Criminal Investigations and Network Analysis
A DHS CENTER OF EXCELLENCE AT GEORGE MASON UNIVERSITY

CINA Annual Request for Proposals, Winter 2024-2025: Submission Guidance

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

1. **Criminal Network Analysis**
2. **Dynamic Patterns of Criminal Activity**
3. **Forensics (both traditional laboratory forensics and digital forensics)**
4. **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. 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/.

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). **For the 2025-2026 program year, CINA is particularly interested in proposals that address DHS's mission to secure U.S. borders and approaches from the threat of Transnational Organized Crime (see: https://www.dhs.gov/secure-us-borders-and-approaches)**. Particularly welcome are proposals that address the following topics, detailed under the relevant challenge area:

1a. Designing performance metrics for counter-network operations
3c. Extracting data from mobile devices
3d. Assessing the role of networked technologies in tactical operations
4a. Supporting law enforcement practitioner resilience
5a. Keeping training current

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 process, and recruitment mechanisms—and to leverage existing capabilities to capture and analyze relevant information from diverse data sources.

Topics of particular interest include, but are not limited to:

a. **Designing performance metrics for counter-network operations:** Law enforcement agencies are successfully using counter-network operations to illuminate, disrupt, and degrade criminal networks. However, lack of performance metrics for these operations limits agencies' ability to establish resource requirements for them. CINA welcomes research proposals in support of an analytic suite to (1) design an effective counter network operation, (2) predict its rate of return, and (3) establish the level of resources needed to support it.

b. **Developing models of transnational criminal organizations (TCOs):** Configurable, parametrizable models of TCO networks could allow law enforcement practitioners to move beyond retrospective analysis of existing organizations. CINA welcomes research proposals to develop models, user interfaces, and training to enable analysts (1) to run what-if scenarios ("if an organization like X existed, what could it do, might it do, and what would the observable data look like?"); (2) configure models to match a known organization to understand their operations, test disruption scenarios, and identify data collection and pressure points; and (3) generate realistic synthetic data.

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 particular interest include: supervised and unsupervised machine learning, predictive analytics, anomaly and outlier detection, real-time data ingestion and analysis, data fusion, and digital twins.

Topics of particular interest include, but are not limited to:

a. **Discovering networks from data:** Law enforcement practitioners have increasing access to both sensitive and publicly available data; however, data sets are usually large, incomplete, heterogeneous, and uncertain (dirty). CINA welcomes research proposals to develop algorithms, techniques, and tools for network discovery from data. (See more information regarding use of data in the "Research data" section below.) Such work might identify non-obvious connections across data sets, suggest additional data to collect/ingest, and present multiple hypothetical networks behind the data.

b. **Generating synthetic data sets:** Law enforcement agencies often cannot share classified and sensitive data with researchers; however, researchers require realistic datasets to develop and test new network analysis techniques. CINA welcomes research proposals to research, develop, evaluate, and validate high-fidelity synthetic data sets representing transnational organized criminal activity that can be freely shared with its research network and the broader scholarly community.

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. Meanwhile, digital forensics has been challenged by new sources of evidence not just from computers or smart phones, but also the so-called "Internet of Things": smart devices, network communication equipment, drones, vehicles, and many other kinds of sensors—anything with the ability to store and process digital data.

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.

Topics of particular interest include, but are not limited to:

<u>Traditional Forensics</u>

a. **Testing and searching for substances**: Improve rapid field testing of suspected illegal drugs; research canine detection of volatiles and perception of the scent of human remains.

b. **Applying 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.

<u>Digital Forensics</u>

c. **Extracting data from mobile devices:** 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. CINA welcomes research proposals to address (1) challenges combatting encryption in both messaging systems and on stand-

alone devices; (2) forensic methodologies for Internet of Things devices; and (3) malware/intrusion response and prevention.

d. **Assessing the role of networked technologies in tactical operations:** Many new technologies important in investigations are also used widely by the law-abiding public—for example, mobile phones, smart speakers, and doorbell cameras. Such technologies frequently communicate remotely and exchange data (the Internet of Things). The resulting practical and legal challenges have been a central focus for cybersecurity and forensic specialists; however, a gap exists in understanding how to interact with these technologies effectively and safely during tactical operations, such as when serving arrest warrants and entering households. CINA welcomes research proposals to help law enforcement agents understand (1) potential nefarious uses of networked technology in tactical contexts; (2) emerging evidence collection needs and challenges; and (3) operational and legal implications of interaction between commercial technologies and operational technologies such as drones and robots.

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.

Topics of particular interest include, but are not limited to:

a. **Supporting law enforcement practitioner resilience:** Law enforcement frequently exposes practitioners to traumatic events, resulting in a prevalence of Post Traumatic Stress Disorder (PTSD) much higher than the general population. This results in vulnerability to a host of adverse health and social outcomes. However, general psychological interventions have proven inadequate to meet practitioners' complex needs. CINA welcomes research proposals that examine the phenomena of (1) trauma and (2) moral injury in the law enforcement context and recommend strategies and interventions specific to these concepts that promote resilience and post-traumatic growth and counter vulnerability and adverse outcomes.

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

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

d. **Assessing effectiveness, impact, and bias:** Systematically review the effectiveness of different investigative approaches, including the influence of investigator bias, 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 go beyond purchase or delivery of existing content.

Topics of particular interest include, but are not limited to:

a. **Keeping training current:** To prepare law enforcement practitioners for the field, cybersecurity, forensics, and counterterrorism instructors stay up to date on new and emerging technologies, tactics, and best practices. Because these fields are evolving daily, it is difficult for instructors to keep up with the latest technologies, new trends in criminal behavior, and cutting-edge investigative tools, independent of the longer cycles of curriculum development and review. CINA welcomes research proposals to develop easily accessible ways for instructors to remain current, as well as ready-made tools and resources they can use with trainees, such as informational bulletins for awareness, short training tutorials, and job aids.

b. **Using Virtual Reality (VR) in training:** Federal partners at the state/local/tribal/territorial levels often cannot support travel and live training to improve their skills and performance in conducting criminal investigations. VR could allow practitioners to participate in hands-on training virtually but effectively in a wide range of areas. CINA welcomes research proposals to design and/or evaluate VR training for law enforcement.

c. **Understanding cryptocurrencies:** Sophisticated criminal organizations are believed to be exploiting cryptocurrencies to facilitate their unlawful activities and to obfuscate their operations. CINA welcomes research proposals to provide law enforcement practitioners basic training on cryptocurrencies and the block chain: both how block chain technology is used in general, and how it is used for cryptocurrency transactions.

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, 2025, to June 30, 2026** (CINA Program Year 9). 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 2025, 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. Research projects selected for funding through this RFP will be subject to the terms and conditions of CINA's cooperative agreement. Proposing teams are strongly encouraged to review the terms in section A.3 (pages 1-2) pertaining to protection of privacy, civil rights, and civil liberties in all DHS S&T supported research and ensure that the proposed data sources and research approach will comply with the conditions of the award. 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.

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, January 31, 2025.**

- 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.
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.
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.

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