CINA Annual Request for Proposals, Winter 2024: Submission Guidance

About the CINA RFP

The Criminal Investigations and Network Analysis Center (CINA) is soliciting proposals for research to address current and imminent challenges faced by the U.S. Department of Homeland Security (DHS). This Request for Proposals (RFP) invites submissions that will address key challenges represented by the four research themes of the CINA Center:

- Criminal Network Analysis
- Dynamic Patterns of Criminal Activity
- Forensics (both traditional laboratory forensics and digital forensics)
- Criminal Investigative Processes

CINA is a multidisciplinary academic consortium that brings together leading researchers and experts in pursuit of innovative approaches to disrupt criminal activities across the physical and cyber spaces. Led by George Mason University and sponsored by the DHS Science and Technology Directorate's Office of University Programs (OUP), the Center partners with university researchers and cross-sector collaborators in industry, government, and non-governmental organizations to advance science, while developing innovative solutions and educational and training activities to support the workforce of today and tomorrow.

In keeping with the mission, nature, and authorities of the CINA Center, we expect research proposals under this RFP to produce algorithms, methods, and/or tools that advance the state of the art and that may subsequently be used by DHS, law enforcement, and others to advance their understanding of, and ability to disrupt, criminal network operations. We are also interested in studies and knowledge products that advance the understanding and investigation of criminal network operations, as well as the development and delivery of training to support DHS and law enforcement in combatting transnational organized crime groups. Proposed research must build upon the existing knowledge in a topic area. Proposals that aim primarily to develop software or hardware, or that directly support law enforcement actions as part of the proposed activities, fall outside of the Center's scope. Internal and external subject matter experts will formally review each proposal, and they will evaluate both the proposals' scientific merit and their relevance to DHS.

For more information about the Center and its ongoing research, please visit cina.gmu.edu/projects/.

Eligibility

To be eligible for funding through this RFP, proposals must be led by a Principal Investigator (PI) employed at an institute of higher education. CINA will make awards only to educational institutions; however, proposals may include collaborators not employed by educational institutions, including employees of non-governmental organizations and private industry, as well as independent consultants. Collaborative proposals must clearly indicate the lead PI and institution on the proposal and include a single cohesive workplan.

Estimated Project Funding and Timeline

The anticipated period of performance for proposals funded under this RFP is **July 1, 2024, to June 30, 2025** (CINA Program Year 8). Projects funded under CINA's cooperative agreement with DHS typically range from six to 24 months (two years) in duration, with funding levels that range from US$50,000 to US$250,000 per year depending on project objectives, resources, and anticipated scope. Multi-year proposals are welcome; work plans may describe the work across all years but should focus on year one objectives. Funding after year one is contingent from year to year on progress and performance, DHS stakeholder feedback, and available funding. Projects funded through this RFP will have an anticipated start date between July and September 2024, pending completion of required Institutional Review Board (IRB) and DHS compliance reviews.

Research Data

Permitted data sources for research are **non-DHS data sources and synthetic or simulated data**. No classified data, controlled unclassified information (CUI), sensitive but unclassified (SBU) data, or DHS operational data may be used for research funded under the terms of CINA's cooperative agreement with DHS.

To be considered, proposals must identify anticipated data sources and describe plans to acquire or access the data. Proposals to use third-party data (which may include certain types of publicly available information, including social media) or any other data which may raise privacy concerns are not precluded from funding, but CINA may require time for additional reviews and approvals before making a funding decision. Please review CINA's definition of third-party data in Appendix A.

When proposals are selected for funding, CINA will work with PIs to facilitate the appropriate level of reviews for the data sources in their proposals. **We encourage proposers to include four to eight weeks as funded activities at the start of the project to accommodate these additional reviews**. Proposals advanced to relevancy review with DHS will submit a Data Acquisition and Management Plan outlining plans for acquisition, handling—that is, processing, cleansing, etc.—secure storage, and disposition of data prior to final reviews.

Deadline and Submission Requirements

- Submissions will be accepted through **11:59 PM EST, March 1, 2024.**
- Project information and required attachments must be submitted to CINA's RFP portal at: https://cina.gmu.edu/2024annualrfp. Submissions must include the documents in the specified formats below. Documents may be zipped together for the submission upload but must be individual files (when unzipped) as listed below.

1. **Project workplan, strictly following the provided template:** Must be in Microsoft Word format, should not exceed ten (10) pages in length (excluding references), single-spaced, eleven or twelve-point font with one-inch margins. Appendices beyond ten pages or external links should only be used when necessary to convey a critical aspect of the proposed research. Required template linked here.
2. **Project budget:** Must be in Microsoft Excel format. Sample template provided; institutions may use their own template if it includes a similar level of detail. Multi-year projects should reflect each year's budget in a new column or tab. Sample template linked here.
3. **Budget justification narrative:** Must be in Microsoft Word or PDF. As above, sample template provided; institutions may use their own template if it includes a similar level of detail. Sample template linked here.

4. **CV or bio-sketch for PI and other key personnel:** Must be in Microsoft Word or PDF. CVs should be combined into one file.

Questions

Questions about the RFP or submission process may be emailed to: cina@gmu.edu

Key Themes for this RFP

We invite proposals that address key challenges represented by the four research themes of the CINA Center (see page 1). **Particularly welcome are proposals that address the following topics, detailed under the relevant challenge area:**

- **2a. Transnational Criminal Organizations (TCOs) and international migration**
- **3d. Accessing encrypted media, containers, and devices**
- **3e. Field collection, filtering, and triage tools**

Challenge Area 1: Criminal Network Analysis

Sophisticated networked criminal activities span communities and borders in pursuit of illicit profit, wreaking havoc on societies and devastating communities around the world. The criminal networks pursuing these activities have evolved from simple, localized, mostly hierarchical structures into complex, distributed, highly sophisticated networks that operate across physical and cyber spaces, from local to international scales.

Proposals in this area should address the scientific and operational challenges in discovering, analyzing, monitoring, and dismantling networked criminal activities. We seek to advance current understanding of the operational models of these networks—for example, their characteristics, interdependencies, vulnerabilities, decision-making processes, and recruitment mechanisms—and to leverage existing capabilities to capture and analyze relevant information from diverse data sources.

In the above context, topics of interest include but are not limited to:

a. **Network discovery and analysis:** Develop algorithms, techniques, and tools for network discovery from data, especially where the data sets are large, incomplete, heterogeneous, and uncertain. Model network structure, detect and disrupt activity, perform link prediction, conduct multilayer network analysis, and use artificial intelligence or other approaches to facilitate the automation of such analysis.

b. **Network modeling:** Develop configurable, parameterizable models of transnational criminal organizations that can be used to run simulations; generate high-fidelity synthetic data sets representing transnational organized criminal activity to support development and training.

c. **Entity discovery, extraction, and resolution:** Supplement existing network analysis capabilities through a combination of natural language processing and graph analytics; extract entities of interest from a corpus of documents, perform entity resolution, and proactively identify additional novel entities not yet known.

Challenge Area 2: Dynamic Patterns of Criminal Activity

"Big data" techniques to analyze patterns of criminal activity create new challenges in assessing the relevance of information within broad and diverse datasets and in studying patterns at both the micro and macro level. Overcoming these challenges will unlock opportunities to understand how, where, and when criminal activities are occurring, and to predict where they will occur next.

Proposals in this area should address analysis of criminal activities across the physical and cyber spaces and over time, with the goal of identifying relevant patterns and trends and facilitating more effective response strategies. Techniques of interest include supervised and unsupervised machine learning, predictive analytics, anomaly and outlier detection, real-time data ingestion and analysis, data fusion, and digital twins.

In the above context, topics of interest include but are not limited to:

a. **Transnational criminal organizations (TCOs) and international migration: Assess how TCOs and their affiliated facilitation networks have evolved in the wake of the COVID epidemic to facilitate transnational movements globally. For example, have TCOs evolved beyond government agencies' existing tactics, techniques, and practices (TTPs)? Have these networks evolved their own TTPs to align with larger trends seen in global migration, such as the use of charter flights as a means of circumventing border controls? What should policy and practitioners countering TCOs consider as these networks seek to align their TTPs to general migration patterns?**

b. **Predictive analytics:** Develop innovative approaches to discover cascading patterns of complex networked criminal activities, with the goal of advancing capabilities to detect emerging threats, predict future events, and devise appropriate responses.

c. **Convergence:** Examine the convergence of different criminal networks and activities—for example, drug networks and migrant smuggling networks that share actors or routes, or supply chains that include both human trafficking and Illegal Unreported and Unregulated (IUU) fishing.

Challenge Area 3: Forensics

CINA's research spans both traditional and digital forensics. Modern technologies are revolutionizing the practice of traditional forensics; nevertheless, even some centuries-old techniques remain poorly understood. For example, canines are widely used in investigative work; however, what canines smell is still not well understood, and more research is needed to support case investigations and the presentation of scent evidence in court.

Meanwhile, digital forensics has been challenged by new sources of evidence not just from computers or smart phones, but also the "internet of things": smart devices, network communication equipment, drones, vehicles, and many other kinds of sensors—in fact, anything with the ability to store and process digital data. Investigators are encountering new and novel chipsets in evidentiary items that are not accessible via existing methods; this has created a need for increased research and methodologies related to hardware and software reverse engineering (RE) and hardware side channel attack development and analysis. Furthermore, while computer forensics agents/analysts often know what software needs to do, they may not be able to write code to accomplish the task; therefore, investigators require updateable and easily maintained toolsets for multiple, dispersed field offices to parse and analyze multiple data structures.

Proposals in this area should advance improvements in traditional forensics or develop new methods for the acquisition and analysis of data stored on digital media.

In the above context, topics of interest include but are not limited to:

Traditional Forensics

a. **Substance testing and searching**: Improve rapid field testing of suspected illegal drugs; research canine scent detection, including but not limited to human remains, currency, and illegal drugs.

b. **Materials forensics**: Advance comparative dating through paper degradation pathways by ways of hydrolysis.

c. DNA analysis: Develop DNA analysis to support human identification from skeletal remains, as well as detection and investigation of migrant smuggling and human trafficking; improve current techniques for rapid DNA analysis and genetic genealogy.

Digital Forensics

d. Accessing encrypted containers, media, and devices: Develop methods for accessing and decrypting encrypted digital content on devices (preferably methods that are broadly applicable, but we are also interested in device or class-specific mechanisms); develop methods for virtualizing devices and encrypted storage to facilitate research, exploration, and brute force methods of access and decryption; develop parallel processing algorithms and techniques for brute force and analytic processing.

e. Field collection, filtering, and triage tools: Develop tools and techniques for collecting digital forensic data from cyber physical and embedded systems in the field. For example, approaches and algorithms for filtering at the point of collection; tools and techniques for field triage on digital devices and media prior to seizure; or cataloging data retention and transmission behaviors of digital devices, whether embedded or standalone.

f. **Dynamic scripting solutions for computer forensics**: Develop capabilities for the dynamic delivery of programming/coding solutions to technical issues that arise during digital forensic analysis. For example, given basic input parameters, such a capability might deliver a script to execute a customized brute force password guessing attack against a non-standard system or SQL instructions to discover the structure of an unknown database and create a report in a format useful to the investigator.

Challenge Area 4: Criminal Investigative Processes

Innovative tools and analyses transform criminal investigative processes by expanding the capability to collect, manage, protect, analyze, and share enormous amounts of structured and unstructured data.

Proposals in this area should assess the impact of investigative processes on networked illicit activities and on society more broadly.

In the above context, topics of interest include but are not limited to:

a. **Integration of automated methods into criminal investigation:** Develop automated and human-in-the loop methods to triage and adjudicate evidence generated by a machine learning analytic.

b. **Virtual reality and crime scenes:** Explore the potential to use virtual reality for crime scene reconstruction, investigation, and training; types of crime scenes may include mass shootings and other crimes of violence.

c. **Human trafficking:** Examine innovative approaches to investigations of human trafficking, with the goal of disrupting transnational criminal organizations.

d. **Effectiveness and impact:** Systematically review the effectiveness of different investigative approaches and/or the social outcomes of investigations.

Challenge Area 5: Training

As a complement to the four challenge areas above, CINA solicits proposals to develop and deliver relevant training, either as a stand-alone proposal or as part of a broader research proposal. For example, a proposal to develop a new tool or technique might include training for DHS investigators and analysts in the use of the tool or technique. We welcome proposals for training in synchronous and asynchronous modalities and in guided and self-directed formats. Training proposals should include development and, optionally, delivery of new training content; they should not be limited to the purchase or delivery of existing content.

In the above context, topics of interest include but are not limited to:

a. **Analytics**: Develop guides, manuals, or training on the use of data in historic, predictive, and prescriptive analytic techniques for intelligence gathering, investigative processes, and alternative analysis methodologies—for example, red teaming, scenario analysis, and tabletop exercises.

b. **Crime scene procedures**: Develop training on basic and advanced crime scene procedures, such as blood spatter, photography, trajectory, and accident reconstruction; emerging threats and best practices in fast, accurate field collection under emergency field crime scene recovery conditions; aerial collection to map crime analysis or other technology that could be used to assist in crime scenes; electronic data recovery and the best tools for basic extraction; and crime scene 360 degree collection including best practices, restrictions, issues, and existing tools.

c. **Financial crimes:** Develop training to investigate financial crimes or crimes with a financial component.

APPENDIX A

Definition of Third-Party Data

Third-party data: Data collected from sources where the researcher is **two or more** steps removed from the original primary or posted source—that is, data that is **not** directly collected from the subjects themselves and **not** collected directly from the website or platform with which the data sources or subjects have interacted (adapted from online source).

Examples that may be considered third-party data:

- Researchers access data through an aggregator or other platform that collects or shares data from several different sources.
    - Example: NIBRS data, or similar aggregated sources. (0) LE agency data → (1) NIBRS → (2) researcher uses NIBRS data. This is **two steps** away from the source.
- Researchers collect data from various sources and post them to a different public platform as a research dataset.
    - Example: A set of public YouTube videos collected by other researchers and posted on a public site such as Kaggle. (0) Original YouTube upload → (1) researcher A's collected dataset posted to Kaggle → (2) researcher B uses collected dataset. This is **two steps** away from the source.

Examples that may not be considered third-party data:

- Researchers collect data directly from a human interaction/intervention or generate data using a digital process—that is, researchers create a set of synthetic, cyber, or digital artifacts.
- Researchers collect data directly from a public social media platform, or public online forum where the original source is posted, and researchers are only one step removed from the source— that is, the source is not a link to someone else's data.
    - Example: Public posts on Twitter/X (where the post is not a link to someone else's data) → (1) PI/researcher. This is **one step** away from the source.
    - Example: Public posts on an online public forum (where the post is not a link to someone else's data) → (1) PI/researcher. This is **one step** away from the source.
- Researchers use publicly posted research data that was directly generated by the sharing party—for example, a researcher creates a set of synthetic, cyber, or digital artifacts.