KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
DIREKTORAT RISET DAN PENGABDIAN KEPADA MASYARAKAT
PUSAT PUBLIKASI ILMIAH
Gedung Pusat Riset Lantai 6 Kampus ITS Sukolilo Surabaya 60111
Telepon: PABX 1404,1405 Fax:
ppi.its.ac.id/iptek.its.ac.id

Nomor : **3318/IT2.IV.1/B/TU.00.09/I/2025**
Lampiran : 4 (empat) berkas
Perihal : Call for Proposals Security AI Research Fund Program

Yth. : Para Kepala Departemen
Kampus ITS Sukolilo
Surabaya

Program hibah penelitian **Security AI Research Fund** yang diselenggarakan oleh AI Safety Fund (AISF) memberikan peluang besar bagi para dosen dan peneliti di Institut Teknologi Sepuluh Nopember (ITS) untuk mendapatkan pendanaan penelitian. Program ini bertujuan untuk mendukung pengembangan langkah-langkah keselamatan dalam aplikasi kecerdasan buatan (AI) dan memperkuat penerapan AI yang bertanggung jawab di skala global.

Skema dan Fokus Penelitian

No	Nama Skema	Topik Utama
1	Cybersecurity AI Research Fund Program	• Evaluasi kemampuan AI dalam eksploitasi kerentanan dan serangan otomatis. • Studi perbandingan kinerja manusia dengan bantuan AI dalam operasi siber. • Penilaian ancaman berbasis manusia, seperti phishing dan rekayasa sosial. • Peramalan dampak AI pada lanskap ancaman keamanan siber.
2	Biosecurity AI Research Fund Program	Evaluasi dan pengembangan langkah-langkah keamanan untuk penerapan AI yang aman di bidang biologi, termasuk biosecurity, bioteknologi, dan ilmu kehidupan.

Nilai Hibah dan Pendanaan

- Pendanaan sebesar $350.000 hingga $600.000 per proyek.
- Durasi proyek: maksimal 1 tahun.

Batas Akhir Pendaftaran

- 20 Januari 2025, pendaftaran melalui portal hibah AISF.

Informasi Lebih Lanjut

- Portal Pendaftaran : https://aisfund.org/funding-opportunities/
- Pengesahan DRPM ITS : http://its.id/PengesahanDRPM

Atas perhatian dan kerjasamanya disampaikan terima kasih.

Surabaya, 14 Januari 2025

Ditandatangani secara elektronik oleh:
Direktur Riset dan Pengabdian Kepada Masyarakat

Fadlilatul Taufany, S.T., Ph.D.
NIP. 198107132005011001

Tembusan Yth :

Catatan:

• UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
"*Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah*"
• Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang diterbitkan **BSrE, BSSN**
• Dokumen ini dapat dibuktikan keasliannya dengan memindai QR Code

1. Wakil Rektor IV
2. Kepala Bagian Tata Usaha, Layanan Terpadu dan Arsip Digital

Catatan:

• UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
"*Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah*"
• Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang diterbitkan **BSrE, BSSN**
• Dokumen ini dapat dibuktikan keasliannya dengan memindai QR Code

RFP: Cybersecurity AI Research

November 2024

While Artificial Intelligence (AI) offers tremendous promise to benefit cybersecurity and defensive capabilities, appropriate testing, evaluation, and best practices are required to mitigate risks in security applications. As AI is increasingly applied in cybersecurity operations and threat detection, ensuring safety is crucial to avoid negative outcomes and build public trust. This RFP focuses specifically on evaluating and improving the safe deployment of AI in cybersecurity contexts.

Objectives

The AI Safety Fund (AISF) seeks to support technical research that evaluates potential risks and develops safety measures for AI systems operating in cybersecurity contexts. This funding aims to promote responsible development of frontier AI models while establishing robust evaluation frameworks for security-related capabilities and safety measures.

This request for proposals will support technical research on frontier AI systems to reduce risks from cybersecurity. The following is a list of examples of the kinds of research we might like to support. We welcome proposals on these topics and other relevant topics under this domain.

For research proposals focusing on the biosecurity aspects of AI systems, we also encourage you to explore our other funding opportunities.

REALISTIC EVALUATIONS OF AI CYBEROFFENSE

While AI systems demonstrate value in defensive cybersecurity applications, their potential to automate or enhance offensive capabilities requires careful evaluation. Key concerns include AI systems' ability to identify vulnerabilities, generate exploit code, and adapt known attack patterns to new contexts.

Research Objectives: Benchmarks and uplift studies to evaluate frontier AI models:

- Capability to identify and exploit novel security vulnerabilities
- Effectiveness at automating complex attack chains
- Ability to adapt and modify existing exploit code

UPLIFT STUDIES

Large Language Models (LLMs) can potentially enhance actors' capabilities in cyber operations, including increasing the number of competent defenders and threat actors in cybersecurity. Uplift studies compare task performance between humans working alone versus humans assisted by AI systems.

Research Needed: Rigorous uplift studies in cybersecurity contexts that:

- Use a representative population from relevant backgrounds and skill sets
- Include robust comparison groups (AI uplift vs. tool use, internet access, expert coaching, etc.)
- Identify variables relevant to successfully executing cyber operations using frontier AI.

INTERDISCIPLINARY TESTING

LLMs may be capable of executing a range of human-centric cyber threats, including social engineering and phishing attacks.

Research Needed: Evaluations developed in partnership with experts from psychology and behavioral science that:

- Assess AI models' ability to execute and defend against human-centric cyber threats.
- Test for the full range of multimodal capabilities, including images and video

FORECASTING STUDIES

LLMs may significantly impact cybersecurity operations and the threat landscape by reducing the operational costs of cybersecurity and increasing the number of attempted and successful cyber attacks.

Research Needed: Research on and the development of methodologies for accurate forecasting of AI impact on cybersecurity operations.

AISF Grantmaking

The AISF plans to fund research projects by academic labs, non-profits, independent researchers, and for-profit mission-driven entities across both Biosecurity and Cybersecurity topics in the range of $350-$600K. Our initial target is to fund 8-10 projects but we will consider increasing this amount based on the quality of proposals received.

Based on our recommendations, we may share particularly strong applications with other philanthropists interested in exploring grant opportunities. Please indicate whether you permit us to share your materials with other potential funders in your application.

Eligible Proposal Types and Applicants

- Technical research projects focused on evaluating and improving AI safety in cybersecurity applications, as described above.
- Projects must focus on frontier AI models and their deployed versions.
- The research duration must be one year or less, and the budget must not exceed $600k.

- Eligibility with the AISF's Conflict of Interest Policy.
- Applicants must review and confirm their ability to sign the grant agreement if their application is successful. A template of the grant agreement can be accessed here.

The AISF is independent of its funders. Critical views of AISF funders will not preclude research proposals from being awarded funds.

Evaluation Criteria

Below is an outline of our grant evaluators' evaluation criteria for assessing the proposals.

Criteria	Description
Impact	Research proposals will be assessed based on their potential to improve safety measures in AI cybersecurity applications. This includes the practical applicability of the expected results and their potential for implementation in real-world settings.
Feasibility	The proposed project should include a clear timeline with well-defined milestones. The proposal should address potential challenges and include strategies for addressing them.
Relevance	The proposed research must directly apply to frontier AI models and their deployment in cybersecurity contexts. The proposal should cover existing research and how it relates to their project.
Peer Review	The proposal must include a robust plan for engaging with the broader research community and receiving feedback. The proposal should demonstrate how peer feedback will be incorporated into the research process and how the broader scientific community will validate findings.
Technical Qualifications	The evaluation will consider the team's AI safety and cybersecurity track record. Proposals should include the applicants' academic degrees, previous publications, projects, and contributions to the field. We're open to applicants without such track records if the project is particularly well-scoped and promising. Especially in this case, having named advisors on the project with relevant subject matter expertise and research experience can be helpful.
Ethics	Proposals must outline specific safety protocols that address both immediate research risks and potential downstream implications of the findings. This should detail how sensitive data and results will be handled, secured, and accessed throughout the project lifecycle. The proposal must also include a clear protocol for identifying and managing security-sensitive findings, particularly any unexpected discoveries that may emerge during the research process. Additionally, proposals should demonstrate an ethical approach to all research methodologies, avoiding any practices that may inadvertently mislead or compromise collaborators without their informed consent.
Equity	Proposals should describe how the project will advance equity and diversity in the research community, particularly regarding underserved populations.

Accessibility	The research product should prioritize open accessibility through open-source licensing, promoting transparency and broad utility. However, if unrestricted access poses a risk of harm or compromises privacy, proposals should provide a justification for limited access. Evaluators will assess the proposal's approach to balancing accessibility with safety and security considerations.

Timeline

- Request for Proposals Opens: November 18, 2024
- Question Deadline: November 25, 2024
- Answers Posted: December 9, 2024
- Proposals Due: January 20, 2025

Submission Process

Proposals can be submitted through the grant portal, accessible on the AISF website.

RFP: Biosecurity AI Research

November 2024

While Artificial Intelligence (AI) offers tremendous promise to benefit scientific research and healthcare, appropriate testing, evaluation, and best practices are required to mitigate risks in biological applications. As AI is increasingly applied in biotechnology and life sciences, ensuring safety is crucial to avoid negative outcomes and build public trust. This RFP focuses specifically on evaluating and improving the safe deployment of AI in biological contexts.

Objectives

The AI Safety Fund (AISF) seeks to support technical research that evaluates potential risks and develops safety measures for AI systems operating in biological contexts. This funding aims to promote responsible development of frontier AI models while establishing robust evaluation frameworks for bio-related capabilities and safety measures.

This request for proposals will support technical research on frontier AI systems to reduce risks from biosecurity. The following is a list of examples of the kinds of research we might like to support. We welcome proposals on these topics and other relevant topics within this domain.

For research proposals focusing on the cybersecurity aspects of AI systems, we also encourage you to explore our other funding opportunities.

EVALUATIONS FOR EVASION AND OBFUSCATION

Large Language Models (LLMs) may hide parts of the biological weapons creation process by interacting with external resources on behalf of an actor (for example, interacting with CROs or cloud labs), allowing them to evade normal oversight measures.

Research Objectives: Benchmarks, red-teaming, and uplift studies to measure LLMs' ability to directly obscure the threat creation process or assist humans in doing so.

Relevant Literature:

- Anthropic – Measuring Progress on Scalable Oversight for Large Language Models
- Apollo Research – Large Language Models can Strategically Deceive their Users when Put Under Pressure.

BIODESIGN TOOLS RISK ASSESSMENT

LLMs may increase the risk of bioweapons development by either directly interacting with Biodesign Tools (BDTs) or facilitating human use of BDT. This can advance R&D efforts and increase the lethality, transmissibility, or 'strategic targeting' of biological weapons.

Research Objectives: Benchmarks and uplift studies to evaluate risks from LLM interaction with BDTs.

Relevant Literature:

- CLTR – Capability-Based Risk Assessment for AI-Enabled Biological Tools
- OpenAI – Building an early warning system for LLM-aided biological threat creation

RESEARCH ASSISTANT CAPABILITY EVALUATION

LLMs demonstrate significant potential as research assistants in biological sciences, offering capabilities that could accelerate legitimate medical research and drug development. However, these same capabilities—particularly in research synthesis, experimental design, and protocol optimization—require careful evaluation for potential misuse.

Research Objectives: Evaluate LLMs' ability to assist in biological misuse via synthesizing research, generating ideas, troubleshooting protocols, and other means.

Relevant Literature:

- RAND – The Operational Risks of AI in Large-Scale Biological Attacks
- CLTR – Why we recommend risk assessments over evaluations for AI-enabled biological tools

PATHOGEN ACQUISITION EVALS

LLMs may possess the knowledge to circumvent control measures and access pandemic-potential viruses.

Research Objectives: Benchmark and uplift studies to evaluate LLMs' knowledge of 1) Pathogen storage locations, 2) Lab security measures, and 3) Methods to circumvent restrictions on controlled substances.

UNLEARNING HAZARDOUS INFORMATION FROM MODEL WEIGHTS

AI developers could aim to remove hazardous information about biosecurity threats from a model's weights so that the model is incapable of assisting in biological misuse. Recent research has worked towards this goal, but existing methods for unlearning are typically vulnerable to adversarial prompting and fine-tuning attacks, which allow users to access knowledge that was supposed to have been unlearned.

Research Objective: Develop and evaluate methods for removing knowledge from models that pose biosecurity risks that are resistant to adversarial prompting and fine-tuning.

Relevant Literature:

- The WMDP Benchmark: Measuring and Reducing Malicious Use With Unlearning
- Do Unlearning Methods Really Remove Information From Model Weights?

TAMPER RESISTANCE FOR OPEN-WEIGHT MODELS

Releasing the weights of an AI system allows users to customize their models. Because of this, it is possible that bad actors may tune and deploy models in ways that can facilitate harmful objectives.

Research Objective: Develop tamper-resistant models with biosecurity guardrails that cannot be easily bypassed.

Relevant Literature:

- Tamper-Resistant Safeguards for Open-Weight LLMs

AISF Grantmaking

The AISF plans to fund research projects by academic labs, non-profits, independent researchers, and for-profit mission-driven entities across both Biosecurity and Cybersecurity topics in the range of $350-$600K. Our initial target is to fund 8-10 projects but we will consider increasing this based on the quality of proposals received.

Based on our recommendations, we may share particularly strong applications with other philanthropists interested in exploring grant opportunities. Please indicate whether you permit us to share your materials with other potential funders in your application.

Eligible Proposal Types and Applicants

- Technical research projects focused on evaluating and improving AI safety in biological applications, as described above.
- Projects must focus on frontier AI models, their applications, or relevant tools, such as BDTs.
- The research duration must be one year or less, and the budget must not exceed $600k.
- Eligibility with the AISF's Conflict of Interest Policy.
- Applicants must review and confirm their ability to sign the grant agreement if their application is successful. A template of the grant agreement can be accessed here.

The AISF is independent of its funders. Critical views of the AISF funders will not preclude research proposals from being awarded funds.

Evaluation Criteria

Below is an outline of our grant evaluators' evaluation criteria for assessing the proposals.

Criteria	Description
Impact	Research proposals will be assessed based on their potential to improve safety measures in AI-bio applications. This includes the practical applicability of the expected results and their potential for implementation in real-world settings.
Feasibility	The proposed project should include a clear timeline with well-defined milestones. The proposal should address potential challenges and include strategies for addressing them.
Relevance	The proposed research must directly apply to frontier AI models and their deployment in biological contexts. The proposal should cover existing research and how it relates to their project.
Peer Review	The proposal must include a robust plan for engaging with the broader research community and receiving feedback. The proposal should demonstrate how peer feedback will be incorporated into the research process and how the broader scientific community will validate findings.
Technical Qualifications	The evaluation will consider the team's AI safety and biosecurity track record. Proposals should include the applicants' academic degrees, previous publications, projects, and contributions to the field. We're open to applicants without such track records if the project is particularly well-scoped and promising. Especially in this case, having named advisors on the project with relevant subject matter expertise and research experience can be helpful.
Ethics	Proposals must outline specific safety protocols that address both immediate research risks and potential downstream implications of the findings. This should detail how sensitive data and results will be handled, secured, and accessed throughout the project lifecycle. The proposal must also include a clear protocol for identifying and managing security-sensitive findings, particularly any unexpected discoveries that may emerge during the research process. Additionally, proposals should demonstrate an ethical approach to all research methodologies, avoiding any practices that may inadvertently mislead or compromise collaborators, such as external CROs or cloud laboratories, without their informed consent.
Equity	Proposals should describe how the project will advance equity and diversity in the research community, particularly regarding underserved populations.
Accessibility	The research product should prioritize open accessibility through open-source licensing, promoting transparency and broad utility. However, if unrestricted access poses a risk of harm or compromises privacy, proposals should provide a justification for limited access. Evaluators will assess the proposal's approach to balancing accessibility with safety and security considerations.

Timeline

- Request for Proposals Opens: November 18, 2024
- Question Deadline: November 25, 2024
- Answers Posted: December 9, 2024
- Proposals Due: January 20, 2025

Submission Process

Proposals can be submitted through the grant portal, accessible on the AISF website.

AI Safety Fund Biosecurity and Cybersecurity Q&A

Published 9 December 2024

General Questions

Q1. I am currently in the process of founding my organization, and it is not yet incorporated. Can I still apply for funding? At the moment, I am not able to create an account in the grantee portal without a Tax ID Number.

Applicants that do not have a Tax ID Number can still apply for funding. A unique ID number is required to register in the FLUXX application portal. In place of a Tax ID Number, please enter "P" and your phone number. The Tax ID Number can be updated once it has been received.

As an alternative, if your organization is being established as an independent nonprofit organization, using a fiscal sponsor might be a practical solution.

Q2. Can a proposal be multi-PI?

Yes, proposals can include multiple PIs. Please designate a lead PI on your application, and list collaborators as Partners in your application. You can add as many Partners as needed for your research team.

Q3. Can a proposal cover more than one topic listed in the RFP?

Proposals can address one or more of the subtopics outlined in the RFP; we will also accept proposals that cover other relevant areas of research addressing AI safety risks in Biosecurity or Cybersecurity.

Q4. Does the $600k budget limit include indirect costs, or is it only for direct costs?

All costs (direct and indirect) listed in the budget associated with the proposed research should not exceed $600k. Please review the AISF Indirect Costs Policy and the AISF Capital Expense Policy for more information about budget requirements.

Q5. Are you open to backing prize challenges like the ML Model Attribution Challenge 2 (mlmac.io), aimed at attributing AI agents?

Eligible candidates for funding from the AISF include independent researchers affiliated with academic institutions, research institutions, NGOs, and social enterprises across the globe that aim to promote the safe and responsible development of frontier models by testing, evaluating, and/or addressing safety and security risks. The AISF does not provide funding for management of, or regranting under challenges, fellowship programs, training and development programs, or similar initiatives.

Q6. Will it be OK to have industrial partners get involved in this proposal and will they be given funding directly? In other words, would sub-contracting be allowed?

Applicants can include partnerships in their proposals with for profit or non-profit entities to accomplish research outcomes. The AISF will take into consideration each proposal on a case-by-case basis to evaluate the nature of proposed partnerships and may request additional information during the evaluation period to understand the nature and benefit of proposed partnership arrangements. Proposed subcontractors must be included in the proposal and budget as Partners with explanation of their role and contributions to project outcomes. Any subcontracting, outside of what is proposed in a grant application, will require Meridian's prior written consent to engage any person or entity to perform any part of the Deliverables for the project. Applicants should review the Grantee Contract Template referenced in the RFP for further clarification.

Q7. Regarding the Grantee Budget AISF form: for the Budget Narrative section, should applicants provide a detailed Cost Justification?

Detailed cost justification is not required. Applicants are encouraged to provide sufficient detail in the budget narrative to address assumptions and reduce the need for clarifying questions during the proposal evaluation process.

Q8. Can an organization submit multiple proposals?

Yes, applicants can submit multiple proposals.

Q9. Is AISF specifically looking for proposals such that all of the work products will be distributed to AI Labs, researchers, AISIs, 3rd party organizations, and the public? Or, if it is acceptable for proposals that are intended for only a subset of those entities, which subsets are "fair game"?

The AISF is interested in advancing the science of AI safety broadly, so by default we would assume all research products will be suitable for public dissemination unless there are legitimate information hazards. Furthermore, the AISF will not fund research for consumption by just one lab/entity.

Q10. The submission website asks for contact information (phone, email, etc.) about our institution (university). Shall we leave the contact of the grant office there, or just general department/college contact information? There is also a checkbox for "Individual Applicant"

in the application form. As university professors, shall we apply "on behalf of an organization" or as individuals?

When applicants register in the FLUXX application system, they should register as the PI, and include contact information for the primary point of contact for the proposal. During registration, applicants should list the organization that would be the recipient of funding. The "Individual Applicant" checkbox is for individual researchers not tied to any organization. An "Individual Applicant" would receive and manage the funding.

Q11. Is the budget a factor when considering our proposal? Our proposal will include three faculty members with complementary expertise, and we might request $400k - $500k as the total budget (about $150k each person). Will that be considered a "high range" and decrease the chance of acceptance?

As long as the proposed budget falls within the target range specified in the RFP, it will not be a primary factor in funding decisions. Proposals that meet the eligibility criteria will be evaluated primarily based on the proposal's merit and feasibility.

Q12. Can you confirm if overheads/indirects are an eligible cost on this grant?

The AISF will consider a maximum indirect cost rate of 20% of the total direct costs. This cap ensures that a significant portion of the funding is allocated directly to project activities and outcomes. For more information, please review the AISF Indirect Cost Policy.

Q13. Is there any additional opportunity for submitting additional questions?

The question-and-answer period is closed for the Cybersecurity and Biosecurity RFPs. Additional questions can be submitted to the AISF (AIsafetyfund@meridprime.org), however we cannot guarantee a response to questions received outside of the Q&A period. If a response is provided, the AISF will include an update to responses posted on the website for all applicants to view.

If another RFP is released, applicants are welcome to submit general questions as well as questions related to the scope of a new RFP.

Cybersecurity

Q14. My organization is building AI-enabled cyberdefense tooling to improve security at frontier AI labs. Is this in scope for this RFP?

Yes, this is in scope for the Cybersecurity RFP as it relates to the core objective of "evaluating and improving the safe deployment of AI in cybersecurity contexts." The proposal may be relevant under a few subtopics. For example, it may relate to "uplift studies" if the proposed research investigates how the AI-enabled tools improve defender performance. Or, it may be suitable under "interdisciplinary testing" if the tooling focuses on defense against human-driven threats such as phishing or social engineering.

Q15. Our proposal will study the offensive capability of novel AI systems, following the "realistic evaluations of AI cyberoffense" topic in the RFP. Since the project duration is one year, we might not have sufficient time to study how to defend against our novel offense, and our project may focus only on offense. Will that lead to any ethical concerns during the proposal review since our novel offense may (theoretically) cause damage or harm without known defense?

It is not disqualifying if the research only addresses the offensive capabilities of novel AI systems. We are interested in funding research that advances the field.

Applicants should consider how they will ensure responsible conduct of the proposed research, particularly when it comes to handling potentially hazardous information discovered during the project. If the research findings do carry significant risks, applicants should explain how they will assess withholding of its publication.

Q16. Do the "novel security vulnerabilities" mentioned under "realistic evaluations of AI Cyberoffense" topic include vulnerabilities of AI models in cyberspace? If we submit a proposal on exploiting the vulnerability of AI systems, rather than using AI systems for offense, will that be out-of-scope?

In general, the AISF is happy to accept proposals for research that is outside the specific research objectives outlined in the Cybersecurity RFP. The same is true for the Biosecurity RFP. As long as a proposal supports the overarching goal of the RFP, evaluating and enhancing the safe deployment of AI in cybersecurity contexts, we will consider it. Applicants should review and address the AISF ethics criteria, especially where research involves exploiting vulnerabilities in proprietary frontier models. Specifically, “proposals should demonstrate an ethical approach to all research methodologies, avoiding any practices that may inadvertently mislead or compromise collaborators without their informed consent.” Researchers should not endeavor to “attack” an AI system without the consent of the frontier lab.

Q17. Our project focuses on forecasting implementation timelines for state-actor level (SL5) security measures, driven by both the increasing offensive capabilities of AI systems and their growing value as targets. While your RFP's forecasting category emphasizes threat landscape changes, would you consider forecasting critical security measure implementation timelines as within scope, given these dual pressures?

In general, the AISF is happy to accept proposals for research that is outside the specific research objectives outlined in the Cybersecurity RFP. The same is true for the Biosecurity RFP. As long as a proposal supports the overarching goal of the RFP, evaluating and enhancing the safe deployment of AI in cybersecurity contexts, we will consider it.

Q18. Our project may include components from more than one topic listed on the RFP. For example, we may build the AI offense system with a human interface so our study will also be relevant to the "uplift studies" topic. Do you want us to focus on one topic only during the short one-year period, or is a combination of multiple topics also encouraged?

Applicants should not feel constrained to a single research objective outlined in the RFP. We welcome all proposals that fit the RFP's goal of evaluating and improving the safe deployment of AI in cybersecurity contexts. The same is true for the Biosecurity RFP.

Biosecurity

Q19. My proposal relates to biomedical research but also relates to data and AI safety, which can relate to Cyber Security as well. Would it be OK for me to submit via the route of Biosecurity if my research relates to both Biosecurity and Cybersecurity?

Applicants should submit proposals under one domain. In this case, submitting under the Biosecurity RFP will ensure that the proposal is assigned to a suitable expert for evaluation.

Q20. To what extent would AISF like to see coverage of material that is clearly hazardous? If such material is included, is it incumbent upon the proposers themselves to outline procedures for safe distribution of work output to relevant users?

It is incumbent on applicants to demonstrate that they have a keen awareness of the implications of their research and have taken into consideration safety measures to mitigate harm from any potentially hazardous information or ethical harms that result from their work. The Frontier Model Forum (the FMF), a partner of the AISF, is developing policies and guidelines for safe distribution of information. We expect the policy and guidance to be finalized prior to the completion of any research funded by the AISF for the Biosecurity and Cybersecurity RFPs and will advise grantees to manage research outcomes under the advice of the FMF.

SUBGRANTEE AGREEMENT

This SUBGRANTEE AGREEMENT (hereafter referred to as this "Agreement"), dated as of XXXXX, is between Meridian Prime, ("Meridian" or "Grantee"), a tax exempt 501(c)(3) organization, with its principal place of business at 323 W Main Street, Suite 202, Frisco, Colorado 80443, United States of America, and XXXXX ("Subgrantee"), an individual or organization doing business at XXXXX. Together, Meridian and XXXXX are referred to as "the Parties." The primary contact for Meridian for this Agreement is: jrichards@meridprime.org and the primary contact for Subgrantee is: XXXXX, XXXXX@XXXX.XXX.

The following Attachments to this Subgrantee Agreement are incorporated fully herein and made part of this Agreement:

Attachment A: Subgrantee Deliverables
Attachment B: Due Diligence Self Reporting Form
Attachment C: Code of Ethics

Meridian and Subgrantee agree as follows:

1. DELIVERABLES

1.1 **Description of Deliverables**. Subgrantee agrees to produce the deliverables as set forth Attachment A (the "Deliverables").

2. SUBGRANTEE'S RESPONSIBILITIES

2.1 **Standards.** Subgrantee warrants and covenants that it will develop the Deliverables in a thorough and professional manner and with the highest ethical standards.

2.2 **Liability for Losses; Indemnity.** Subgrantee agrees to be liable for and defend (at Meridian's election), indemnify and hold harmless, Meridian and their respective directors, officers, employees and agents, and each of them, for, from and against all Losses (as defined below), except to the extent that the Loss results from the negligent acts or willful misconduct of Meridian, its officers, employees or agents. "Loss" means any liability, claim, demand, damage, loss, fine, penalty, cause of action, suit or cost, of any kind or description, including, but not limited to, judgments, liens, expenses (including, but not limited to, court costs, attorneys' fees, costs of investigation, removal and remediation and governmental oversight costs) and amounts agreed upon in settlement, caused by, arising out of, resulting from, attributable to or in any way incidental to the development of the Deliverables, this Agreement, or both, including, but not limited to, all claims that the Meridian's use of the Deliverables, or any portion of the Deliverables, infringes or violates any patent, copyright, trade secret, trademark or other third-party intellectual property right.

2.3 **Intellectual Property Rights and Licenses**.

All research results and grant Deliverables funded by the Project will be intended for the public's benefit. **Plans for public circulation of research results and deliverables must be submitted to Meridian Prime in advance of any information release. Such plans must include recommendations and rationale to withhold any information and specific justifications for same, including any potential national security issues.** Appropriate methodological details and scientific findings will be made freely available and searchable by major internet search engines. Results that are not published will be made freely available upon request to any organization with a track record of working on AI safety or security, including model-developers, research organizations, academic institutions, or government agencies. Any data created with subgrant funds will be made freely available upon request to any organization with a track record of working on AI safety or security, including model-developers, research organizations, academic institutions, or government agencies, subject to privacy laws and export restrictions. However, Meridian reserves the right to withhold any information from disclosure that has been identified by Subgrantee, in collaboration with Meridian, to be highly sensitive and poses significant societal risks, including U.S. national security risks.

If this subgrant results in the creation of intellectual property, Subgrantee agrees to place (i) any code or other inventions under the Apache 2.0 license (https://opensource.org/licenses/Apache-2.0), and (ii) any other intellectual property (e.g. creative works that are not code, or patentable) under the CC-BY 4.0 International license (https://creativecommons.org/licenses/by/4.0/), each within three (3) months of the date of creation. For any intellectual property rights (including patent and trade secret rights) not licensed by the Subgrantee under one of the above licenses, the Subgrantee will place such intellectual property in the public domain. Subgrantee will not file any patent applications in connection with any intellectual property created with Project funds.

Subgrantee's work may result in the development of software code related to AI safety, but such work is not expected to be a significant outcome of the Deliverables.

2.4 **Insurance**. Meridian will not provide Workers' Compensation insurance, Employer's Liability insurance, Commercial General Liability insurance, Automobile Liability insurance or any other insurance to Subgrantee. Subgrantee is solely responsible, at its expense, for procuring and maintaining insurance in amounts required by applicable law.

2.5 **Contractors/Other Parties.** Subgrantee may not, without Meridian's prior written consent in each instance, engage any person or entity to perform any part of the Deliverables, other than those outlined in the approved proposal and budget.

2.6 **Compliance with Laws, Data Security, and Privacy**. Subgrantee will comply, and will cause its employees and agents to comply, with all applicable laws, rules, ordinances, codes, and regulations. Subgrantee will, at its expense, acquire and maintain all licenses or permits required for the performance of the Deliverables prior to commencing the activity for which a license or permit is required. In addition, Subgrantee is responsible for maintaining data privacy and security and complying with all applicable laws. Subgrantee is solely responsible for complying with any privacy laws, whether foreign or domestic. Subgrantee further acknowledges that Meridian has no control over or access to the data that is used to produce the Deliverables.

2.7 **Records**. Subgrantee will maintain detailed records of all matters that relate in any way to the Deliverables, all in form, format, and media acceptable to Meridian (the "Records"). During the term of this Agreement and for a minimum period of four (4) years after its expiration or termination, Meridian will have

the right to copy and audit the Records during Subgrantee's regular business hours or, at Meridian's request and expense, Subgrantee will make copies of the Records and provide them to Meridian, regardless of whether such Records are created before or after the expiration or termination of this Agreement.

2.8 **Permissions.** By entering into this Agreement, Subgrantee represents that it has either received necessary permissions or has reasonable assurances that any permissions necessary to carry-out the Deliverables will be granted.

3. TAXES

Subgrantee is solely responsible for paying taxes, if any, associated with the Agreement and any grant funds disbursed hereunder.

4. MERIDIAN'S RESPONSIBILITIES

4.1 **Indemnity**. To the fullest extent the law allows, Meridian will defend, indemnify and hold harmless Subgrantee for, from and against all liability, losses, damages, claims, liens, privileges, charges and expenses, including reasonable attorneys' fees caused by or resulting from: (i) Meridian's breach of its obligations under this Agreement; or (ii) any claims by the Funders or any third party (including, without limitation, other Subgrantees of Meridian) solely to the extent Meridian has directly caused the claim.

4.2 **Out-of-Pocket Expenses**. Subgrantee may use grant funds for reasonable travel related expenses actually incurred by Subgrantee in connection with the performance of Deliverables. Budgets for allowable expenses must be included in the approved budget, in advance, by Meridian.

5. DEFECTIVE OR DEFICIENT DELIVERABLES

If the performance of the Deliverables is defective or deficient or Subgrantee otherwise fails to develop the Deliverables in accordance with this Agreement, Meridian may suspend future payments otherwise scheduled to Subgrantee until Subgrantee corrects the defect to Meridian's satisfaction. If Subgrantee fails to cure the defective performance within 30 days of written notice, Meridian may terminate this subgrant and request repayment of any unexpended funds.

6. CONFIDENTIAL INFORMATION

6.1 **Non-Disclosure**. Both Parties acknowledge that each Party owns valuable trade secrets and other confidential information and possesses similar information that is licensed from third parties. The Parties will treat as strictly confidential and will not use for its own or third parties' purposes, or divulge or permit to be divulged to or examined or copied by others, any information and data that such party obtains in connection with this Agreement or otherwise that: (i) are confidential or proprietary; (ii) relate to the operations, policies, procedures, techniques, accounts or personnel; or (iii) are confidential or proprietary to a third party (including, but not limited to, the Funders). In addition, each party will keep confidential the existence and contents of this Agreement. If either Party breaches or threatens to breach any of the provisions of this Section in addition to any other rights and remedies available at law, in equity or under this Agreement, the other Party

will be entitled to an injunction restraining the breach or threatened breach without having to prove actual damages or threatened irreparable harm and without the necessity of posting a bond.

6.2 **Use of Name and Publicity.** Neither Party will, without the prior written consent of the other Party in each instance, use in advertising, publicity or otherwise, the name of Subgrantee or Meridian, the names of any personnel of Meridian or any trade name, trademark or logo owned by Meridian, except Meridian reserves the right to use Subgrantees name in any reporting or general description of the project.

7. MODIFICATION AND TERMINATION

7.1 **Modification**. This Agreement may be modified only in writing and by mutual agreement of the Parties.

7.2 **Termination for Convenience.** Meridian has the right to terminate this Agreement without cause with 30 days advance written notice to Subgrantee. In the case of termination for convenience, Meridian agrees to compensate Subgrantee the amount due to Subgrantee through the date of the termination notice, provided that the Subgrantee: (i) submits to Meridian a properly prepared invoice within 30 days after the effective date of termination; (ii) stops all Services to the extent specified in the notice and incurs no further expenses beyond those authorized in the notice; and (iii) satisfactorily performs the portion of Deliverables for which Subgrantee invoices. Subgrantee waives all claims for compensation or charges (including any claim for lost profits), beyond that to which it may be entitled under this Section 7.2 as a result of any termination. Subgrantee agrees that its sole remedy in connection with any termination will be to receive compensation in accordance with this section.

7.3 **Termination for Cause.** Meridian may terminate in writing this Agreement for material breach. In the case of termination for cause, Meridian will only compensate Subgrantee for work that Meridian, in its sole discretion, determines meets the quality standards and the statement of work as set forth in Attachment A.

8. DISCLAIMERS, ACKNOWLEDGEMENT AND PROPRIETARY RIGHTS

8.1 **Cooperation**. Subgrantee will cooperate fully in disclosing to Meridian all work product related to the Deliverables.

8.2 **Title; Return of Documents**. Title to all materials and documentation that Meridian furnishes to Subgrantee will remain in Meridian. Subgrantee will deliver to Meridian all work product related to the Deliverables, on whatever media rendered, on the first to occur of: (i) Meridian's request or (ii) termination of this Agreement.

9. LIMITATION OF LIABILITY

Except for Meridian's indemnification obligations set forth in Section 4.1 of this Agreement, Meridian will not be liable for any loss, injury or damage to the person or property of Subgrantee, its agents, employees, or representatives, arising out of or in connection with the Deliverables or any incidental activities or travel.

Meridian will not be liable to Subgrantee, its agents, employees or representatives, for any punitive, exemplary, special, indirect, incidental or consequential damages (including, but not limited to, lost profits, lost business opportunities, loss of use or equipment down time, and loss of or corruption to data) arising out of or relating to this Agreement, regardless of the legal theory under which Subgrantee seeks those damages, and even if the Parties have been advised of the possibility of those damages or loss.

10. SPECIFIC LAWS

10.1 **Political Campaign/Lobbying Activity**. Subgrantee will not use any amounts received under this Agreement to influence the outcome of any election for public office or to carry on any voter registration drive. Subgrantee represents and warrants that Subgrantee is not a party to any agreement, oral or written, permitting any of the amounts received under this Agreement to be directed to or earmarked for lobbying activity or other attempts to influence local, state, federal or foreign legislation. Subgrantee agrees to comply with lobbying, gift, and ethics rules applicable to the Deliverables under local, state, federal or foreign law.

10.2 **Compliance with Anti-Corruption Laws**. Subgrantee represents and warrants that it is in compliance with all applicable anti-corruption laws, and that it has not taken, and will not take, any action that would cause Meridian to violate any anti-corruption law including, but not limited to, the Foreign Corrupt Practices Act of 1977 (FCPA), United Nations Convention Against Corruption and any implementing laws of the United States or any similar applicable statutes or regulations, including the United States Foreign Corrupt Practices Act and the U.K. Bribery Act 2010; and local anti-corruption laws in the jurisdictions in which Subgrantee performs any Deliverables. Without limiting the foregoing, Subgrantee warrants that it and its employees, agents and representatives have not and will not, directly or indirectly, offer, pay, give promise or authorize the payment of any money, gift or anything of value to:

a. Without limiting the foregoing, Subgrantee warrants that it and its employees, agents and representatives have not and will not, directly or indirectly, offer, pay, give promise or authorize the payment of any money, gift or anything of value to:
    i. any Government Official (defined as any officer, employee or person acting in an official capacity for any government department, agency or instrumentality, including state-owned or controlled companies, and public international organizations, as well as a political party or official of a political party or candidate for political office) or official to commit or omit to commit any act in violation of his or her lawful duty; or to obtain or retain business for, or direct business to any individual or entity. Under no circumstances shall any payments or anything of value be given, made, promised or offered to any U.S. federal, state or local employee or official, or

    ii. any person while Subgrantee knows or has reason to know that all or a portion of the money, gift or thing of value will be offered, paid or given, directly or indirectly, to any Government Official, for the purpose of:
        - influencing an act or decision of the Government Official in his or her official capacity;
        - inducing the Government Official to do or omit to do any act in violation of the lawful duty of that official;
        - securing an improper advantage; or

- inducing the Government Official to use his influence to affect or influence any act or decision of a government or instrumentality, to assist Meridian in obtaining or retaining business.

b. Subgrantee agrees that should it learn or have reason to know of any payment or transfer (or any offer or promise to pay or transfer) that would violate applicable anti-corruption laws, it will immediately disclose it to Meridian.

10.3 OFAC Compliance. "OFAC" means the Office of Foreign Assets Control of the U.S. Department of the Treasury, which administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted individuals, organizations, and foreign countries and regimes.

"OFAC List" means the Specially Designated Nationals and Blocked Persons List and any other lists administered or enforced by OFAC, published by OFAC and available at http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx or any official successor website.

"OFAC Regulations" means (a) the rules and regulations promulgated by OFAC, as may be published in Chapter 31, Part 500 of the Code of Federal Regulations from time to time, and (b) any Executive orders administering or imposing economic sanctions on individuals, organizations or foreign countries and regimes.

As of the date hereof, and at all times during the Agreement Term, Subgrantee agrees that it has not, shall not, and shall ensure that none of its directors, officers, employees, affiliates, agents, or persons acting on its behalf will, directly or indirectly, use, lend, make payments of, contribute or otherwise make available, all or any part of the Agreement funds to fund any activities (i) involving or for the benefit of any person included in any OFAC List or otherwise subject to sanctions under OFAC Regulations, (ii) that could result in any person (including Meridian and the Funders) being in breach of OFAC Regulations, becoming included in any OFAC List, or otherwise becoming subject to sanctions under OFAC Regulations, or (iii) that could be considered a "prohibited transaction" (defined by OFAC as trade or financial transactions and other dealings in which U.S. persons may not engage unless authorized by OFAC or expressly exempted by statute). Subgrantee hereby expressly binds itself to include this provision in all subcontracts and sub-grants issued under this Agreement.

10.4 Anti-Terrorism. Subgrantee confirms that it is familiar with the U.S. Executive Orders and laws, similar laws of the U.K. and EU, prohibiting the provision of resources and support to individuals and organizations associated with terrorism, and the terrorist-related lists promulgated by the U.S. Government. Subgrantee will use reasonable efforts to ensure that it does not support or promote terrorist activity or related training, or money laundering.

10.5 Export Compliance. Subgrantee will comply with all applicable laws and regulations, including U.S. export laws and regulations relating to the import or export of any technical data contemplated under this Agreement, subject to the Export Administration Regulations (EAR, 15 CFR 730-774). Subgrantee represents and warrants that it will not transfer any technical data directly or indirectly to any individual, company or other entity without first complying with all requirements of the International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130) and the EAR, including the requirements for obtaining any export license, if applicable. Furthermore, Subgrantee will first obtain the written consent of Meridian before submitting any

request for authority to export or transfer any technical data. Technical data that is controlled by the ITAR or the EAR will not be released to foreign individuals, companies, or other entities, whether within or outside the U.S., by a U.S. person unless the U.S. person obtains, in advance of the transfer or export, the appropriate export license or other approval from the U.S. Government. This requirement for prior U.S. Government authorization applies to the return, to the country of origin, of foreign origin technical data that incorporates any U.S. origin technical know-how, content, improvements, or other design modifications.

10.5 Ethics. Meridian Institute is committed to upholding the highest standards of ethics and requires all subgrantees to adhere as a condition of funding to its Code of Business Conduct and Ethics. By signing this Agreement, Subgrantee acknowledges that they will comply with **Meridian Prime's Business Code of Conduct and Ethics,** which is included below.

11. MISCELLANEOUS

11.1 Binding Agreement; No Assignment. Subgrantee may not assign or transfer any interest in or obligation under this Agreement without the prior written consent of Meridian.

11.2 Qualification and Independence of Subgrantee. In performing and carrying out the Deliverables, Subgrantee agrees that it is an independent Subgrantee and not an agent or employee of Meridian. Subgrantee has represented itself as an expert with respect to the performance and completion of the Deliverables.

11.3 Integration. This Agreement constitutes the entire agreement between the Parties relating to its subject matter, and there are no agreements or understandings between the Parties, express or implied, unless explicitly set forth in this Agreement.

11.4 Governing Law and Language. The laws of the State of Colorado, United States of America, will govern the enforcement and interpretation of this Agreement. Subgrantee agrees that, at Meridian's election, all actions and proceedings arising from or related to this Agreement will be litigated in local, state, or federal courts located within the City of Denver, State of Colorado, United States of America. Subgrantee consents and submits to the personal jurisdiction and venue of those courts. English shall be the official language of this Agreement and the official language used for litigation.

11.5 Invalidity; Unenforceability. If any portion of this Agreement is declared to be invalid or unenforceable, the declaration will not affect the validity or enforceability of the remainder of this Agreement, which will be construed as nearly as possible as if the invalidity or unenforceability had not been declared. If the scope of any restriction or obligation is too broad to permit enforcement to its full extent, then that restriction or obligation will be enforced to the maximum extent permitted by applicable law, and Subgrantee consents and agrees that the scope and reach of those restrictions and obligations may be judicially modified in any proceedings brought to enforce them.

11.6 Waivers. No waiver of any provision of this Agreement, waiver of any default under this Agreement or failure to insist on strict performance under this Agreement will affect the right of Meridian or Subgrantee to enforce that provision or to exercise any right or remedy if there is a further default, whether or not similar.

11.7 Notices and Invoices. All notices provided for or required under this Agreement will be in writing to the applicable party at Meridian Prime, P.O. Box 1829, Dillon, Colorado 80435. Subgrantee will submit all invoices to Meridian electronically at the following: wdottavio@meridprime.org. All invoices and notices will

be considered given when received. Either party may, from time to time and in accordance with the procedures set forth in this Section 11.7, specify a different address for receipt of notices or invoices.

11.8 Force Majeure.

- Neither Party to this Agreement shall be liable to the other Party for any cancellation, delay, or omission in the performance of any part of this agreement occasioned by any incidence of force majeure.
- For the purpose of this Agreement, force majeure includes those forces beyond the control of the Parties that would render performance impractical, illegal, or impossible to perform, such as, but not limited to, Acts of God, laws and regulatory requirements, war, or riots.

.

11.9 Counterparts. The Parties may execute this Agreement in counterparts, including by facsimile or electronic transmission, all of which together will be treated as one and the same instrument.

11.10 Code of Business Ethics and Conduct. Subgrantees are expected to comply with all laws and maintain high ethical standards, including complying with Meridian's Code of Business Conduct and Ethics ("Code"). By signing this Agreement, Subgrantee agrees you have read and will comply with the Code. Failure to do so is grounds for Agreement termination.

11.11 Red Flag Reporting. As part of Meridian's ongoing commitment to proactively maintain the highest standards of ethical and safe practices in our organization, Meridian Institute uses the Red Flag Reporting platform, which has been designed specifically for contractors and vendors to report any concerns related to unethical or unsafe practices that they may encounter in their interactions with Meridian. Meridian believes that this will empower our contractors and vendors to contribute positively to our ethical standards and help us maintain a safe and respectful organizational environment.

Red Flag Reporting is an independent hotline services for reporting unethical or unsafe behavior. You can access this service at Meridian Vendor Case (redflagreporting.com). Meridian encourages you to use this platform should you have any concerns that you wish to bring to our attention. Please rest assured that all reports will be treated with the utmost confidentiality and professionalism.

11.12 Survival. The provisions of Sections 1.2, 1.3, 2.3, 3, 4, 5, 6, 7.2, 8, 9, 10 and 11 will survive the termination of this Agreement and Subgrantee's completion of the Deliverables.

11.13 Authority. Subgrantee warrants that it has the full legal right, power, and authority to enter into this Agreement and perform the obligations set forth herein and when executed and delivered by Subgrantee, this Agreement will constitute the legal, valid, and binding obligation of Subgrantee, enforceable against Subgrantee in accordance with its terms.

11.14 Offer Expiration. The subgrant award must be executed within 30 business days (i.e., excluding weekends and U.S. holidays) of transmittal by the AI Safety Fund. After 30 business days, the subgrant offer expires and is void. The substantive terms in this Agreement are non-negotiable.

ACKNOWLEDGED AND AGREED:

MERIDIAN PRIME

By: _____

Print Name: _____

Title: _____

Date: _____

SUBGRANTEE

By: _____

Print Name: _____

Title: _____

Date: _____

Attachment A: Subgrantee Deliverables

1.0 Scope of Work

1.1 Title: XXXXX (XXXXX.00)

1.2 Purchase Order Number: XXX-MP-XXX

1.3 Period of Performance: *date* to *date*

1.4 Agreement Value: [insert per budget]

1.5 Project Indirect Costs: Indirect costs will not exceed 20%.

1.6 Meridian Project Director: Molly Mayo, mmayo@meridprime.org.

***1.7* Deliverables: [set forth deliverables here]**

1.7 Due Diligence: Subgrantee is required to conduct "due diligence" when entering into any agreement, contract, or purchase order. Subgrantee must confirm that due diligence has been conducted using the standards below to verify any mitigation of risk and to satisfy due diligence requirements. Subgrantee will continue to monitor the standards below throughout the life of the project and report any risks or issues that arise to Meridian as soon as possible.

Due diligence requirements you are expected to monitor and ensure is:

- Formal Identification (confirmation of registration/incorporation)
- Compliance with applicable laws as well as insurance and health and safety regulations
- Government Relationships (declaring instances where the Organization principal(s)/Individual are closely related to a public official)
- Prior Conduct (declaring past instances of criminal, corrupt, unethical, or unlawful cost related to the Organization/Individual or subsidiaries).

2.0 Description of Deliverables

[insert]

3.0 Subgrant Amount and Disbursement Terms:

3.1 Agreement Amount. In consideration of the Services to be performed, Meridian will pay Subgrantee the amount specified in Section 1.4 of the Attachment A of this Subgrantee Agreement.

3.2 Invoicing. Subgrantee shall submit invoices in USD to Meridian for payment based on the above terms and this Attachment. Subgrantee shall submit invoices to Wendy D'Ottavio, WDottavio@meridprime.org.

3.3 Disbursement. Meridian will review invoices that Subgrantee submits and will make payment of the undisputed portion of an invoice within thirty (30) business days of its receipt of the invoice, unless

otherwise specified in Section 3.2 above. Payment of approved invoices will be made by electronic fund transfer (EFT) or wire transfer. Invoices will be paid in the normal course of business, absent any unresolved performance, compliance, or billing issues. Meridian Prime will not be liable to reimburse any currency exchange rate losses and bank charges that may arise as a result of receiving payments in USD.

ACKNOWLEDGED AND AGREED:

MERIDIAN PRIME	SUBGRANTEE
By: _____	By: _____
Print Name: _____	Print Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Meridian Prime Code of Business Conduct and Ethics

CODE OF BUSINESS CONDUCT AND ETHICS FOR MERIDIAN PRIME'S SUBCONSULTANTS, SUBCONTRACTORS, PARTNERS & SUPPLIERS

Meridian Prime ("MP") expects integrity, honesty and ethical law-abiding behavior by all its subconsultants, subcontractors, partners, and suppliers ("SUBs") when they are dealing with MP, MP's clients, MP's other SUBs, or working on MP project-related business. MP requires that its SUBs meet the standards set out in this Code of Business Conduct and Ethics ("Code").

1. **BUSINESS CONDUCT:** SUBs must comply with all applicable statutes, regulations, bylaws, human rights codes and other legal requirements when they are dealing with MP, MP's clients, MP's other SUBs, or working on MP project-related business.

2. **BRIBERY:** A bribe (or "kickback") is the offering, giving, receiving or soliciting of an item of value, service or favor to influence others, or any valuable thing given or promised, or any preferment, advantage, privilege, given or promised corruptly or against the law, as an inducement to any person acting in an official capacity to violate or forbear from their duty, or to improperly influence their behavior in the performance of such duty. When performing business with, for or on behalf of MP, SUBs are forbidden, under any circumstances, from paying a bribe to, or receiving a bribe from any third party. SUBs must immediately report any knowledge of any bribery, or attempted bribery or inappropriate transactions to MP.

3. **WORKING WITH OTHERS:** SUBs will treat everyone in the workplace with proper dignity and respect the health, safety and fundamental human rights of their employees and others working on MP projects. MP SUBs will adhere to the general principles of respect, fairness, and non-discrimination and agree to maintain a workplace that is harassment and bullying free. Under no circumstances will MP SUBs or their business partners employ underage workers or forced labor.

4. **WORKING WITH SECONDARY SUPPLIERS:** MP requires that its SUBs ensure that their own SUBs (secondary suppliers) comply with the standards set out in this Code when they are dealing with MP, MP's clients, MP's other SUBs, or working on MP project-related business. SUBs are expected to select and retain their own SUBs fairly and objectively, based on the quality of service or goods, with proper consideration of cost.

5. **INSIDER TRADING:** SUBs must not divulge or act on any non-public information that could influence the price or trade of MP's client securities. SUBs are prohibited from disclosing such information to any other people, including family and friends. SUBs must disclose in writing to MP, if any of their personnel have any substantial direct or indirect financial relationship or ownership of shares of a publicly traded MP client company.

6. **CONFLICTS OF INTEREST:** The term "conflict of interest" includes any circumstance that could cast doubt on the Sub's ability to act with total objectivity in regard to the supply of materials or services to MP. SUBs will prevent or immediately disclose any possible conflict of interest as soon as possible to MP. SUBs will not engage in any activity that might conflict with or impair the Sub's obligations to MP or MP's clients, including:

    i Personnel of SUBs may not be an owner, director, officer or employee of a business competing with MP.

    ii SUBs will not seek or accept gifts, payments, personal loans, services, or offers of employment or future contracts, which might obligate the Sub to a competitor firm of MP, or those trying to do business with MP.

7. **TRADE SECRETS AND CONFIDENTIALITY:** SUBs are not to reveal any information that might reasonably be considered a trade secret or proprietary information belonging to MP or to MP's clients. SUBs will not divulge any MP confidential information regarding MP operations, projects or relationships with any other MP SUBs, partners, competitors, clients or MP employees.

8. **CLASSIFIED INFORMATION:** When performing business for or on behalf of MP, SUBs are responsible for obtaining valid security clearances when handling classified information and must ensure such information is handled per legal requirements.

9. **DATA AND DATA PRIVACY:** SUBs must comply with all privacy laws related to the processing and protection of data, including as applicable, U.S., European Union and United Kingdom laws and regulations.

10. **FINANCE & ACCOUNTING:** SUBs' invoices and financial statements, and the books or records on which they are based, must accurately reflect all transactions with MP and MP's client. SUBs must not create any false, artificial or misleading statements or accounting entries when conducting business with MP or working on a MP project. SUBs' invoices and financial statements, and the books or records on which they are based, must be prepared in accordance with generally accepted accounting principles. SUBs' business records must be retained in accordance with all applicable laws and regulations. SUBs must honestly and accurately report time worked on each activity as required and must not deliberately misallocate time charges.

11. **COMMUNICATIONS:** SUBs will represent MP and MP's clients in a completely professional and positive manner. SUBs will not make any public statements (including social media comments) regarding MP, MP's clients, or the Sub's business with MP, without written approval from MP.

12. **REMEDY FOR BREACH OF CODE:** If a SUB violates any provision of this Code, it may be subject to investigation and disciplinary action, which may include reprimand, contract suspension or termination of contract. MP will also be entitled to pursue further legal action, including claims for damages, against the SUB.

13. **ENVIRONMENTAL MANAGEMENT:** SUBs are expected to work actively to prevent environmental harm, minimize environmental impact and provide green solutions. SUBs shall make every effort to limit the environmental impact of your business and have in place effective environmental management systems that are appropriate for the nature and scale of your business.

14. **EQUALITY, DIVERSITY & INCLUSION:** MP is committed to promoting equal opportunities to all its employees, customers and supply chain partners and believes it enhances our capability. MP treats all people equally with respect and dignity including those contracting to supply goods or services. MP does not discriminate on the grounds of age, color, disability, ethnicity, gender, marital status, sexual orientation, religion, faith or on any other unjustifiable or illegal grounds. MP expects SUBs appointed for the provision of goods, services or works to demonstrate the same commitment to promoting equal opportunities in how they operate.

15. **HEALTH AND SAFETY:** SUBs will comply with all health and safety requirements for its employees.

16. **DIVERSITY:** SUBs will support opportunities for access and growth of entities owned and controlled by minorities, women, and disabled persons with an emphasis on measurable results and continuous improvement. SUBs will be expected to report on results specifically pertaining to diversity as required by MP.

17. **SPECIFIC LAWS:**

16.1 POLITICAL CAMPAIGN/LOBBYING ACTIVITY. SUBs will not use any amounts received under this Agreement to influence the outcome of any election for public office or to carry on any voter registration drive. SUB represents and warrants that SUB is not a party to any agreement, oral or written, permitting any of the amounts received under this Agreement to be directed to or earmarked for lobbying activity or other attempts to influence local, state, federal or foreign legislation. SUB agrees to comply with lobbying, gift and ethics rules applicable to the Services under local, state, federal or foreign law.

16.2 COMPLIANCE WITH ANTI-CORRUPTION LAWS. SUB represents and warrants that it is in compliance with all applicable anti-corruption laws, and that it has not taken, and will not take, any action that would cause Meridian to violate any anti-corruption law including, but not limited to, the Foreign Corrupt Practices Act of 1977 (FCPA) and local anti-corruption laws in the jurisdictions in which SUBs performs any Services.

A. Without limiting the foregoing, SUB warrants that it and its employees, agents and representatives have not and will not, directly or indirectly, offer, pay, give promise or authorize the payment of any money, gift or anything of value to:

i any Government Official (defined as any officer, employee or person acting in an official capacity for any government department, agency or instrumentality, including state-owned or controlled companies, and public international organizations, as well as a political party or official of a political party or candidate for political office), or

ii any person while SUB knows or has reason to know that all or a portion of the money, gift or thing of value will be offered, paid or given, directly or indirectly, to any Government Official, for the purpose of:

- influencing an act or decision of the Government Official in his or her official capacity;
- inducing the Government Official to do or omit to do any act in violation of the lawful duty of that official;
- securing an improper advantage; or
- inducing the Government Official to use his influence to affect or influence any act or decision of a government or instrumentality, in order to assist Meridian in obtaining or retaining business.

B. SUB agrees that should it learn or have reason to know of any payment or transfer (or any offer or promise to pay or transfer) that would violate applicable anti-corruption laws, it will immediately disclose it to Meridian.

16.3 ANTI-TERRORISM. SUB confirms that it is familiar with the U.S. Executive Orders and laws prohibiting the provision of resources and support to individuals and organizations associated with terrorism and the terrorist-related lists promulgated by the U.S. Government. SUBs will use reasonable efforts to ensure that it does not support or promote terrorist activity or related training, or money laundering.

16.4 EXPORT COMPLIANCE. SUBs will comply with all applicable laws and regulations, including U.S. export laws and regulations relating to the import or export of any technical data contemplated under this Agreement, subject to the Export Administration Regulations (EAR, 15 CFR 730-774). SUBs represents and warrants that it will not transfer any technical data directly or indirectly to any individual, company or other entity without first complying with all requirements of the International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130) and the EAR, including the requirements for obtaining any export license, if applicable. Furthermore, SUBs will first obtain the written consent of Meridian before submitting any request for authority to export or transfer any technical data. Technical data that is controlled by the ITAR or the EAR will not be released to foreign individuals, companies or other entities, whether within or outside the U.S., by a U.S. person unless the U.S. person obtains, in advance of the transfer or export, the appropriate export license or other approval from the U.S. Government. This requirement for prior U.S. Government authorization applies to the return, to the country of origin, of foreign origin technical data that incorporates any U.S. origin technical know-how, content, improvements or other design modifications.

18. **FAIR LABOR STANDARD ACT (FLSA).** The Fair Labor Standards Act (FLSA) establishes minimum wage, overtime pay, recordkeeping, and youth employment standards affecting employees in the private sector and in Federal, State, and local governments. https://www.dol.gov/agencies/whd/flsaAt Meridian Institute, we recognize that our interconnected world is becoming more complex every day. Most of the challenges that shape our future involve people and organizations whose goals may be imperfectly aligned—or even in outright conflict. We help people and organizations solve problems with an innovative approach that brings together three elements.

Attachment C: Code of Ethics

ACKNOWLEDGED AND AGREED:

MERIDIAN PRIME	SUBGRANTEE
By: _____	By: _____
Print Name: _____	Print Name: _____
Title: _____	Title: _____
Date: _____	Date: _____