CINA Annual RFP, Winter 2022-23: Submission and Review Process

CINA is seeking white papers presenting research ideas intended to address questions and challenges that CINA, DHS, and/or its federal partners are currently facing, or are expected to be facing in the near future. This RFP invites proposals that will address main challenges represented by the four research themes of the CINA Center. CINA leadership and DHS center managers and sponsors will review white paper submissions and will request detailed workplans for proposals selected for further review. A formal request for full workplan development does not guarantee a grant award. Projects typically range from 6-24 months in duration (pre-transition) and have funding levels from $50k to $250k per year. Research projects selected for funding are expected to start work between July – September, 2023.

In keeping with the mission, nature, and authorities of the CINA center, research proposals are expected to produce algorithms, methods, and/or tools which 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. Also of interest are studies and knowledge products that advance our understanding of criminal network operations and investigations of them, as well as training development and delivery in support of DHS and law enforcement efforts to combat transnational organized crime groups and their activities. Research proposals which are primarily software or hardware development efforts, or which directly support law enforcement actions as part of the research project activities, are outside of the scope of the center's operation.

A white paper submission should contain the following sections and is expected to be no more than five (5) pages in length, single-spaced, 11- or 12-point font with 1" margins. Appendices beyond five pages or external links should only be used when necessary to convey a critical aspect of the proposed research.

White Paper sections:

- **Executive Summary**
- **Problem**: Description of the essential problem area.
- **Prior and Related Work**: Discussion of prior work, related work, and state of the art.
- **Approach**: A sufficiently detailed description of the proposed approach to address the identified problem.
- **Data**: Describe the data or datasets to be collected and/or used for the research[1].
- **Institutional Review Board (IRB)**: Whether or not the project is expected to include Human Subjects Research (HSR) or require IRB approval for other reasons.

[1] Under CINA’s cooperative agreement, no raw research data may be shared with DHS, and DHS cannot provide data to be utilized for research. Projects which use 3rd party data (which includes social media and other public data) or data which may raise privacy concerns are not precluded from funding, but may require time for additional reviews and approvals. CINA will work with PIs to facilitate these reviews, and proposers may include these additional reviews in their estimated timelines as funded activities.

- **Team Experience and Resources**: Provide evidence supporting the team's ability to perform the proposed effort.
- **DHS Relevance**: Identify the anticipated impact for DHS and/or law enforcement, and the DHS component or components most likely to be interested in the conduct and outcomes of the proposed research.
- **Timeline**: A high level timeline for the project.
- **Cost Estimate**: Rough order of magnitude cost estimate for the project.
- **References**: Not included in page count.

Submissions will be accepted through Jan 31, 2023. Please send white paper submissions via email to cina@gmu.edu, with the subject line “CINA Annual RFP 2023.”

White papers will be subject to a formal review process, including evaluation by external subject matter experts, to identify those proposals that will be invited for full workplan development and consideration for potential grant awards.

If a white paper results in a request for a workplan, that document will be expected to include the following sections and is expected to be no more than ten (10) pages in length, single-spaced, 11- or 12-point font with 1" margins. Appendices beyond ten pages or external links should only be used when necessary to convey a critical aspect of the proposed research.

Workplan sections:

- **Project Title**
- **List of Principal Investigators/Other Personnel**
- **Overall Budget**: Broken down by cost type (direct and indirect) and quarter.
- **Background and Purpose**: Including executive summary, purpose, operational need and alignment to DHS strategic goals, and impact to the HSE and specific stakeholders.
- **Research Objectives and Resulting Products**
- **Technical Approach and Risks**
- **Data**: Describe the data or datasets to be collected and/or used for the research, and how the data will be (or was) collected, stored and protected, de-identified (if needed), and shared (if appropriate).
- **Institutional Review Board (IRB)**: If appropriate, describe the Human Subjects Research (HSR) aspects of the project or other aspects which may require IRB approval. If IRB review is anticipated, confirm that the PI(s) are familiar with their institutions IRB process, are willing to participate in that process, and provide a rough timeline for IRB review and approval.
- **Project Milestones**
- **Customer Engagement and Requirements**
- **Technology Transition Plan and Intellectual Property Management**
- **References**: Not included in page count.

Workplans should not be submitted at this time. If appropriate, they will be requested after white paper review. A template will be provided at that time.

Key Themes for this RFP

This RFP invites proposals that will address main challenges represented by the four research themes of the CINA Center:

Challenge Area 1: Criminal Network Analysis

Today, sophisticated networked criminal activities cross 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 the physical and cyber spaces, and also at a variety of scales, ranging from local to international. Detecting, analyzing, monitoring, and dismantling such activities presents a number of scientific and operational challenges. Overall, we seek to advance our understanding of the operational models of these networks (e.g. their characteristics, interdependencies, vulnerabilities, decision-making process, and recruitment mechanisms), and our ability to capture and analyze relevant information from diverse data sources (ranging from authoritative to open-source content).

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

- **Entity extraction, resolution, and discovery**. Projects will supplement our network analysis capabilities by using a combination of natural language processing and graph analytics to extract entities of interest from a corpus of documents, perform entity resolution, and proactively identify additional novel entities not yet known.

- **Cryptocurrency and criminal activity:** Detecting and tracing money laundering and other criminal activity in digital currency services and markets.

- **Network analysis:** Network structure discovery and modeling, activity detection and disruption, link prediction, multilayer network analysis, and artificial intelligence or other approaches to facilitate the automation of such analysis.

- **Criminal network operations:** Advancing our understanding of how such networks recruit members, organize their operations (including assessing the extent to which they rely on technology to pursue their goals), advertise their services, communicate and interact internally and externally (e.g. with other illicit networks, such as terrorist networks), invest their profits, and how they respond to threats.

- **Evidence correlation and discovery:** Methods and algorithms for discovering correlations and associations across diverse evidence sources and types (approaches may be automated or human-assisted).

Challenge Area 2: Dynamic Patterns of Criminal Activity

Analyzing criminal activities across the physical and cyber spaces and over time, to identify relevant patterns and trends, is essential for the emergence of more effective response strategies. As the analysis of patterns of criminal activity meets big data, we are facing newfound challenges and opportunities. Some challenges and opportunities are associated with the breadth and diversity of relevant datasets, and the ability to study relevant patterns at both macro and micro spatiotemporal settings. Conquering these challenges will allow us to better understand how, where, and when criminal activities occur, and to better predict where they will be occurring next.

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

- **Environment and criminal activity**. Projects in this area will study the link between natural disasters/climate change and downstream criminal activities, to include impact mapping.

- **Innovative spatiotemporal pattern detection:** The detection of relevant spatiotemporal patterns from diverse datasets, and the ability to contrast such data to diverse complementary datasets (e.g., sociodemographic or economic data) in order to advance our understanding of the correlation between place and crime and the mechanisms that drive the birth and death of crime hotspots, including forecasting future hotspots with machine learning and other tools.

- **Predictive analytics:** Innovative approaches for the discovery of cascading patterns of complex networked criminal activities in order to advance our ability to predict forthcoming events, detect emerging threats, and devise appropriate response strategies.

- **Convergence:** Convergence of different criminal networks and activities, e.g., drug networks and human smuggling (for example shared actors and routes**)**, or connections between Illegal Unreported and Unregulated (IUU) fishing and human trafficking in supply chains into the United States and other areas.

Challenge Area 3: Forensics

In the context of networked criminal activities as they are studied by the CINA Center, the center's research interests span both traditional and digital forensics. Traditional forensics are boosted by the emergence of technological solutions that may revolutionize the manner in which they are conducted. Digital forensics presents some emerging challenges, as digital evidence is no longer just specific to information obtained from computers or smart phones, but now includes smart devices, the internet of things, vehicles, and a myriad of sensors - essentially anything with the ability to store and or process digital data. Accordingly, investigators require updated 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:

- **Latent fingerprints**: Projects in this area will address one or more of the following:
  - Statistical model for latent fingerprint decisions.
  - Technology to capture developed latent prints and determine sufficiency scale for value.
  - Black box study of LP 5 point scale with LP set to determine feasibility of agencies using scale consistently.

- **Materials forensics**: Comparative dating through paper degradation pathways by ways of hydrolysis.

- **DNA analysis**: DNA analysis to support human identification from skeletal remains, detection and investigation of human smuggling and human trafficking activity to include improvement of current techniques, rapid DNA analysis and genetic genealogy.

- **Substance testing and searching**: Rapid field testing of suspected illegal drugs; research into volatiles and the study of canines; human remain search canines.

- **Forensic confirmation biases.** Research in this area will study the well-established phenomenon that biases that creep into the forensic sciences, many of which were not developed using scientific methods (e.g., toolmark, bitemark analyses; hair analysis; etc.) and rely on human judgement.

Digital Forensics:

- **Software and Hardware Reverse Engineering for Computer Forensics**. Given the widespread prevalence of embedded microcontrollers in IoT, network communication equipment, drones, vehicles, etc., investigators encounter new and novel chipsets in evidentiary items that are generally not accessible via existing methods. There is a need for increased research and methodologies related to hardware and software reverse engineering (RE) and hardware side channel attack development and analysis. Such research will support accessing forensic evidence via hardware vulnerabilities and associated exploits. Reverse engineering hardware will allow for examiners to determine how the device functions at the circuit level and find vulnerabilities that can allow for the potential to obtain evidence. Software RE is a complementary skill set to hardware RE and is also of interest. Projects should propose research and development of novel RE techniques (vs executing RE on a specific platform), should apply to as large a set of devices as possible, and will ideally be extensible and long term (as opposed to limited shelf-life bug hunting).

- **Dynamic Scripting Solutions for Computer Forensics**. While the computer forensics agent/analyst often knows what needs to be done, they may lack the ability to write the code to accomplish the task. Projects in this area will 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.
    - SQL instructions to discover the structure of an unknown database and create a report in a format useful to the investigator.

- **Cloud Based Analytic Tools to Analyze Computer Forensic Data**. Investigators require updateable and maintainable toolsets for multiple, dispersed field offices to parse and analyze multiple data structures. Projects may study and report on the existing state of the art (to include gap analysis and emerging/future developments), and/or may propose to develop new tools and techniques.

- **Field collection, filtering, and triage tools:** Tools and techniques for collecting digital forensic data from cyber physical and embedded systems in the field:
    - Approaches and algorithms for filtering at the point of collection.
    - Performing field triage on digital devices and media prior to seizure.
    - Studies which catalog data retention and transmission behaviors of digital devices, whether embedded or standalone.

- **Accessing encrypted containers, media, and devices:** Methods for accessing and decrypting encrypted digital content on devices (broadly applicable methods are of the most interest, but device- or class-specific mechanisms are of interest as well), methods for virtualizing devices and encrypted storage to facilitate research, exploration, and brute force methods of access and decryption, and parallel processing algorithms and techniques for brute force and analytic processing.

Challenge Area 4: Criminal Investigative Processes

Criminal investigative processes are transformed through innovative tools and analyses that expand our capability to collect, manage, protect, analyze, and share large amounts of structured and unstructured data. Furthermore, there is an increased need to assess the impact of these investigative processes not only on the networked illicit activities, but also on society at large.

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

- **Labor trafficking**. Research on this topic will include studies at the investigation and interviewing phases, understanding why and how perpetrators engage in these activities, and examining challenges to prosecution.

- **Virtual reality and crime scenes.** Research and development into virtual reality for crime scene reconstruction, investigation, and training. Types of crime scenes may include mass shootings and other crimes of violence.

- **Effectiveness and impact**. Systematic review of the effectiveness of different investigative approaches, and/or a study of the social outcomes of investigations.

- **Open source intelligence**. Projects in this area will develop analytical tools and techniques re: identification, collection, and analysis of open source information to support activities such as vetting individuals entering the U.S., vetting companies engaged in the export of technology to disrupt shipments to embargoed nations, and enforcement of UFLPA.

Challenge Area 5: Training

Proposals for training development and delivery across the CINA areas of interest are invited. Synchronous and asynchronous, as well as guided and self-directed, modalities are of interest. Proposals should include development and optionally delivery of new training content and not be limited to the purchase or delivery of existing content. Training may be incorporated into research proposals which also address one or more of the four areas and topics above (e.g., research to develop a new tool or technique and training DHS investigators and analysts on the use of such a tool or technique).

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

- **Crime scene training/courses**:
  - Basic and advanced crime scene courses:
    - Blood spatter, photography, trajectory, accident reconstruction
    - Emerging threats and best practices in fast but accurate field collection in emergency field crime scene recovery
  - Aerial collection: map crime analysis or other technology that could be used to assist in crime scenes
  - Electronic data recovery and best tools for basic extraction
  - Crime scene 360 degree collection – best practices, restrictions, issues, existing tools

- **OSINT**: Training on the use and analysis of open source information for investigations.

- **Analytics**: Guides, manuals, and/or training to support the use of data-centric analytic techniques, and/or training to provide a deeper understanding of potential applications for historic, predictive, and prescriptive analytic techniques on intelligence gathering, investigative processes, and alternative analysis methodologies (red teaming, scenario analysis, tabletop exercises).

- **Financial Crimes.** Training on the investigation of financial crimes, and crimes with a financial component.