' digital thread to ensure product integrity and supply chain traceability while reducing costs. The project will implement CyManII's Secure Defensible Architecture and deploy the Cyber-Physical Passport to an additive production process reflective of that in a small machine shop in the production of components and system (e.g. sand cast moldings, metal parts, or polymer prototypes). This topic addresses the challenges of small and medium additive manufacturing enterprises around the security of design files and the monitoring of machine critical production parameters. The applicant's solution should aid in the detection or defense of production specific data

---

[9] Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring (mitre.org),
https://www.mitre.org/sites/default/files/2021-11/prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

or the sabotage of additive manufacturing equipment. A successful IUC will be defined when a solution is deployed in the industry environment and quantifiable impact measures are collected. To complete this IUC, the capabilities from the following Technical Areas are needed:

Table 3. Technical Area capabilities needed for Additive Manufacturing Industrial Use Case

Technical Area	Specific IUC Outcomes
(TA1) Industry Environments	The project should reflect an industrial environment that specializes in additive manufacturing processes and that already adopts a moderate degree of digitization[10]. The project should represent the needs and constraints of a small to medium manufacturer within a sector that is traditionally energy intensive for clean energy manufacturing.
(TA2) Industry Solutions	The project should develop a solution applicable to the above industrial environment (TA1) that incorporates the following CyManII technologies: 1) design and deploy the at least a portion of the industrial environment around CyManII's Secure Defensible Architecture (SDA) principles 2) deploy CyManII's Cyber-Physical Passport (CPP) using the SDA to secure design files, 3) conduct a Cyber Energy Efficiency Quantification (CEEQ) analysis along the defined system to identify potential secure energy savings and identify areas where sensor monitoring for security also increases energy awareness/optimization. For more information on the above technologies, please contact rfp@cymanii.org.
(TA3) Industry Integration	The project should deploy the developed solution into the actual industrial environment such that impact can be measured on solution effectiveness. While specific impact metrics will be defined through the course of the use case, general measures should consider impacts to energy savings, system efficiency, cyber threat identification and mitigation, system resiliency[11] and intended design to production provenance traceability. For the purposes of this use case, example impact metrics may include, but are not limited to: Energy saved and process cost reduction with the addition of secure IIoT and/or sensors to the manufacturing process scope as defined by the proposal; identification of critical parameters for additive manufacturing such as melt pool, deposition rates, void detection design file integrity assurance as a result of CPP deployment.
(TA4) Research	Per the foundational technologies identified in the CyManII Roadmap, the project should produce the following new innovations: *Cybersecure Energy and Emissions Quantification:* A novel risk, energy, and carbon interdependency model of the selected industrial process. The model

---

[10] ISO/ASTM 52900 standard classifies additive manufacturing in seven process categories: binder jetting, directed energy deposition, material extrusion, material jetting, powder bed fusion, sheet lamination and vat polymerization.

[11] Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring (mitre.org), https://www.mitre.org/sites/default/files/2021-11/prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

should enable analysis of flows of risk, energy, and carbon in the context of CyManII's current models and methods.

Secure Defensible Architecture: Used to protect design file integrity from reception through production. This application must be in the context of CyManII's current models, methods, and tools. This effort addresses the challenge of protecting sensitive production information in additive supply chains that are more vulnerable to insitu manipulation.

Secure Research and Development Infrastructure: Novel use of virtual containers to allow the secure integration of protected intellectual property (e.g., software) in a production environment relevant to additive manufacturing. The use of secure containers must be in the context of CyManII's current tools, methods, and processes. This effort addresses the challenge of protecting proprietary capabilities (software, hardware, data) in a shared pre-competitive environment.

Coordinated Vulnerability Awareness: Novel descriptions in mathematical logic of an additive manufacturing process. The use of formal expressions of CWEs will facilitate the use of SDA to verify/prove mitigation of categories of vulnerabilities including vulnerabilities in those categories not yet discovered. The expression of CWEs in mathematical logic must be in the context of CyManII's current models, tools, methods, and processes.
For more information on these foundational technologies, the applicant should refer to the 2022 CyManII Roadmap, which can be requested at the following link: https://cymanii.org/roadmap2022/

(TA5) General capabilities	The project deliverables include a final report and quarterly presentations that highlight key findings, lessons learned, and educational opportunities. The General Capabilities Technical Area will be responsible for assembling these deliverables, facilitating cross-TA integration, and promoting CyManII mission alignment. A minimum of 10% of the overall project budget must be in this TA.

2   RFP Topic Areas

This RFP seeks proposals to support completion of the three CyManII IUC projects initiated in Budget Period 3. Because a single applicant/enterprise may not have all the capabilities necessary to complete an entire IUC project, applicants are encouraged to apply for individual or multiple Technical Areas that contribute to a single IUC. While a single proposal may address multiple Technical Areas, a separate proposal must be submitted for each Industrial Use Case. All applicants must allocate at least 10% of their total budget to TA5 activities. The following Technical Areas are available for application:

Energy Controllers Industrial Use Case

- (TA1) Industry Environments
- (TA2) Industry Solutions
- (TA3) Industry Integration

- (TA4) Research
- (TA5) General Capabilities

Secure Digitalization Industrial Use Case

- (TA1) Industry Environments
- (TA2) Industry Solutions
- (TA3) Industry Integration
- (TA4) Research
- (TA5) General Capabilities

Additive Manufacturing Industrial Use Case

- (TA1) Industry Environments
- (TA2) Industry Solutions
- (TA3) Industry Integration
- (TA4) Research
- (TA5) General Capabilities

Proposals should communicate how the applicant intends to support one or more Industrial Use Cases and to which Technical Area(s) they will contribute. For each Industrial Use Case intended, applicants should specify:

- Technical Area(s) of expertise
- Experience in the Technical Area
- Enabling capacities that may support the overall Use Case

3 Award Information

3.1 Estimated Funding

A total of $4,700,000 is available, subject to Department of Energy approval and availability of funds. Fifteen Technical Area awards will be available to support IUCs. A proposal may apply for a single IUC-specific technical area, or multiple technical areas. A proposal may represent a single organization or a team of organizations (for more details, see Section 4.2 "Teaming"). While a single proposal may address multiple Technical Areas, a separate proposal must be submitted for each Industrial Use Case. These funds will require a minimum 20% cost share commitment from the awardee. CyManII is not obligated to make any awards under this RFP.

Table 4. Awards per Topic Area

Award Type	No. Awards.	Award Ceiling
Industrial Control Systems Use Case	**5**	**$1,700,000 (total)**
(TA1) Industry Environments	1	$240,000
(TA2) Industry Solutions	1	$340,000
(TA3) Industry Integration	1	$340,000
(TA4) Research	1	$440,000
(TA5) General Capabilities	1	$340,000
Secure Digitalization Industrial Use Case	**5**	**$1,500,000 (total)**
(TA1) Industry Environments	1	$250,000
(TA2) Industry Solutions	1	$400,000
(TA3) Industry Integration	1	$400,000
(TA4) Research	1	$200,000
(TA5) General Capabilities	1	$250,000
Additive Manufacturing Industrial Use Case	**5**	**$1,500,000 (total)**
(TA1) Industry Environments	1	$240,000
(TA2) Industry Solutions	1	$300,000
(TA3) Industry Integration	1	$300,000
(TA4) Research	1	$300,000
(TA5) General Capabilities	1	$360,000

Note: Topic Area award ceilings do not sum to IUC award ceilings.

3.2 Period of Performance

Maximum of 15 months with work expected start November 1, 2023.

3.3 Subaward Agreements

All awardees will be required to sign a CyManII Master Sponsored Research Agreement (MSRA) and a project agreement. These agreements include mandatory flow-down terms and conditions from the cooperative agreement DE-EE0009046 between DOE and the University of Texas San Antonio. Drafts of the MSRA and project agreement can be requested at RFP@cymanii.org.

3.4   Intellectual Property Management Plan

Intellectual property developed under an award will be managed in accordance with the Intellectual Property Management Plan ("IPMP") as agreed to by the Subrecipient and attached to this RFP. At the time of execution of a Project Agreement under the MRSA, all parties will agree on an IP model for the specific Project to be conducted and will agree upon specific IP terms implementing said IP model.

4   Eligibility Information

4.1   Requirements to Receive Funding

- All project team members must be at least a Collaborative-level CyManII member in good standing by the time the project is awarded by CyManII. Note: Applicants are not required to hold CyManII membership at the time of submission, but if selected all teaming organizations within the proposal must pursue and be approved for CyManII membership.
- The Principal Investigator (PI) is approved for access to the CyManII TII.
- A 20% cost share of the total allowable cost of the project is required. See Section 5 for further detail on cost share.

4.2   Teaming

It is likely that a single enterprise does not contain all the Technical Area capabilities required for a single Industrial Use Case, therefore teaming is encouraged and will be considered during evaluation. A team ideally includes a manufacturer, and one or more of the following: a systems integrator, an app vendor, a college or university, a DOE National Laboratory, a machine builder, or Original Equipment Manufacturer (OEM), and other manufacturers, especially small and medium-sized manufacturers. For any teaming arrangement, a lead organization shall be identified. Additionally, if an applicant does not provide all the Technical Area capabilities required for a single Industrial Use Case, they may submit a proposal to address only those Technical Area to which they can address. If selected, CyManII will facilitate post-award teaming to complete the necessary Technical Area capabilities required for a single Industrial Use Case.

While a single proposal may address multiple Technical Areas, a separate proposal must be submitted for each Industrial Use Case.

U.S. Citizenship Requirements. All applicants and team members must be domestic entities. To qualify as a domestic entity, the organization must be incorporated (or otherwise formed) under the laws of a State or territory of the United States with majority domestic ownership or control and have a physical place of business in the United States.

5   Cost Share

A minimum cost share of 20% of total project cost is required. Where teaming occurs, cost share will be considered in aggregate. The lead organization must ensure that the cost share requirement is met. See 2 CFR200.306 and 2 CFR 910.130 for information on allowable cost share contributions. Letters of cost share commitment, signed by a representative with approval to bind the organization, must be submitted with all proposals.

Any cost share provided through award of a selected proposal may be used to fulfill the cost share requirements of CyManII membership.

6 Proposal Submission Requirements

6.1 General

Proposals must be submitted via email at RFP@cymanii.org. Proposals must be received by the due date specified in Section 8 of this document. Late proposals will not be accepted.

Please check https://cymanii.org/project_calls/ for any updates to this RFP.

Must be written in English Language
- All pages must be 8.5 x 11-inch with margins of no less than one inch on every side.
- Proposals must use Times New Roman or Calibri font, no smaller than 12 points, and at least 1.0 line spacing.
- Tables and figures may use no smaller than 10-point font and at least 1.0 line spacing.
- Proposals must be submitted in a .pdf format.
- Do not include any proprietary information in the proposals.
- RFP templates are in this document's Appendices section.

6.2 Proposal Package

A project proposal may respond to more than one Technical Area, but applicants must submit a separate proposal for each Industrial Use Case if they intend to propose to more than one. Each proposal package must contain the following:

- **Cover Page and Abstract** – Limited to 1 page. See APPENDIX A
- **Technical Volume** – Limited to 5 pages. Provide technical approach to solving the problem statement. Proposals shall identify any risks in meeting the requirements. See APPENDIX B.
- **Management Volume** – No page limit. Provide CV/resumes of team members, details on any special facilities or other resources available for effort, proposed schedule, and risk assessment and mitigation plan. See APPENDIX C.
- **CyManII Cost Summary Form** – The CyManII cost summary form shall be completed detailing total project costs. One Budget Justification form from each organization expecting an agreement with CyManII shall be submitted. See APPENDIX D.
- **Cost Share Letter of Commitment** – Using the template provided in APPENDIX E, provide a cost share letter of commitment that details type, valuation, and benefit to CyManII signed by an authorized representative of the organization. Committed cost share for CyManII membership requirements may be utilized to fulfill this requirement.

7 Evaluation and Selection Criteria

7.1 Technical Evaluation Criteria

These are the criteria by which each proposed project will be technically evaluated and prioritized.

A. Technical Merit (Weight: 25%) – The application's technical objectives are clearly stated, well-conceived, and technically feasible. The application fully addresses one or more Technical Areas for a single Industrial Use Case as described in Section 1.3 of this RFP. The proposed project has potential to make a valuable contribution to the competitiveness of U.S. manufacturing.

B. Alignment (Weight: 25%) – The proposed project aligns with, and will materially advance, the mission of the Institute per the CyManII Roadmap.

C. Capabilities and Capacity (Weight: 50%) – Adequacy and feasibility of the proposed approach to achieving the stated objectives of the project. Likeliness that the proposed work can be accomplished within the proposed performance period by the team, given their organizational diversity, experience, expertise, past accomplishments, available resources, institutional commitment, and access to technologies. Clarity, completeness and appropriateness of the project plan and timeline. Clarity, logic, and effectiveness of the project organization, including team members to successfully complete the project. Credentials, capabilities, experience of the key personnel. Adequacy and availability of personnel, facilities, and equipment (both hardware and software) to perform the proposed project within proposed performance period.

7.2   Selection Criteria

Following a technical evaluation, applicants must meet the following selection criteria to receive an award.

A. Meets strategic goals of the Institute
B. Fit with current Budget Period (BP) funding profiles
C. Cost-efficient use of CyManII funds and degree of technical amplification/acceleration/innovation with cost share resources
D. Cross-industry applicability and broad-based relevance and impact
E. Commitment to use of the CyManII Technical Innovation Infrastructure and Institute Approach
F. Full compliance with DOE and CyManII requirements
G. High-level fit to create balance in the Institute's portfolio of work

8   Proposal Due Date and Award Timeline

RFP Release	August 17, 2023 at 11:30 a.m. EST
Informational Webinar	September 6, 2023 at 4 p.m. EST
Proposal Due Date	September 29, 2023 at 7 p.m. EST
Notification of Selection	October 31, 2023
Anticipated Award Date	November 17, 2023

9   Other Information

Please send all questions regarding this RFP to RFP@cymanii.org

For more information on membership please go to www.Cymanii.org/membership

To register for the informational webinar on September 6, 2023, please visit:
https://events.teams.microsoft.com/event/d86503d6-2386-4938-95da-7a4ecf6be85b@3a228dfb-c647-44cb-8835-7b20617fc906

10 Appendices

The following Appendices are included:

Proposal Package	Page Limit	Template Provided
Proposal Cover and Abstract	1	Appendix A
Technical Volume	5	Appendix B
Management Volume	Unlimited	Appendix C
CyManII Cost Summary Form	Unlimited	Appendix D
Cost share Letter of Commitment	Unlimited	Appendix E
Reference Material		
Intellectual Property Management Plan (IPMP)		Appendix F
DOE Intellectual Property Provisions		Appendix G

Project Title	*Your title here*		
Project Cost Summary (all team members combined)	**Total Project cost share provided:** *$ value here* **Total CyManII funding requested:** *$ value here* **Total project cost: (Cost Share + CyManII):** *$ value here*		
Project Team Members:	*Please list all organizations on team*		
Lead Organization:	*Lead organization here*		

Technical POC: Name: Title: Organization: Phone: Email:	**Administrative POC:** Name: Title: Organization: Phone: Email:

IUC and Technical Area Designation:

Energy Controllers Industrial Use Case			
(TA1) Industry Environments	☐	$0	$0
(TA2) Industry Solutions	☐	$0	$0
(TA3) Industry Integration	☐	$0	$0
(TA4) Research	☐	$0	$0
(TA5) General Capabilities	☐	$0	$0
Secure Digitalization Industrial Use Case			
(TA1) Industry Environments	☐	$0	$0
(TA2) Industry Solutions	☐	$0	$0
(TA3) Industry Integration	☐	$0	$0
(TA4) Research	☐	$0	$0
(TA5) General Capabilities	☐	$0	$0
Additive Manufacturing Industrial Use Case			
(TA1) Industry Environments	☐	$0	$0
(TA2) Industry Solutions	☐	$0	$0
(TA3) Industry Integration	☐	$0	$0
(TA4) Research	☐	$0	$0
(TA5) General Capabilities	☐	$0	$0

Project Abstract: *Please briefly describe your overall project summary here.*

Technical Volume

A. Team

List the organizational team members of your application. Provide a brief 1-2 sentence description of each organization highlighting any relevance to specific Technical Areas. Detailed information on the team will be provided in the Management Volume.

B. Project Goals and Objectives:

Describe the primary goals and objectives of your proposed engagement with the IUC and how your team will support the Technical Areas necessary for this IUC.

Describe what you hope to contribute to the CyManII IUC project and what your teaming organization(s) hope to gain/learn from this engagement.

C. Approach:

Describe your approach for addressing the challenges and specific IUC outcomes listed in Section 1.3 "CyManII Projects for Budget Period 3." Be sure to describe how you will support specific Technical Areas in coordination with your selections in the "Proposal Cover Sheet and Summary" page.

Describe your project management approach and how you will allocate/coordinate people to support the larger CyManII Industrial Use Case project.

Describe how you support the development and capture of the IUC outcomes (specified in Section 1.3 "CyManII Projects for Budget Period 3.")

D. Deliverables:

Required Deliverables (in addition reporting requirements in the corresponding CyManII Master Sponsored Research Agreement (MSRA).

- Project briefing for the kickoff meeting
- Mid-point demonstration narrative, briefing, and underlying technical artifacts
- Final fully detailed demonstration narrative, briefing, and underlying technical artifacts
- Condensed demonstration narrative and briefing for CyManII members
- Technical elements specific to the technical project topics
- Scrum artifacts: product and sprint backlogs, sprint review & demonstrations materials, sprint deliverables, team technical discussions on CyManII mailing lists
- Other deliverables as the applicant deems appropriate

Management Volume

A. **Lead Organization**
   a. **Organization Name**
   b. **Organization Summary**
   c. **Organization Headquarters Location**
   d. **Key Technical Areas**
   e. **Key Individual Team Members** (for each individual)
      i. **Name:**
      ii. **Nationality:**
      iii. **Skills/Experience Summary:** *(5-6 sentences)*
      iv. **Percent effort:**
   f. **Key Resources.** *List and describe any key resources, tools, solutions, IP, facilities that the organization will bring to support the IUC.*

B. **Supporting Organizations**
   a. **Organization Name**
      i. **Organization Summary**
      ii. **Organization Headquarters Location**
      iii. **Key Technical Areas**
      iv. **Key Individual Team Members** (for each individual)
         1. **Name:**
         2. **Nationality:**
         3. **Skills/Experience Summary:** *(5-6 sentences)*
      v. **Key Resources.** *List any key resources, tools, solutions, IP, facilities that the organization will bring to support the IUC*
   b. *(additional below)*

C. **Risk Assessment & Mitigation Plan:**
   Please identify any anticipated risk and provide a plan to mitigate the effects of such risk.

CYMANII COST SUMMARY FORM

Organization Name	Total Period of Performance
Organization Address	Proposal Title
Administrative Contact: Phone Number: Email Address:	Total Amount of Proposal USD$

Cost Data provided by Participant will be treated as Proprietary to Participant.

				Funding Requirement	Cost Share	Total Cost
1 **Direct Labor**						
Position Title	Hours	Pay Rate				
a. Position Title						
b. Position Title						
c. Position Title						
d. Position Title						
			TOTAL DIRECT LABOR			
2 **Indirect Costs - See * note below for further requirements**						
Fill out as applicable	Rate					
a. Fringe Benefits						
b. Material Overhead						
c. Labor Overhead						
d. General & Administrative						
e. Other						
			TOTAL INDIRECT COSTS			
3 **Direct Costs - Insert rows as necessary**						
Item Description		Qty				
a. Equipment						
b. Supplies						
c. Contractual						
Sub-recipient						
Vendor						
FFRDC						
d. Meetings & Conferences						
e. Other						
			TOTAL DIRECT MATERIAL			
4 **Project Related Travel - Only include travel necessary for project proposed**						
a. Domestic						
b. Foreign						
			TOTAL TRAVEL COSTS			
5 **Sub-Total Estimated Cost**						
6 **Total Estimated Cost**						

This proposal reflects our best estimates as of this date, in accordance with the instructions to participants.		
Typed Name and Title	Signature	Date

* A federally approved fringe benefit rate agreement, or a proposed rate supported and agreed upon by DOE for estimating purposes is required at the time of award negotiation if reimbursement for fringe benefits is requested. Please check (X) one of the options below and provide the requested.

_____A fringe benefit rate has been negotiated with, or approved by, a federal government agency. A copy of the latest rate agreement must be included with the project application.

_____There is not a current federally approved rate agreement negotiated and available. Please provide the organization's benefit package and/or a list of the components/elements that comprise the fringe pool and the cost or percentage of each component/element allocated to the labor costs identified in the Indirect Justification tab. Sample located at: https://www.energy.gov/eere/funding/downloads/sample-indirect-rate-proposal-and-profit-compliance-audit

* *TA Specific cost summary forms available upon request at rfp@cymanii.org*

(Please print on company letterhead)

Date

Entity Name
Entity Point of Contact
Entity Address

Subject: *[Proposal Title], [Industrial Use Case Title]*

Please describe the type of cost share committed and how it applies to the proposal and/or benefits CyManII. Include a note if utilizing committed membership fee cost share.

Please detail the valuation method used to determine the amount of cost share. Include any quotes or additional documentation as needed.

_____
(Signature of Entity Authorized Representative)

Name
Title

Intellectual Property Management Plan (IPMP)

Background

1. This IP Management Plan is established to govern the management and disposition of INTELLECTUAL PROPERTY directly resulting from joint research and/or development between the Parties directed to support advancing cybersecurity in energy efficient manufacturing through the Cybersecurity Manufacturing Innovation Institute ("CYMANII"), a new private-public collaboration led by The University of Texas at San Antonio ("UTSA") and funded in part through DOE award (said joint research and/or development is referred to as the "Joint Work").

2. The IP Management Plan objectives include:

   (a) Promoting the patenting, licensing, and rapid commercialization of SUBJECT INVENTIONS when the public good is best served by controlling the activities of those commercializing the SUJBECT INVENTIONS and/or by providing economic rewards necessary to encourage commercial partners to make the investment required to move an early-stage technology to the market, and

   (b) Promoting the rapid dissemination of breakthrough scientific discoveries and technological innovations for the public good.

3. All actions by UTSA documented in this IP Management Plan are subject to available funding from DOE to UTSA.

4. This IP Management Plan shall not be used to obligate or commit funds or as the basis for the transfer of funds. This IP Management Plan does not commit any Party to take any actions; the actions of each Party are independent of the actions of the other Party. In no event shall any Party be required to perform work outside the scope of the Joint Work.

5. Each Party will bear all costs, risks and liabilities incurred by it arising out of efforts under this IP Management Plan, and no Party shall have any right to any reimbursement, payment or compensation of any kind from the other, hereunder, unless agreed to in writing by separate agreement.

General Provisions

1. Inventorship or authorship of PROJECT INTELLECTUAL PROPERTY and PROJECT TECHNICAL DATA will be determined in accordance with applicable U.S. patent, trademark and copyright law and any corresponding state laws. Disposition of any resulting PROJECT INTELLECTUAL PROPERTY may be determined by the operable funding agreement or CRADA according to the terms and conditions outlined therein.

2. Each Party shall retain title to their BACKGROUND TECHNICAL DATA and BACKGROUND INTELLECTUAL PROPERTY used during the Joint Work. Each Party's BACKGROUND TECHNICAL DATA and BACKGROUND INTELLECTUAL PROPERTY shall be identified as such and, in the event, that such materials include proprietary information, shall contain such proprietary markings pursuant to any separate non-disclosure agreement(s) governing such disclosures between the Parties. BACKGROUND TECHNICAL DATA and BACKGROUND INTELLECTUAL PROPERTY shall be used during the Joint Work solely at the discretion of the owner and under conditions established by the owner.

3. Each Party shall have the right to use another Party's PROJECT TECHNICAL DATA, and PROJECT INTELLECTUAL PROPERTY along with the related BACKGROUND TECHNICAL DATA and BACKGROUND INTELLECTUAL PROPERTY identified in Exhibit C for the sole purpose of carrying out the Joint Work, but may not disclose the other Party's PROJECT TECHNICAL DATA, PROJECT INTELLECTUAL PROPERTY, BACKGROUND INTELLECTUAL PROPERTY and BACKGROUND TECHNICAL DATA to any person or third party except with the prior, express written permission of the other Party, or Parties, and under suitable confidentiality obligations pursuant to a separately executed non-disclosure agreement. Each Party shall establish and implement specific measures and protocol to protect such information and data from disclosure. Exhibit C will be amended to include additional BACKGROUND TECHNICAL DATA and BACKGROUND INTELLECTUAL PROPERTY that the Parties mutually agree is relevant to accomplish the Joint Work. The INTELLECTUAL PROPERTY rights of a Funded Research and Development Center (FFRDCs) will be solely dictated by a Cooperative Research and Development Agreement (CRADA) and not subject to this section A.

<div align="center">

Title to Subject INVENTIONS and Other Project INTELLECTUAL PROPERTY

</div>

1. **Preferred IP Rights Model**
   A. Any Party that first conceives or reduces to practice SUBJECT INVENTIONS or PROJECT INTELLECTUAL PROPERTY and is named as an assignee(s) on corresponding patent application(s), patent(s), or owners of copyrights(s) by operation of law shall hereafter be known as an "Inventing Member."
   B. Each Inventing Member shall solely own its SUBJECT INVENTIONS and other PROJECT INTELLECTUAL PROPERTY developed solely by its employees and agents and shall obtain patent protection for SUBJECT INVENTIONS at its sole discretion.
   C. Any SUBJECT INVENTIONS and PROJECT INTELLECTUAL PROPERTY jointly developed shall be jointly owned by the Inventing Members. Any jointly developed SUBJECT INVENTIONS may be protected by one or more patent applications filed by any of the Inventing Members. Inventing Members may appoint a single Inventing Member to manage and facilitate the filing, prosecution, and maintenance of patents and copyrights, as well as the licensing of such SUBJECT INVENTIONS and PROJECT INTELLECTUAL PROPERTY, under the terms of a separate joint commercialization agreement to be negotiated in good faith between them.
   D. Unless agreed to otherwise, the Inventing Member filing a patent application on a SUBJECT INVENTION, whether solely or jointly owned, shall pay all preparation and filing expenses, prosecution fees, issuance fees, post issuance fees, patent maintenance fees, annuities, interference expenses, and attorneys' fees for that patent applications and any resulting patent(s). The Inventing Members will use reasonable efforts to cooperate with each other with respect to the preparing, filing and prosecuting any such patent applications.
   E. Inventing Member may grant PROJECT PARTICIPANTS a worldwide, non-exclusive, fully paid-up license to the SUBJECT INVENTIONS and PROJECT INTELLECTUAL PROPERTY that includes the right to make, have made, use, have used, disclose, lease, sell, offer to sell, import, or otherwise transfer any product, to practice any process, to make and distribute copies, to make and distribute derivative works without the right to sublicense, except such participants can license to wholly-and majority-owned subsidiaries. Potential Inventing Member(s) may opt-out from granting the license described in this section (E) during negotiation of the award contract.
   F. Royalties generated stay with the licensing party.

G. CyManII/UTSA may license to other entities for further non-commercial R&D purposes and can publish research results as necessary to comply with any applicable law or regulation. Potential Inventing Member(s) may opt-out from granting the right to license described in this section (G) during negotiation of the award contract.

H. The INTELLECTUAL PROPERTY rights of a Funded Research and Development Center (FFRDCs) will be solely dictated by a Cooperative Research and Development Agreement (CRADA) and not subject to this section 1.

2. **Historical IP Rights Model**

A. Parties may choose in their own discretion, and with no obligation, to enter into an agreement(s) to transfer any SUBJECT INVENTIONS and PROJECT INTELLECTUAL PROPERTY either solely or jointly developed to The Board of Regents of the University of Texas System ("BOARD"). The following will apply if and only to the extent Parties choose to enter such agreement(s).

B. BOARD shall grant PROJECT PARTICIPANTS a worldwide, non-exclusive, fully paid-up license to the SUBJECT INVENTIONS and PROJECT INTELLECTUAL PROPERTY owned by the BOARD that includes the right to make, have made, use, have used, disclose, lease, sell, offer to sell, import, or otherwise transfer any product, to practice any process, to make and distribute copies, to make and distribute derivative works without the right to sublicense, except such participants can license wholly-and majority-owned subsidiaries.

C. BOARD, through CyManII management, is free to license SUBJECT INVENTIONS and PROJECT INTELLECTUAL PROPERTY owned by the BOARD to members of CyManII that did not participate in the project and to qualified members of the general public on a nonexclusive reasonable royalty basis 18 and 30 months following completion of the research project respectively.

D. CyManII shall pay for patent, copyright, trademark and other legal protection.

E. CyManII can license to third parties for non-commercial R&D purposes and can publish research results as necessary to comply with applicable laws or regulations.

F. Any such agreement shall be subject to a reservation of certain rights to the Federal Government, which include Government use rights, march-in rights and U.S. Competitiveness.

G. Assignments by non-profit entities may be subject to federal agency approval under 35 USC 202(7).

H. The INTELLECTUAL PROPERTY rights of a FFRDC will be solely dictated by a Cooperative Research and Development Agreement (CRADA) and not subject to this section 2.

3. **Exclusive IP Rights Model**

A. Where one project participant possesses a wealth of background intellectual property and contributes significantly to the development of research project intellectual property, and applicable law or regulation concerns relative to the grant of exclusive rights can be addressed, the Parties may choose in their own discretion, and with no obligation, to enter into an agreement(s) to transfer right, title and interest to SUBJECT INVENTIONS and PROJECT INTELLECTUAL PROPERTY to a single Project Participant. The following will apply if and only to the extent Parties choose to enter such agreement(s).

B. Where title or exclusive rights ultimately vest in only one Project Participant, the other PROJECT PARTICIPANTS may receive or retain nonexclusive, royalty-free licenses and/or product discounts and allowances.

C. Any such agreement shall be subject to a reservation of certain rights to the Federal Government, which include Government use rights, march-in rights and U.S. Competitiveness.

D. Assignments by non-profit entities may be subject to federal agency approval under 35 USC 202(7).

E. CyManII can license to third parties for non-commercial R&D purposes and can publish research results as necessary to comply with any applicable laws or regulations.

F. The INTELLECTUAL PROPERTY rights of a FFRDC will be solely dictated by a Cooperative Research and Development Agreement (CRADA) and not subject to this section 3.

4. **FFRDC IP Rights**

A. FFRDC's IP rights will be dictated by a Cooperative Research and Development Agreement (CRADA). The INTELLECTUAL PROPERTY rights of a FFRDC will be solely dictated by a Cooperative Research and Development Agreement (CRADA) and not subject to this IP Management Plan. In the event of any inconsistency between the terms of the CRADA and any other agreement, including this IP management plan, the membership agreement, or any other documents related to this consortium, the terms of the CRADA will control.

EERE T 540.137-16: Intellectual Property Provisions (CDSB-115)

Attachment 4, Intellectual Property Provisions
DE-EE0009046 / 0001
The University of Texas at San Antonio

01.	FAR 52.227-1	Authorization and Consent (DEC 2007) Alternate I (APR 1984)
02.	FAR 52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement (DEC 2007)
03.	2 CFR 910 Appendix A of Subpart D	Rights in Data – Programs Covered under Special Data Statutes
04.	2 CFR 910 Appendix A of Subpart D	Patent Rights (Small Business Firms and Nonprofit Organizations)
05.	Attachment 1	Determination of Exceptional Circumstances
06.	Attachment 2	W(C) 2016-004 EERE Class Patent Waiver Terms and Conditions

NOTE: In reading these provisions, any reference to "contractor" shall mean "recipient," and any reference to "contract" or "subcontract" shall mean "award" or "subaward."

These documents are available on the CyManII website

www.CyManII.org

Template Version 07/07/20