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

CINA Special Request for Proposals on Cyber-Enabled Human Crime: Submission Guidance

The Criminal Investigations and Network Analysis Center (CINA) is soliciting proposals for research to address current and imminent challenges that the United States Department of Homeland Security (DHS) and its federal partners face in **Cyber-Enabled Human Crime**.

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

This Request for Proposals (RFP) invites submissions that address the three themes and support the related strategic initiatives developed during the Cyber-Enabled Human Crime (CEHC) Workshop hosted jointly by CINA and The Knoble in Arlington, VA, April 29-30, 2024 (https://cina.gmu.edu/cyber-enabled-human-crime-workshop/).

"Cyber-Enabled Human Crime" is the act of leveraging cyber infrastructure (the internet) to exploit victims to commit financial scams, human trafficking, child exploitation, and elder financial exploitation. The Workshop was a first-of-its-kind initiative, where leaders from law enforcement, financial services, and academia gathered to identify and solve challenges facing the financial and law-enforcement community. CINA welcomes proposals that contribute to the evidence base for the Workshop's broad themes and support the specific initiatives it launched. CINA and The Knoble can facilitate researchers' access to initiative participants and materials as a source of data for projects.

Theme 1: Advancing information sharing between law enforcement and the private sector

Financial Institutions (FIs) provide millions of Suspicious Activity Reports (SARs) and other reports to the U.S. Treasury Department's Financial Crimes Enforcement Center (FinCEN) and Law Enforcement (LE) every year. These may meet regulatory requirements and identify suspicious activity, but the information provided may not lead to, or add to, an active investigation, arrest, and prosecution. It is necessary to improve or enhance the type and quality of the information provided in the reports to: (1) provide more actionable intelligence that could be used to begin or enhance proactive detection by the Fis, and (2) expand investigation efforts leading to higher value information passed to LE. Proactive intelligence and expanded sharing in various forms may include a modernization of the current SAR process, reinforcing SAR formats with data that can be used in LE analytic efforts and/or targeted intelligence sharing by LE across financial entities. All of these must preserve the privacy of citizens and the security of the data being delivered.

The Workshop launched an initiative to bring together law enforcement and financial institutions to discuss and document effective practices for including key information in Suspicious Activity Reports (SARs) that will make financial institution information and data provided more usable for law enforcement. This project's output will be a best practice guide and a pilot initiative to measure the effectiveness of the guide in use; CINA welcomes research that can support development of the guide or its validation.

Theme 2: Mounting nationally coordinated education and awareness campaigns

Various agencies, financial institutions, associations, and non-governmental organizations (NGOs) have developed and deployed education and awareness campaigns. However, campaigns in the private sector are driven by individual entities, limiting their impact and reach. What is needed is a series of nationally coordinated education and awareness campaigns. Like other global approaches, a coordinated collective impact model can bolster individual efforts and significantly increase the effectiveness of human crime prevention.

The Workshop endorsed nationally coordinated education and awareness campaigns for customers of financial institutions and/or the public, creating simple and clear messaging that leverage the best insights and ideas from industry to help reduce human crime.

Theme 3: Educating law enforcement and private sector professionals

Financial institutions and law enforcement engage thousands of professionals. They are smart, educated and trained by their agency or institution to do their jobs well. Often, information regarding the capabilities and processes of other agencies or institutions is acquired over time, through experience and relationships developed throughout a career. It would be beneficial if professional education could be developed and accelerated to instruct and align the language, capabilities and processes of different agencies and institutions. A better mutual understanding and appreciation of supporting approaches will lead to a higher quality collaborative approach, beyond what is minimally required by regulation.

The Workshop identified countering sextortion as an urgent priority for law enforcement and private sector education. It created a forum that brings together a cross section of subject-matter expert leaders to map this crime from channels of engagement through interaction, money movement, escalation, law enforcement, and prosecution. The objective is to identify which player(s) in the ecosystem can take preventive or detective education and/or action at every point in the execution of the crime.

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

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/rfps/cina-targeted-rfp-2024-cyber-enabled-human-crime/ 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