



**Criminal Investigations  
and Network Analysis**

A DHS CENTER OF EXCELLENCE

## **Request for White Papers Spring 2019**



### **CINA Request for White Papers**

Issue Date: March 15, 2019

Extended white paper submission due date for full consideration: April 12, 2019

Contact info:

Ms. Kerry Riddle

Phone: (703)9934409

Email: [cinaRFP@gmu.edu](mailto:cinaRFP@gmu.edu)

Web: <https://cina.gmu.edu>

## **TABLE OF CONTENTS**

---

<b>I. About CINA</b>	4
I.a Mission of the CINA Center	4
<b>II. RFP Focus Areas</b>	5
II.a Scope of the White Paper Submission and Review Process	5
II.b CINA Research Thematic Areas	5
II.c Key Themes for this RFP	5
<b>III. RFP Submission Guidelines</b>	9
III.a Estimated Funding	9
III.b Eligibility	9
III.c Deadline and Submission Instructions	9
III.d White Paper Content	9
III.e Review Criteria	11
III.f Notifications	11
III.g Proposal-Related Communications	11
III.h Equity Statement	11
III.i Intellectual Property Guidelines	11

## **I. ABOUT CINA**

---

### **I.a Mission of the CINA Center**

The [Criminal Investigations and Network Analysis \(CINA\) Center](#) is a DHS Center of Excellence. It is an academic consortium comprising an evolving network of University partners, with George Mason University (Mason) serving as its home.

The rapid pace of innovation in information and communication technologies has revolutionized the world as we know it, both here in the United States and around the globe, fueling growth in many sectors of the economy and improving public services in areas such as education, healthcare and public policy. While these technological innovations promise continuing improvements in the quality of life for individuals the world over, criminal organizations have also capitalized on these transformative advances to become more agile and expand their illicit activities. Today, sophisticated criminal networks can easily appear, disappear, and reorganize in response to operational opportunities and authority gaps. These networks function as complex social structures across the cyber and physical spaces, and operate at a variety of scales, ranging from local to international.

Given the newfound agility and increased complexity of these networks, we need a better understanding of their operations, collaborations, and societal impact. There is, therefore, an urgent and persistent need for innovation in the fields of criminal investigations and network analysis, to allow us to better comprehend and respond to these new and evolving challenges.

In response to the above-stated need, the mission of the CINA Center is to be a *strategic innovation partner* for Homeland Security Enterprise (HSE) stakeholders in their efforts to combat networked criminal activities. By concurrently pursuing scientific advancements and practice breakthroughs, CINA will help the HSE to better comprehend and respond to the challenges posed by such illicit operations, to better anticipate the evolution of these operations and anticipate emerging challenges.

## **II. RFP FOCUS AREAS**

---

### **II.a Scope of White Paper Submission and Review Process**

CINA is seeking white papers presenting research ideas intended to address research questions/challenges that CINA, DHS, and/or its federal partners are currently facing, or are expected to be facing in the future. CINA leadership and DHS sponsors will review white paper submissions to identify those for which a full proposal will be requested.

The purpose of a white paper submission is to convey to the submission reviewers the essential problem area, demonstrate knowledge of prior art, identify a research gap, propose a sufficiently detailed approach to address said problem, and provide evidence supporting the ability to perform the proposed effort. These white papers will be subject to a formal proposal review process, including evaluation by external subject matter experts, to identify those proposals that will be invited for full proposal development and will be considered for potential grant awards. A formal request for full proposal development does not guarantee a grant award.

### **II.b CINA Research Thematic Areas**

In pursuit of its mission, the CINA Center is pursuing the advancement of science and practice across four **research themes**, described below:

- **Criminal Network Analysis:** intended to advance the understanding of the operational structure and particularities of networked criminal activities, in order to support the emergence of more effective means to disrupt the organizations that pursue them.
- **Dynamic Patterns of Criminal Activity:** intended to advance the analysis of criminal activities across the geographical, social, and cyber dimensions, and across a wide variety of data sources, in order to support the emergence of more effective means to identify and monitor such patterns and the activities they signify.
- **Forensics:** intended to advance the state-of-the-art in forensic methods, tools, and technologies.
- **Criminal Investigative Processes,** intended to improve HSE end user investigative processes used to detect, pursue and solve networked criminal activities.

A high-level overview of currently funded CINA research projects may be found at:

<https://cina.gmu.edu/research/>

### **II.c 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:

**Network analysis:** Issues of interest include advancing community structure and detection, link prediction, and multilayer network analysis.

**Criminal network operations:** Issues of interest include 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.

**Cryptocurrency, blockchain, and money laundering:** Issues of interest include tracing money laundering operations through digital coin services, including the nexus of illicit networks and terrorism, as well as trade-based money laundering activities.

**Illicit supply and value chains:** Issues of interest include improving our ability to map illicit supply and value chains in the physical and cyber spaces, identifying the nexus of various illicit chains (e.g. human trafficking, opioids, weapons, terrorism), and devise methodologies and tools to assess vulnerabilities of these chains.

**Online content similarity assessment:** Issues of interest include techniques that advance our ability to analyze anonymously contributed online content (e.g. tweets, posts, ads) in order to identify network structure, information diffusion and influence patterns, authorship attribution, and commonalities across diverse data sources.

## **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 enters the era of 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:

**Innovative spatiotemporal pattern detection:** Issues of interest include 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

**Predictive analytics:** Issues of interest include innovative approaches for the discovery of cascading patterns of complex networked criminal activities in order to advance our ability to predict forthcoming events and devise appropriate response strategies.

### **Challenge Area 3: Forensics**

In the context of networked criminal activities as they are studied by the CINA Center, the spectrum of forensics spans from traditional to digital forensics. Traditional forensics are boosted by the emergence of technological solutions that may revolutionize the manner in which they are conducted. The digital part of this spectrum presents in particular some newfound challenges, as digital evidence is no longer just specific to information obtained from computers or cell phones, but can now include smart devices across the internet of things. Accordingly, investigators require updated methods for the acquisition and analysis of digital media.

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

**Field collection / filtering / triage tools:** Issues of interest include tools and techniques for collecting data from cyber physical and embedded systems in the field, to include approaches and algorithms for filtering at the point of collection and performing field triage on digital devices and media prior to seizure (of particular interest are methods which apply across a wide range of devices based on ubiquitous access interfaces and common internal structures).

**Accessing encrypted containers/media/devices:** Issues of interest include 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.

**Biometrics:** Issues of interest include methods for circumventing and deceiving biometric authentication mechanisms (may include, but is not limited to, creation of fake biometric inputs), and issues associated with privacy in the use of such information.

**Deployed Biometrics:** Issues of interest include the utilization of DNA short nucleotide polymorphisms (SNP) technology to more quickly and more thoroughly identify related/unrelated individuals than current rapid DNA short tandem repeat (STR) technology.

**Evidence correlation / discovery:** Issues of interest include methods and algorithms for discovering correlations and associations across diverse digital evidence sources and formats (approaches may be automated or human-assisted).

### **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 the society at large.

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

**Multimedia analytics:** Issues of interest include advanced video and audio analysis solutions that support investigations, including but not limited to advancements in the

content-aware transmission of large image data in mobile environments, and the synthesis of multiple views in support of forensics analysis.

**Assessing intelligence gaps in criminal investigations:** Issues of interest include techniques to assess information gaps in on-going investigations, and use this knowledge to better focus said investigations (e.g. through the recommendation of additional data collection, evaluation, and analysis processes).

**Measures of effectiveness:** Criminal investigative processes have direct and indirect impacts: directly on the criminal operation itself, by disrupting it, and indirectly on society, by improving the conditions of communities that were affected by these criminal operations. We are interested in innovative approaches to assess these impacts of investigations.

**Interviewing Human Trafficking Victims:** Human trafficking victims pose unique challenges to interviewers, though their cooperation is essential to the prosecution of human traffickers. Research studies identifying and/or testing appropriate and developmentally appropriate methods to interview this understudied population are requested

**Predictive policing:** Issues of interest include establishing and validating behavioral factors and indicators exhibited by suspected perpetrators to be utilized by law enforcement officers at entry portals via human observation and/or video analytics.

### **Cross-Cutting Application Areas of Interest**

There is particular interest at this time in applications that relate to opioids, human trafficking, and the use of cryptocurrency to support illicit activities. Therefore, we would particularly encourage proposals that present innovative approaches to study these problems. This includes, in addition to the above-identified challenge areas set in the context of these application areas, the establishment of searchable databases for these problems.

ALL SELECTED PROJECTS MUST BE ABLE TO COMPLETE THE PROPOSED RESEARCH USING SIMULATED AND/OR SYNTHETIC DATA OR VIA NON-DHS DATA SOURCES. PROJECTS NEED TO IDENTIFY THEIR ANTICIPATED DATA SOURCES.

Researchers and analysts should be able to obtain access to needed analytical products, criminal investigative data, and open source and publicly available information. They also should anticipate interacting with criminal investigators and other subject matter experts. Applicants must discuss any needs for unique or sensitive data, testing, or laboratory facilities that will be required to conduct the research, and how the applicant will ensure its researchers can access the data and facilities

DHS is unable to provide operational data suitable for algorithm development and testing to performers under this award. Each proposal must identify how and where it will acquire real, simulated, or other synthetically generated data.



### **III. RFP SUBMISSION GUIDELINES**

---

#### **III.a Estimated Funding**

CINA research projects typically range from small exploratory efforts, at a level of effort of 6 months and funding of up to \$50,000 to full projects at a level of effort of up to 24 months and a total budget (including indirect) of up to \$400,000.

#### **III.b Eligibility**

CINA grants are made to US Universities. CINA does not directly award grants to private industry, private nonprofit organizations and foundations, or to federal, state, county, or local government entities — though those groups may be partners in the work conducted by the grant recipient. Collaborations among organizations are encouraged, but not required. The proposal's designated principal investigator must be an employee of the organization applying for a CINA grant.

#### **III.c Deadline and Submission Instructions**

For full consideration, white papers should be received by 5pm Eastern Time on **April 12, 2019**.

White papers must be submitted via email to [cinaRFP@gmu.edu](mailto:cinaRFP@gmu.edu). White papers should not exceed 5 pages, excluding bibliography and CVs, and must be submitted as a single PDF file. White papers should use 1-inch margins, and at least 11-point font. Submissions that exceed the stated page limit may be rejected without review.

CINA will treat white papers as proprietary. If a white paper is eventually selected for funding, that proposal may eventually become subject to public disclosure. Non-selected white papers may be retained by CINA for possible future consideration and, if retained, will continue to be treated as proprietary. Please note that white papers will be reviewed by internal and external expert reviewers.

#### **III.d White Paper Content**

White papers **must contain** all of the following elements.

##### **PART 1. COVER PAGE (1 page)** containing the following information

- Principal Investigator name, affiliation, and contact information
- Co-Principal Investigators and their affiliations
- Administrative contact
- Project title
- Primary CINA Theme Area that the proposal is addressing (also list secondary areas if applicable)
- Projected duration of the effort
- Projected total budget

##### **PART 2. PROJECT NARRATIVE (up to 5 pages)** containing the following sections:

###### **2.i Executive summary**

- Identify the research question/challenge and/or operational need that this research project will address.
- Provide an overview of the research concept being proposed.
- Identify your research objective.

- Detail how you will pursue this objective.
- Identify deliverables and tangible outcomes of this effort, and detail how they will advance CINA’s mission and DHS operations.
- Identify the targeted DHS components that are expected to directly benefit from this project.

**2.ii Background**

- Identify the current state of science and best practices in your target domain.
- Identify the gap or opportunity for operational improvement that your project is addressing.

**2.iii Scope of Work**

- Identify in detail the goals and objectives of the project with particular emphasis on the immediate period of performance.
- Describe in adequate detail the project concept, including:
  - a. Describe how your project will improve upon the above (2.ii) identified current state-of-the-art.
  - b. Clearly describe your proposed research methodology.
  - c. Identify key risks for the performance of the proposed effort, and present mitigation strategies to address them.
  - d. Include a table with comprehensive descriptions of anticipated milestones and deliverables to be provided to CINA, including mid-project and final reports. (A couple of sample entries for this table are provided below. Edit and add rows as necessary.)

<b>Description of Proposed Deliverable</b>	<b>Completion Date After Receipt of Order</b>
<i>Example: Report - Results of Literature Review</i>	<i>4 weeks</i>
<i>Example: Software – A solution for Task A</i>	<i>16 weeks</i>
<i>Example: Software – Demo to Customer</i>	<i>24 weeks</i>

- e. Discuss plans for the transition of the project findings to the stakeholder community.

**2.iv Benefits to DHS and/or the Homeland Security Enterprise**

Describe the benefits that would accrue to DHS and/or the Homeland Security Enterprise through successful completion of your research. To the extent possible identify *specific* DHS components and agencies that you consider as the primary beneficiaries of this project (herein referred to as *customers*), and describe your proposed plan for customer engagement throughout the project (e.g. regular conference calls, regular visits, plans for transition of findings).

**2.v Qualifications**

Summarize the expertise and capabilities of the research team, including:

- The senior personnel (PI and co-PIs) credentials in this topic area, including past relevant accomplishments.
- Potential public- and private-sector partners.
- Any commitments from partners in terms of collaboration and resources.

## **2.vi Estimated Cost**

Detail the total estimated cost for the research discussed in the white paper for the duration of the effort.

**PART 3. APPENDIX (page limit: as appropriate)** containing the following information:

- 2-page biographical summaries for senior personnel members (PI and co-PIs)
- A brief summary (up to 1 page) of notable in-house capabilities/facilities that the research team will use to pursue this project, if applicable.
- Additional documentation that the PIs feel as critical to the project (e.g. letters of commitment from potential partners).

Although a page limit is not specified for the Appendix, the applicants are strongly encouraged to exercise discretion in providing additional material.

## **III.e Review Criteria**

White papers will be reviewed for two sets of criteria:

- i) **Academic Merit (50%):** The proposal must present a thorough understanding of the current state-of-art of the corresponding scientific domain and make a contribution to advance that field. The CVs of the PIs must support their ability to pursue and complete the proposed research effort.
- ii) **CINA Mission Relevance (50%):** The proposal must present a clear contribution to the mission of CINA and address the priority areas identified herein. Typically, mission relevance can be expressed through the identification of a suitable stakeholder from the Homeland Security Enterprise (HSE).

## **III.f Notifications**

CINA will strive to notify applicants within 3 weeks after white paper submission whether a full proposal will be requested. Information on the content of that full proposal will be provided directly to the successful applicants. The grant award process may take an additional 4 to 6 weeks after submission of proposals, so applicants should adequately accommodate this in the project planning.

## **III.g Proposal-Related Communications**

Specific questions about this request for white papers should be addressed by email to Ms. Kerry Riddle, at: [cinaRFP@gmu.edu](mailto:cinaRFP@gmu.edu)

## **III.h Equity Statement**

The CINA Center reserves the right to fund, in whole or in part, any, all, or none of the applications submitted in response to this request for proposals. Submission requirements for this grant program may be waived at the discretion of CINA.

In accordance with George Mason University policy, CINA does not discriminate on the basis of race, color, religion, sex, sexual orientation, gender identity, national origin, age, disability of veteran status, or any characteristic protected by law.

## **III.i Intellectual Property Guidelines**

Intellectual Property (IP) that will either be brought into the project (Background Intellectual Property) or will be developed via the project will require a basic IP Management Plan **PRIOR**

**TO BEING AWARDED** should your project be selected. The IP plan should address the following if applicable to your project.

- Identify ownership of Project IP (who will *own* the IP?);
- Licensing rights of project-developed IP, including revenue sharing amount joint owners of project participants, if applicable (who will have what license rights to the IP?);
- The project participant(s) that will have rights to enforce rights in project-developed IP (who can enforce those rights?)
- Background Intellectual Property (BIP) needed for the Project and terms (if any) under which that BIP will be made available to Project Participants both during and after performance of the Project;
- Terms under which the collective IP will be made available to government and/or industry upon its transition to general use;
- Who will bear the filing and other costs of managing that Project IP, including the cost of prosecuting foreign and domestic patent rights.